AZƏRBAYCAN RESPUBLİKASININ DÖVLƏT STANDARTI

AZS ISO/IEC 23894:2024

Birinci nəşr
2024

İnformasiya texnologiyaları – Süni intellekt – Risklərin idarə edilməsi üzrə təlimat

Information technology – Artificial intelligence – Guidance on risk management

AZƏRBAYCAN STANDARTLAŞDIRMA İNSTİTUTU

İstinad nömrəsi
AZS ISO/IEC 23894:2024

Elçin İsaqzadə küç., 7-ci köndələn
Qaynar xətt: +994125149308
Email: office@azstand.gov.az

MÜQƏDDİMƏ

1. Bu standart Azərbaycan Elm Fondunun qrant layihəsi (Qrant №AEF-MQM-QA-1-2021-4(41)-8/03/1) çərçivəsində işlənib hazırlanıb və “İnformasiya-kommunikasiya texnologiyaları” standartlaşdırma üzrə Texniki Komitə (AZSTAND/TK 05) tərəfindən təqdim edilib.
2. Azərbaycan Standartlaşdırma İnstitutunun ..... 2024-cü il tarixli ..... saylı qərarı ilə təsdiq edilib.
3. Bu standart Beynəlxalq Standart ISO/IEC 23894 nəşr 1.0 (2023-02) ilə eynidir.
4. Dövlət standartında müəyyən edilən tələblərin beynəlxalq standartlara, norma, qayda və tövsiyələrə və digər dövlətlərin müvafiq mütərəqqi milli standartlarına, elm, texnika və texnologiyanın müasir nailiyyətlərinə əsaslanmasını müəyyən etmək üçün standartın dövri yoxlama müddəti ildə 1 dəfədir.

MÜNDƏRİCAT

ÖN SÖZ **6**
GİRİŞ **7**
1 TƏTBİQ SAHƏSİ **8**
2 NORMATİV İSTİNADLAR **8**
3 TERMİN VƏ ANLAYIŞLAR **8**
4 SÜNİ İNTELLEKT RİSKLƏRİNİN İDARƏ EDİLMƏSİ PRİNSİPLƏRİ **9**
5 RİSKLƏRİN İDARƏ EDİLMƏSİ ÇƏRÇİVƏSİ **14**
5.1. Ümumi müddəalar 14
5.2. Liderlik və öhdəçilik 15
5.3. İnteqrasiya 15
5.4. Layihələndirmə 15
5.4.1. Təşkilat və onun kontekstini başa düşmə 15
5.4.2. Risklərin idarə edilməsi öhdəliyinin ifadə edilməsi 19
5.4.3. Təşkilati rolların, səlahiyyətlərin, məsuliyyətlərin və hesabatlılığın müəyyən edilməsi 19
5.4.4. Resursların ayrılması 20
5.4.5. Kommunikasiya və məsləhətləşmə əlaqələrinin qurulması 20
5.5. İcra 20
5.6. Dəyərləndirmə 20
5.7. Təkmilləşmə 20
5.7.1. Adaptasiya 20
5.7.2. Fəsiləsiz təkmilləşmə 20
6 RİSKLƏRİN İDARƏ EDİLMƏSİ PROSESİ **20**
6.1. Ümumi müddəalar 20
6.2. Kommunikasiya və məsləhətləşmə 21
6.3. Əhatə dairəsi, kontekst və meyarlar 21
6.3.1. Ümumi müddəalar 21
6.3.2. Əhatə dairəsinin müəyyən edilməsi 21
6.3.3. Xarici və daxili kontekst 21
6.3.4. Risk meyarlarının müəyyən edilməsi 22
6.4. Risklərin qiymətləndirilməsi 23
6.4.1. Ümumi müddəalar 23
6.4.2. Risklərin identifikasiyası 24
6.4.2.1. Ümumi müddəalar 24
6.4.2.2. Aktivlər və onların dəyərlərinin identifikasiyası 24
6.4.2.3. Risk mənbələrinin identifikasiyası 24
6.4.2.4. Potensial hadisələrin və nəticələrin identifikasiyası 25
6.4.2.5. Nəzarət vasitələrinin identifikasiyası 25
6.4.2.6. Risklərin təsirinin nəticələrinin identifikasiyası 26
6.4.3. Risklərin təhlili 26
6.4.3.1. Ümumi müddəalar 27

