İnformasiya təhlükəsizliyinin menecmenti standartlarının əlaqəli standartlarla harmonizasiyası xəritəsi: təkliflər

Elçin Əliyev[1], Yadigar İmamverdiyev[2]

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

[1]elchinaa@gmail.com, [2]yadigar@lan.ab.az

***Xülasə*— Bu məqalədə informasiya təhlükəsizliyinin menecmenti standarlarının və sisteminin digər sahələrin menecment standartları və sistemləri arasında koordinasiya məsələləri qoyulur. Bunun üçün informasiya təhlükəsizliyinin və digər əlaqəli sahələrin menecment standartları identifikasiya edilir; bu menecment prosesləri PDCA modeli üzrə təsnifatlaşdırılır; informasiya təhlükəsizliyinin menecmenti standarlarının əlaqəli standartlarla harmonizasiyası, o cümlədən səbəb-nəticə asılılıqları, terminoligiyada uyğunsuzluqlar barədə problemlər qoyulur; *“ISMS”* (ISO/IEC-27001) və *“SMS”* (ISO/IEC-20000) arasında “maraqların münaqişəsi”nin “maraqların uzlaşdırılması”na transferi məsələsi üçün həll variantları verilir.**

Açar sözlər*— *informasiya təhlükəsizliyi; menecment sistemi; menecment standartları; PDCA modeli; prosesli yanaşma; standartların harmonizasiyası; ümumi kordinasiya

I. GİRİŞ

İnformasiya təhlükəsizliyi bir praktiki fəaliyyət sahəsi və bir elmi tədqiqat istiqaməti kimi son bir neçə onillikdə formalaşmışdır. İlkin yanaşmalarda hansısa bir texniki həll vasitəsi ilə problemləri həll etməyə çalışırdılar, həllər çoxaldıqca informasiya təhlükəsizliyinin təmin edilməsinə kompleks yanaşma meydana çıxdı. Tezliklə bu yanaşmanın da problemi həll edə bilmədiyi aydınlaşdı. Hazırda əsas yanaşma ***informasiya təhlükəsizliyinin menecmenti*** paradiqmasıdır.

Bu paradiqmada əsas ideya informasiya təhlükəsizliyinə sistemin keyfiyyət göstəricisi kimi baxmaqdır. Keyfiyyəti idarə etmək mümkündür, deməli, təhlükəsizliyi də idarə etmək olar. Bu yanaşmada informasiya təhlükəsizliyi sisteminin əsas komponenti kimi texniki aspektlər deyil, menecment komponentləri götürülür.

İnformasiya təhlükəsizliyinin menecmentini optimal necə həyata keçirmək olar? Müəyyən mənada optimal yanaşma ən yaxşı təcrübədən istifadə etməkdir. Standartlaşdırma təşkilatları informasiya təhlükəsizliyi sahəsində ən yaxşı təcrübələri 1990-cı illərdən beynəlxalq standartlar kimi qəbul etməyə başlamışlar. Məlumdur ki, ISO/IEC-2700* standartlar ailəsi və ISO-9001 standartı informasiya təhlükəsizliyinin menecmenti üçün təşkiledici standarlardır.

II. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN MENECMENT ELEMENTLƏRİ

ISO/IEC-27001 standartında populyar *“Annex A” (Əlavə-A)* informasiya təhlükəsizliyinin menecment elementi olan məqsədləri (gözləntiləri, *“objective”*) və realizasiya üsullarını (təhlükəsizlik alətlərini) müəyyən edir və onları bir neçə bölmə üzrə qruplaşdırır:

(A.5) İnformasiya təhlükəsizliyi siyasətləri – təşkilatın rəhbərliyi tərəfindən informasiya təhlükəsizliyi sahəsində siyasətin dəstəklənməsi;

(A.6) İnformasiya təhlükəsizliyinin təşkili – təşkilatda informasiya təhlükəsizliyi sisteminin iş qabiliyyətini təmin edəcək təşkilati strukturun yadradılması;

(A.7) İnsan resurslarının təhlükəsizliyi – insan səhvləri riskinin, oğurluğun və avadanlığın qeyri-düzgün istifadəsinin azaldılması (əməkdaşların təlimi və insidentlərin izlənməsi);

(A.8) Aktivlərin (resursların) idarə edilməsi – informasiya resurslarına onların dəyər dərəcələrinə görə prioritet verilməsi və onlara görə məsuluyyətin paylanması;