6.4.3.2. Risklərin təsirinin nəticələrinin qiymətləndirilməsi 27
6.4.3.3. Ehtimalın qiymətləndirilməsi..... 28
6.4.4. Risklərin dəyərləndirilməsi..... 28
6.5. Risklərin aradan qaldırılması 28
6.5.1. Ümumi müddəalar 28
6.5.2. Risklərin aradan qaldırılması variantlarının seçilməsi..... 28
6.5.3. Risklərin aradan qaldırılması planlarının hazırlanması və həyata keçirilməsi 29
6.6. Monitorinq və yenidən baxış..... 29
6.7. Sənədləşdirmə və hesabatlılıq 29
Əlavə A. Məqsədlər..... 31
Əlavə B. Risk mənbələri..... 35
Əlavə C. Risklərin idarə edilməsi və Sİ sistemlərinin həyat dövrü..... 39
ƏDƏBİYYAT..... 44

ÖN SÖZ

ISO (Beynəlxalq Standartlaşdırma Təşkilatı) və IEC (Beynəlxalq Elektrotexniki Komissiya) dünya üzrə standartlaşdırma sahəsində ixtisaslaşmış sistemi formalaşdırırlar. ISO və ya IEC üzvü olan milli orqanlar texniki fəaliyyətin konkret sahələri ilə məşğul olmaq üçün müvafiq təşkilat tərəfindən yaradılmış texniki komitələr vasitəsilə beynəlxalq standartların hazırlanmasında iştirak edirlər. ISO və IEC texniki komitələri qarşılıqlı maraq doğuran sahələrdə əməkdaşlıq edirlər. ISO və IEC ilə əməkdaşlıq edən digər beynəlxalq təşkilatlar, dövlət və qeyri-hökumət təşkilatları da bu işdə iştirak edirlər.

Bu standartın hazırlanması üçün istifadə olunan və həmçinin sonrakı texniki xidmət üçün nəzərdə tutulan prosedurlar ISO/IEC Direktivlərinin 1-ci hissəsində təsvir edilmişdir. Müxtəlif növ sənədlər üçün tələb olunan fərqli təsdiq meyarlarına xüsusilə diqqət yetirilməlidir. Bu sənəd ISO/IEC Direktivlərinin 2-ci hissəsində (www.iso.org/directives və ya www.iec.ch/members_experts/refdocs) verilmiş qaydalara uyğun olaraq hazırlanmışdır.

Bu sənədin bəzi elementləri patent hüquqlarının predmeti ola bilər. ISO və IEC bu patent hüquqlarının hər hansı birinin və ya hamısının müəyyən edilməsinə görə məsuliyyət daşımır. Sənədin hazırlanması zamanı müəyyən edilmiş patent hüquqlarının təfərrüatları Girişdə və/və ya ISO və IEC təşkilatlarının qeydə alınmış patent bəyannamələrinin siyahısında (www.iso.org/patents və patents.iec.ch) təqdim olunur.

Bu standartdakı ticarət adları (“trade name”) haqqında məlumatlar istifadəçilərin rahat istifadəsi üçün təqdim olunur və bu təqdimat tövsiyə xarakteri daşımır.

Standartların könüllü xarakter daşıması, uyğunluğun qiymətləndirilməsi üzrə ISO-nun xüsusi termin və ifadələrinin mənası ilə bağlı izahlar, eləcə də Ticarətdə Texniki Maneələrin (Technical Barriers to Trade, TBT) aradan qaldırılması ilə əlaqədar ISO-nun Ümumdünya Ticarət Təşkilatının (ÜTT) prinsiplərinə sadiqliyi haqqında məlumat “www.iso.org/iso/foreword.html” internet informasiya ehtiyatından əldə edilə bilər. IEC ilə bağlı “www.iec.ch/understanding-standards” internet informasiya ehtiyatına müraciət etmək olar.

Bu sənəd ISO/IEC JTC 1 “İnformasiya texnologiyaları” Birgə Texniki Komitəsinin “SC 42, Süni intellekt” Altkomitəsi tərəfindən hazırlanmışdır.

Bu sənədlə bağlı istənilən rəy və suallar milli standartlaşdırma qurumuna yönəldilməlidir. Bu qurumların tam siyahısı ilə “www.iso.org/members.html” və “www.iec.ch/national-committees” internet informasiya ehtiyatlarında tanış olmaq olar.

GİRİŞ

Risklərin idarə edilməsinin məqsədi dəyərin yaradılması və qorunmasıdır. Bu, işin məhsuldarlığını artırır, innovasiyaları təşviq edir və qarşıya qoyulan məqsədlərə nail olmağa imkan yaradır.

Bu standart normativ əsas kimi ISO 31000:2018 “Risk management. Guidelines” (AZS ISO 31000:2022 “Risklərin idarə olunması. *Rəhbəredici göstərişlər*”) standartından istifadəni nəzərdə tutur. Bu sənəd AZS ISO 31000:2022 təlimatında verilmiş müddəaları genişləndirdikdə, AZS ISO 31000:2022 standartının bəndlərinə müvafiq istinadlar olunur və ehtiyac olduqda, süni intellekt üzrə də xüsusi təlimat verilir. Bu sənədlə AZS ISO 31000:2022 arasındakı əlaqəni daha aydın əks etdirmək üçün AZS ISO 31000:2022 standartının strukturu bu sənəddə təkrarlanır və lazım gəldikdə bənd və altbəndlər əlavə olunur.

Bu standart üç əsas hissəsi aşağıdakılardan ibarət olan bölmələrdən ibarətdir:

Bölmə 4: Prinsiplər - Bu bölmə risklərin idarə edilməsinin əsasını təşkil edən prinsipləri əks olunur. AZS ISO 31000:2022 təlimatının 4-cü bölməsində göstərildiyi kimi, süni intellektdən istifadə bu prinsiplərdən bəziləri ilə bağlı xüsusi yanaşma tələb edir.

Bölmə 5: Çərçivə - Risklərin idarə edilməsi çərçivəsinin (konsepsiyasının) məqsədi təşkilatlara risklərin idarə edilməsini onların mühüm fəaliyyət istiqamətlərinə və funksiyalarına inteqrasiya etməkdə kömək etməkdir. Süni intellekt sistemlərinin işlənməsi, tələb və təkliflərin formalaşdırılması və ya istifadəsi ilə bağlı məsələlər AZS ISO 31000:2022 təlimatının 5-ci maddəsində təsvir edilmişdir.

Bölmə 6: Proseslər - Risklərin idarə edilməsi proseslərinə siyasətlərin, prosedurların və təcrübələrin risklərlə bağlı məlumat mübadiləsi, məsləhətləşmə, tətbiq sahəsinin müəyyən olunması, həmçinin qiymətləndirmə, emal, monitorinq, təhlil, sənədləşmə və hesabatlılıq üzrə fəaliyyət istiqamətlərinə sistemli tətbiqi aiddir. Belə proseslərin süni intellektə uyğunlaşdırılması AZS ISO 31000:2022 təlimatının 6-cı maddəsində təsvir edilmişdir.

standart ilə əlaqəli ümumi məqsədlər və risk mənbələri Əlavə A və Əlavə B-də verilir. Əlavə C-də risklərin idarə edilməsi prosesləri və süni intellekt sisteminin həyat dövrü arasında uyğunluq cədvəli təqdim olunur.

AZƏRBAYCAN RESPUBLİKASININ DÖVLƏT STANDARTI

İnformasiya texnologiyaları – Süni intellekt – Risklərin idarə edilməsi üzrə təlimat

AZE ISO/IEC 23894:2024

Information technology – Artificial intelligence – Guidance on risk management

Tətbiq edilmə tarixi ... . 2024-cü il

1 TƏTBİQ SAHƏSİ

Bu standart süni intellektdən (Sİ) istifadə edən məhsulların, sistemlərin və xidmətlərin işlənməsi, istehsalı, quraşdırılması və ya istifadəsi ilə məşğul olan təşkilatların bilavasitə Sİ liə əlaqəli riskləri idarə etməsinə dair tövsiyələri ehtiva edən təlimatdır. Təlimat, həmçinin təşkilatlara Sİ liə bağlı fəaliyyət və funksiyalarına risklərin idarə edilməsini inteqrasiya etməkdə kömək etmək məqsədi daşıyır. Bu standart, o cümlədən Sİ-dən istifadə ilə bağlı yaranan risklərin idarə edilməsinin, yəni Sİ risklərinin idarə edilməsinin (“AI risk management”) effektiv tətbiqi və inteqrasiyası proseslərini təsvir edir.