(A.9) Girişə nəzarət – biznes-informasiyaya girişin idarə edilməsi;

(A.10) Kriptoqrafiya – şifrləmə və açarların idarə edilməsi sahəsində idarəetmə vasitələri

(A.11) Fiziki təhlükəsizlik və ətraf mühitin təhlükəsizliyi – avtorizə olunmamış girişin və təşkilatın informasiya sisteminin işinin pozulmasının qarşısının alınması;

(A.12) Əməliyyatların təhlükəsizliyi – IT-sahənin idarə edilməsinə aid olan vasitələr: dəyişikliklərin idarə edilməsi, zərərli proqram təminatından mühafizə, ehtiyat surətlər, qeydiyyat, monitorinq, quraşdırma, boşluqlar və s.

(A.13) Kommunikasiyaların təhlükəsizliyi – şəbəkələrin və kompüterlərin təhlükəsiz fəaliyyətinin təmin edilməsi;

(A.14) Sistemin alınması, yaradılması və istismarı – təşkilatın informasiya sisteminin yaradılması və ya inkişafı zamanı informasiya təhlükəsizliyi tələblərinin

DOI: 10.25045/NCInfoSec.2017.12

yerinə yetirilməsi, tətbiqi proqramların və verilənlərin təhlükəsizliyinin dəstəklənməsi;

(A.15) Təchizatçılarla münasibətlər – təşkilatın təchizatçılara əlyetər informasiyasının təhlükəsizliyi məsələsini həll etməyə yönəlir; təchizatçılarla müqavilələrdə informasiya təhlükəsizliyinin nəzərə alınması və təchizatçıların monitorinqi

(A.16) İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi – informasiya təhlükəsizliyi hadisələri və nöqsanlar haqqında məlumatlandırma, vəzifələrin müəyyən edilməsi, insidentlərə reaksiya və sübutların toplanması prosedurları

(A.17) Fəaliyyətin fasiləsizliyinin təmin edilməsində informasiya təhlükəsizliyi aspektləri – fövqəladə hallarda təşkilatın fasiləsiz işinin təmin edilməsi üçün fəaliyyət planı;

(A.18) Qanunvericiliyin tələblərinə uyğunluq – müvafiq mülki və cinayət qanunvericiliyinin, müəllif hüquqları və informasiyanın mühafizəsi qanunları daxil olmaqla, tələblərinin yerinə yetirilməsi.

III. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN MENECMENT PROSESLƏRİ

ISO-9001 standartından başlayaraq, demək olar ki, bütün funksional fəaliyyət sahələrinin menecmentinə aid standartlarda menecment prosesləri spiralvari PDCA tsiklik modelinə *(Deming-Shewhart cycle PDCA: “Initiating, Plan – Do – Check – Act, Feedback”)* uyğun müəyyən edilir.

ISO/IEC-27001 standartına görə informasiya təhlükəsizliyinin menecment prosesləri PDCA modelinə uyğun olaraq mərhələlər üzrə müəyyən edilir, biznesin menecment mərhələrinə inteqrasiya olunur:

A. Biznesin funksional menecment modeli:

1) Planlaşdırma, qərar qəbuletmə:
- fəaliyyət imkanlarını və riskləri qiymətləndirmə;
- fəaliyyət proseslərini və fasiləsizlyini planlaşdırma, qərar qəbuletmə.

2) İcra və qeydiyyat:
- resursları formalaşdırma;
- qərarları həyata keçirmə;
- nəticələri təqdimetmə, təhvilvermə;
- proses və nəticələrin, əks-əlaqə məlumatlarının qeydiyyatı.

3) Nəzarət və təhlil:
- qeydiyyatların monitorinqi;
- fəaliyyət sisteminin, komponentlərinin auditi;
- nəticələrin, vəziyyətin analizi və dəyərləndirmə.

4) Təkmilləşdirmə, aktuallaşdırma:
- fəaliyyət planını və proseslərini təkmilləşdirmək üçün təkliflərin verilməsi;
- fəaliyyət prosedurları üçün aktuallığın təmin edilməsi.

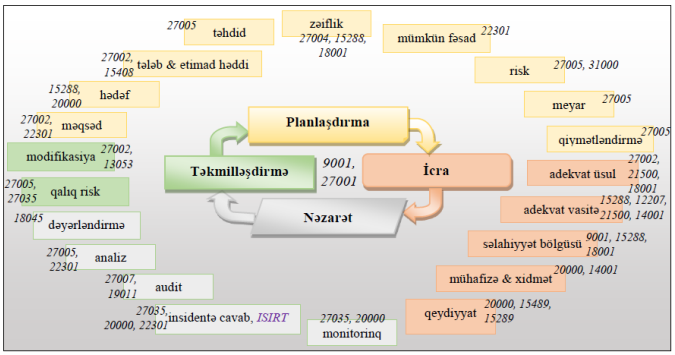
B. İnformasiya təhlükəsizliyinin menecment modeli:

1) Planlaşdırma, qərar qəbuletmə:
- İTİS üzrə fəaliyyət üçün məqsəd və vəzifələri, hədəfləri, tələbləri və etimad hədlərini, təhdidləri və zəiflikləri, riskləri və meyarları dəqiqləşdirmə, imkanları və riskləri qiymətləndirmə;
- İTİS üzrə perspektiv və cari tədbirlər planlarını hazırlama.

2) İcra və qeydiyyat:
- risklərə adekvat mühafizə üsulları və vasitələri ilə, kompetent işçi heyətlə təminat, texniki xidmət və maarifləndirmə;
- İTİS üzrə siyasət, prosedur, səlahiyyət bölgüsü və digər mühafizə üsullarını icraetmə, mühafizə hədəflərinə, risklərə, prosedurlara və vasitələrə aid reyestrləri istifadə və idarəetmə;
- informasiya təhlükəsizliyi üzrə hadisələrin müntəzəm qeydiyyatı, məlumatlandırma.

3) Nəzarət və təhlil:
- informasiya təhlükəsizliyi üzrə hadisələrin müntəzəm monitorinqi və auditi, insidentlərə cavabvermə və fəsadları ölcmə;
- uyğunsuzluqlar və səbəblərin təhlili, informasiya təhlükəsizliyi menecmentinin effektivliyini dəyərləndirmə.

4) Təkmilləşdirmə, aktuallaşdırma:
- qalıq riskləri müəyyənetmə, informasiya təhlükəsizliyi menecmentinin davamlı təkmilləşdirilməsi təshihedici və qabaqlayıcı təklif vermə (İKT-nin inkişaf intensivliyini, istifadəçilərin artan tələblərini nəzərə almaqla);
- mühafizə hədəflərinə, risklərə, prosedurlara və vasitələrə aid reyestrləri təkmilləşdirmə.



IV. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN MENECMENTİNDƏ STANDARTLARARASI ƏLAQƏLƏNDİRMƏ PROBLEMLƏRİ

A. Səbəb-nəticə asılılıqları

İnformasiya təhlükəsizliyinin menecmenti üçün əsas prinsiplərdən biri – prosesli yanaşmadır, səbəb-nəticə asılılıqlarının nəzərə alınmasıdır.

Proses – konkret məqsəd (*“objective”*) üçün lazım olan (*“input”*) aktivi (informasiyanı, dəyəri, müraciəti) təqdim olunan (*“output”*) aktivə (informasiyaya, dəyərə, xidmətə) çevirən, bir-biri ilə qarşılıqlı əlaqəsi olan fəaliyyət funksiyaları toplusudur.

B. Koordinasiya

İnformasiya təhlükəsizliyinin menecment proseslərinin sxemdə göstərilən müəyyən (çox) hissəsi üçün lazım olan (*“input”*) informasiya digər standartlarla müəyyən olunan proseslərdən təqdim edilməli olan (*“output”*) informasiyadır.

Bu səbəb-nəticə asılılıqlarının nəzərə alınması həm korporativ mühitdə və həmdə standartlaşma mühitində koordinasiya məsələsinin həll vasitəsidir.

C. Standartların harmonizasiyasına zərurət

ISO/IEC 27001 və 20000 standatlarında informasiya təhlükəsizliyinin menecmenti sistemi *(“ISMS”)* və İT-servislərin menecmenti sistemi *(“SMS”)* arasında “maraqların münaqişəsi”nə zəmin yaradan, bu sistemlərin inteqrasiyalı tətbiqinə maneə törədən kritik faktorlar aşağıdakılardır:

1) ISMS və SMS üçün müəyyən edilmiş əsas məqsədlərdəki fərqlər bu sistemlər arasında qarşılıqlı tamamlanma problemini yaradan ilkin faktordur:

- ISO/IEC-27001 informasiya təhlükəsizliyinə risklərin və insidentlərin menecmentinə imkan yaratmaq məqsədi daşıyır.
- ISO/IEC-20000 İT xidmətlərin effektif təchiz olunmasına əminliyi təmin etmək məqsədi daşıyır.