Bu təlimatın tətbiqi istənilən təşkilata, onun iş mühitinə uyğunlaşdırıla bilər.

2 NORMATİV İSTİNADLAR

Aşağıdakı sənədə mətn boyu istinad onun məzmununun tam və ya qismən bu sənədin tələblərinə uyğun gəldiyi təqdirdə edilmişdir. Tarix qeyd edilmiş istinadlarda yalnız istinad olunan nəşrlər istifadə edilir. Tarix qeyd edilməmiş istinadlarda istinad olunan sənədin (düzəlişlər daxil olmaqla) sonuncu nəşri istifadə edilir.

AZE ISO/IEC 22989:2023, *İnformasiya texnologiyaları — Süni intellekt — Süni intellekt üzrə anlayışlar və terminologiya*

AZS ISO 31000:2022 *Risklərin idarə olunması. Rəhbəredici göstərişlər*

ISO Guide 73:2009, *Risk management — Vocabulary*

3 TERMİN VƏ ANLAYIŞLAR

Bu sənədin məqsədləri üçün AZS ISO 31000:2022, AZE ISO/IEC 22989:2023 və ISO Guide 73:2009 standartlarındakı terminlər və anlayışlar istifadə edilir.

ISO и IEC-in standartlaşdırma sahəsində istifadə olunan terminoloji məlumat bazaları aşağıdakı ünvanlarda saxlanılır:

— ISO Onlayn baxış platforması: https://www.iso.org/obp;

— IEC Electropedia: http://www.electropedia.org/.

4 SÜNİ İNTELLEKT RİSKLƏRİNİN İDARƏ EDİLMƏSİ PRİNSİPLƏRİ

Risklərin idarə edilməsi təşkilatın ehtiyaclarını inteqrasiya olunmuş, strukturlaşdırılmış və hərtərəfli yanaşmadan istifadə etməklə qarşılamalıdır. Rəhbər prinsiplər təşkilata öz prioritetlərini identifikasiya etməyə və qeyri-müəyyənliyin təşkilatın məqsədlərinə təsirinin idarə edilməsi barədə qərarlar qəbul etməyə imkan verir. Bu prinsiplər təşkilatın bütün səviyyələri və istər strateji, istərsə də fəaliyyətin təşkili (operational) ilə bağlı məqsədləri üçün tətbiq edilir.

Sistemlər və proseslər adətən xüsusi istifadə halları üçün müxtəlif mühitlərdə müxtəlif texnologiyalar və funksiyaların kombinasiyasından istifadə edir. Risklərin idarə edilməsi bütün texnologiyaları və funksiyaları ilə birlikdə sistemi bütövlükdə və həmçinin onun ətraf mühitə və maraqlı tərəflərə təsirini də nəzərə almalıdır.

Sİ sistemləri təşkilat üçün onun məqsədləri baxımından risklərin təsirinin müsbət və ya mənfi nəticələrinə səbəb olan yeni və ya gözlənilməz risklər yarada və ya mövcud risklərin baş vermə ehtimalını dəyişə bilər. Onlar, həmçinin təşkilat tərəfindən xüsusi yanaşmanın tətbiqini zəruri edə bilər. Bu sənəddə təşkilatın həyata keçirə biləcəyi risklərin idarə edilməsi prinsipləri, çərçivələri və prosesləri üzrə əlavə təlimatlar verilmişdir.

Qeyd: Müxtəlif Beynəlxalq Standartlarda “risk” sözünün əhəmiyyətli dərəcədə fərqli tərifləri mövcuddur. AZS ISO 31000:2022 standartında və əlaqəli Beynəlxalq Standartlarda “risk” sözü məqsədlərdən mənfi və ya müsbət sapmanı nəzərdə tutur. Bəzi digər Beynəlxalq Standartlarda “risk” sözü yalnız potensial mənfi nəticələrlə bağlı məsələləri (məsələn, təhlükəsizliklə əlaqəli problemləri) ehtiva edir. Bu fərq risklərin idarə edilməsi ilə bağlı müvafiq prosesi başa düşməyə və lazımi qaydada həyata keçirməyə çalışarkən çox vaxt çaşqınlığa səbəb ola bilər.

AZS ISO 31000:2022 standartının 4-cü bölməsi risklərin idarə edilməsi üçün bir neçə ümumi prinsip müəyyən edir. Cədvəl 1-də AZS ISO 31000:2022 standartının 4-cü bölməsindəki təlimata əlavə olaraq, zəruri hallarda bu cür prinsiplərin necə tətbiq edilməsi barədə əlavə təlimat təqdim edilir.

Cədvəl 1 — Süni intellektə tətbiq olunan risklərin idarə edilməsi prinsipləri

	Prinsiplər	Prinsipin təsviri (AZS ISO 31000:2022 standartının 4-cü bölməsinə uyğun olaraq)	Sİ-nin işlənməsi və istifadəsində prinsipin tətbiqi ilə nəzərdə tutulan məsələlər
a)	İnteqrasiyalılıq	Risklərin idarə edilməsi bütün təşkilati fəaliyyətlərin tərkib hissəsidir.	AZS ISO 31000:2022 standartından başqa digər xüsusi təlimat yoxdur.
b)	Strukturlaşdırılma və hərtərəflilik	Risklərin idarə edilməsinə dair strukturlaşdırılmış və hərtərəfli yanaşma ardıcıl və	AZS ISO 31000:2022 standartından başqa digər xüsusi təlimat yoxdur.

		müqayisə edilə bilən nəticələrin əldə edilməsini təşviq edir.	
c)	Fərdiləşdirilmə	Risklərin idarə edilməsi çərçivəsi (strukturu) və prosesi təşkilatın məqsədlərinə müvafiq olaraq onun xarici və daxili kontekstinə (iş mühitinə) uyğunlaşdırılır (fərdiləşdirilir) və tənzimlənir.	AZS ISO 31000:2022 standartından başqa digər xüsusi təlimat yoxdur.
d)	İnklüzivlik	Maraqlı tərəflərin aidiyyəti üzrə və vaxtında cəlb edilməsi onların bilik, baxış, rəy və təkliflərinin nəzərə alınmasına imkan verir. Bu, risklərin idarə edilməsi sahəsində maariflənmə və məlumatlılıq səviyyəsinin yüksəlməsi ilə nəticələnir.	Sİ maraqlı tərəflərə potensial olaraq böyük və hərtərəfli təsir göstərdiyindən, həm zərər və faydaları əlaqələndirmək, həm də risklərin idarə edilməsi prosesinə geridönüş nəticəsində rəyləri nəzərə almaq və maariflənmə proseslərini əlavə etmək üçün təşkilatların müxtəlif daxili və xarici tərəflərlə dialoq qurması vacibdir. Təşkilatlar, həmçinin Sİ sistemlərinin istifadəsinə əlavə maraqlı tərəflərin cəlb edə bilinməsi barədə məlumatlı olmalıdırlar. Maraqlı tərəflərin bilik, baxış və rəylərinin faydalı olduğu sahələrə aşağıdakılar daxildir (lakin bunlarla məhdudlaşmır): - Xüsusilə, maşın öyrənməsi (ML) çox vaxt məqsədlərinə çatmaq üçün zəruri olan verilənlər çoxluğuna əsaslanır. Maraqlı tərəflər verilənlərin toplanması, emal əməliyyatları, verilənlərin mənbəyi və növü, verilənlərin konkret situasiyalarda və ya verilənlər subyektlərinin qeyri-standart olduğu hallarda istifadəsi ilə bağlı risklərin identifikasiyasına kömək edə bilər.

			- Sİ texnologiyalarının mürəkkəbliyi Sİ sistemlərinin şəffaflığı və izahlılığı ilə bağlı çətinliklər yaradır. Verilənlər modallığının çoxsaylı növləri, Sİ model topologiyaları və hər bir maraqlı tərəfin ehtiyaclarına görə seçilməli olan şəffaflıq və hesabatlılıq mexanizmləri kimi xarakteristikalar səbəbilə Sİ texnologiyalarının müxtəlifliyi bu çətinlikləri daha da artırır. Maraqlı tərəflər hədəfləri identifikasiya etməyə və Sİ sistemlərinin şəffaflığını və izahlılığını artırmaq üçün vasitələr təsvir etməyə kömək edə bilər. Müəyyən hallarda, bu məqsədlər və vasitələr bütün istifadə halları və cəlb olunan müxtəlif maraqlı tərəflər üzrə ümumiləşdirilə bilər. Digər hallarda, şəffaflıq çərçivələri və hesabatlılıq mexanizmləri üzrə maraqlı tərəflərin seqmentasiyası hər bir istifadə halına görə müvafiq şəxslərə (məsələn, “tənzimləyicilər”, “biznes sahibləri”, “model risk qiymətləndiriciləri”) uyğunlaşdırıla bilər. - Avtomatlaşdırılmış qərarların qəbulu üçün Sİ sistemlərindən istifadə daxili və xarici maraqlı tərəflərə birbaşa təsir göstərə bilər. Bu maraqlı tərəflər, məsələn, insan nəzarətinə harada ehtiyac olacağına dair öz baxış və rəylərini təqdim edə bilərlər. Maraqlı tərəflər ədalətlilik meyarlarını təyin etməyə və həmçinin Sİ sistemlərinin işində qərəzliliyin nədən ibarət olduğunu