2) İnsident menecmentdə terminlərdəki uyğunsuzluq ISMS və SMS arasında sinxronizasiya problemini yaradan ilkin faktordur:

- insident – əvvəldən məlum olan və ya hələ məlum olmayan və böyük ehtimala malik riskin reallaşmasıdır;
- ISO/IEC-27001: İnformasiya təhlükəsizliyi insidenti – biznes proseslərin davamlılığını pozmaq və ya nüfuzdan salmaq və informasiya təhlükəsizliyinə təhdid yaratmaq üçün böyük ehtimala malik olan bir və ya sistematik təkrarlanan bir neçə arzuolunmaz və ya gözlənilməz informasiya təhlükəsizliyi hadisəsidir.
- Təhlükəsizlik hadisəsi – təhlükəsizlik siyasətinin pozulması və ya təhlükəsizlik alətlərinin çatışmazlığı nəticəsində yaranan vəziyyətin və ya təhlükəsizlik baxımından əvvəl məlum olmayan situasiyanın aşkar edilməsidir, ifadəsidir.

(riski müəyyənetmə → insidenti aşkarlama → bisnesə fəsadı qiymətləndirmə)

- ISO/IEC-20000: İnsident – İT-xidmətin standart istismarına aid olmayan, bu xidmətin dayanaqılığının pozulmasına və ya keyfiyyət göstəricilərinin azalmasına gətirib çıxaran və yaxud çıxara bilən hər bir hadisədir.
- İnsidentin müxtəlif dərəcələrə bölünür: insidnet, çiddi insident, problem, məlum səhv və s. Konfiqurasiya vahidinin nasazlığı da insidentdir.

(insidenti aşkarlama → problemi/səbəbi müəyyənetmə → xidmətə fəsadı qiymətləndirmə)

3) Qiymətləndirilən risklərin mahiyyətcə müxtəlif olması “ISMS” və “SMS” arasında maraqların izolyasiyası problemini yaradan ilkin faktordur:

- ISO/IEC-27001 informasiya təhlükəsizlyinə olan riskləri və onların biznes proseslər üçün təsirini müəyyən edir, biznes tərəfi bu risklərin mütləq sahibidirr;
- ISO/IEC-20000 isə yalnız “*SMS”* və İT xidmətlərə olan riskləri müəyyən edir, biznes tərəfi bu risklərin nadir hallarda sahibi olur.

ISO/IEC-27001 satndartı və ISMS üşün mühüm olan müəyyən terminlər ISO/IEC-20000 və SMS üçün kənarda qalır, istifadə olunmur:

- informasiya aktivi;
- təhdid, hücum;
- biznes davamlılığı *(“business continuity”)*;
- təhlükəsizlik meyarları və alətləri *(“control”)*;
- hadisə;
- informasiya təhlükəsizliyi hadisəsi;
- informasiya təhlükəsizliyi üzrə insident menecment;
- informasiya təhlükəsizliyi riski;
- risk menecmenti, riski qəbuletmə, risk analizi, riski qiymətləndirmə, riskin emalı və s.

V. STANDARTLARARASI ƏLAQƏLƏNDİRMƏ ÜZRƏ TƏKLİFLƏR

ISO/IEC/IEEE-15289 standartında prosesli yanaşma prinsipinə uyğun olaraq, proqram təminatı vasitələrinin (ISO/IEC-12207) və İT sistemlərin (ISO/IEC-15288) həyat tsilki proselərinə, İT xidmətlərin menecmenti (ISO/IEC-20000) proseslərinə tətbiq olunan model həmçinin ISO/IEC-27001 və digər əlaqəli menecment standartları arasında səbəb-nəticə əlaqələrinin təyin olunması üçün də tətbiq olunarsa, bu məqalədə qeyd olunan problemlərin həll olunmasına və aşağıda göstərilən nəticələrin əldə olunmasına standart zəmin yaradıla bilər:

- Menecment standartları və sistemləri arasında səbəb-nəticə asılılıqlarının dəqiqləşdirilməsi və uzlaşdırmanın təmin edilməsi;
- Koporatv mühitdə müxtəlif sahələrin menecment sistemləri üzrə səlahiyyətlər bölgüsünün və koordinasiyanın inteqrasiyası (*general koordinasiya*);
- İnformasiya təhlükəsizliyinin menecmenti standarlarının əlaqəli standartlarla harmonizasiyası;
- *“ISMS”* (ISO/IEC-27001) və *“SMS”* (ISO/IEC-20000) arasında “maraqların münaqişəsi”nin “maraqların uzlaşdırılması”na transfer məsələsinin həlli.

CƏDVƏL 1. KORPORATİV FƏALİYYƏTİN, İNFORMASİYA TƏHLÜKƏSİZLİYİNİN, İT-SİSTEMLƏRİN və İT-XİDMƏTLƏRİN MENECMENT MƏRHƏLƏLƏRİ ARASINDA UZLAŞMA

Korporativ fəaliyyətin menecment mərhələləri ISO-9001	**İnformasiya təhlükəsizliyinin menecment mərhələləri** ISO/IEC-27001	**İT-sistemlərin menecment mərhələləri** ISO/IEC-12207&15288	**İT-xidmətlərin menecment mərhələləri** ISO/IEC-20000
Korporativ fəaliyyəti planlaşdırma Qərar qəbuletmə	Korporativ fəaliyyət proseslərinin informasiya təhlükəsizliyini planlaşdırma Qərar qəbuletmə	-	-
Plan və qərarları həyata keçirmə Resurslarla təminat Qeydiyyatlar	Mühafizəni həyata keçirmə Risklərə adekvat resurslarla təminat Qeydiyyatlar	Korporativ fəaliyyətin İT üzrə tələbatını Planlaşdırma Texniki tələblər/ Layihə	
		Təchizat/ İşləyib hazırlama Quraşdırma Verifikasiya	
		Təlim Validasiya İstismara tətbiq	
		İT-xidmətlər	İT-xidmətləri planlaşdırma
			İT-xidmətləri həyata keçirmə Qeydiyyatlar
			İT-xidmət nəticə-lərinin monitorinqi Hesabat/ Dəyərləndirmə
			İT-xidmətləri davamlı təkmilləşdirmə
		İstismardan çıxarma Utilizasiya	-
Audit Analiz/ Dəyərləndirmə	Monitorinq Analiz/ Dəyərləndirmə	-	
Korporativ fəaliyyəti davamlı təkmilləşdirmə	İnformasiya təhlükəsizliyini davamlı təkmilləşdirmə		

ƏDƏBİYYAT

[1] ISO/IEC-27001:2013 “Information technology. Security techniques. İnformation security management systems. Requirements”, 2013. 23 p.

[2] ISO-9001 “Quality management systems. Requirements”, 2015. 29 p.

[3] ISO/IEC-12207 “Systems and software engineering. Software life cycle processes”, 2017, 145 p.

[4] ISO/IEC/IEEE 15288 “Systems and software engineering -- System life cycle processes”, 2015. 108 p.

[5] ISO/IEC/IEEE-15289 “Systems and software engineering. Content of life cycle information products (documentation)”, 2011.

[6] ISO/IEC-20000-1 “Information technology -- Service management -- Part 1: Service management system requirements”, 2011. 26 p.

[7] ISO/IEC-27013 “Information technology. Security techniques. Guidance on the integrated implementation of ISO/IEC-27001 and ISO/IEC-20000-1”, 2015. 39 p.

[8] COBIT 5 (“Control Objectives for Information and Related Technologies”), 2012.

MAP OF HARMONIZATION OF INFORMATION SECURITY MANAGEMENT STANDARDS WITH RELATED STANDARDS: SUGGESTIONS

Elchin A.Aliyev[1], Yadigar İmamverdiyev[2]
[1,2]Institute of Information Technology of ANAS,
Baku, Azerbaijcan,
[1]elchinaa@gmail.com, [2]yadigar@lan.ab.az

Abstract – This article sets out the problems of coordination between standards and information security management systems and management standards and systems of other related areas. For this it identifies standards and systems for managing information security and other related areas, and these control processes are classified according to the PDCA model and are studied. The paper also identifies problems of harmonization of information security management standards with relevant standards, including cause-effect relations and incompatibilities in terminology. Solutions for the transformation of "conflict of interest" into "communication of interests" are provided between ISMS (ISO / IEC-27001) and SMS (ISO / IEC-20000).

Keywords – information security; management system; management standards; PDCA model; process approach; harmonization of standards