			identifikasiya etməyə kömək edə bilər.
e)	Dinamiklik	Risklər təşkilatın xarici və daxili konteksti dəyişdikcə yarana, dəyişə və ya yox ola bilər. Risklərin idarə edilməsi həmin dəyişiklik və hadisələri aidiyyəti üzrə və vaxtında təxmin edir, aşkar edir, təsdiqləyir və cavablayır.	AZS ISO 31000:2022 standartında verilmiş təlimatın icrası məqsədilə təşkilatlar Sİ sistemləri ilə bağlı yaranan yeni risklər, tendensiyalar, texnologiyalar, istifadələr və aktorlarla bağlı məsələləri və imkanları identifikasiya etmək üçün təşkilati strukturlar yaratmalı və tədbirlər görməlidirlər. Risklərin dinamik idarə edilməsi Sİ sistemləri üçün xüsusilə vacibdir, çünki: - Sİ sistemləri fasiləsiz öyrənmə, dəqiqləşdirmə, dəyərləndirmə və validasiya ilə məşğul olduğu üçün təbiətcə dinamikdir. Bundan əlavə, bəzi Sİ sistemləri bu dövr əsasında müstəqil olaraq dinamik dəyişikliklər formalaşdırmaqla adaptasiya olmaq və optimallaşdırmaq qabiliyyətinə malikdir. - Sİ sistemləri ilə bağlı istehlakçıların gözləntiləri yüksəkdir və potensial olaraq sistemlərin özləri kimi tez dəyişə bilərlər. - Sİ ilə bağlı hüquqi və tənzimləyici tələblər tez-tez dəyişir və yenilənirlər. Sİ ilə bağlı təşkilatlar, fərdlər və cəmiyyət üçün yarana biləcək risklərin mahiyyətini anlamaq və onları idarə etmək üçün keyfiyyətin idarə edilməsi, ətraf mühitə təsirlər (ekoloji iz), təhlükəsizlik, sağlamlıq, hüquqi və ya korporativ məsuliyyət (yaxud onların hər hansı kombinasiyası) üzrə təşkilat

			tərəfindən dəstəklənən idarəetmə sistemlərinin inteqrasiyası da nəzərdə tutula bilər.
f)	Ən keyfiyyətli əlçatan informasiya əsaslanma	Risklərin idarə edilməsi üçün giriş verilənləri keçmiş və cari informasiyaya, habelə gələcək gözləntilərə əsaslanır. Risklərin idarə edilməsi bu cür informasiya və gözləntilərlə bağlı hər hansı məhdudiyyət və qeyri-müəyyənlikləri açıq şəkildə nəzərə alır. İnformasiya müvafiq maraqlı tərəflər üçün aktual, aydın və əlçatan olmalıdır.	Fərdlərin texnologiyalarla qarşılıqlı əlaqəsi və onlara reaksiyasına Sİ-nin təsirləri ilə bağlı gözləntiləri nəzərə alaraq, Sİ sistemlərinin işlənməsi ilə məşğul olan təşkilatlara hazırladıqları Sİ sistemlərinin gələcək istifadəsi ilə bağlı müvafiq əlçatan informasiyanı izləmək tövsiyə olunur, bu müddətdə Sİ sistemlərinin istifadəçiləri Sİ sisteminin bütün həyat dövrü ərzində həmin sistemlərdən istifadənin qeydlərini saxlaya bilərlər. Sİ daim inkişaf edən yeni texnologiya olduğundan, tarixi informasiya məhdudlaşdırıla və gələcək gözləntilər sürətlə dəyişə bilər. Təşkilatlar bunu nəzərə almalıdır. Mövcud olduğu təqdirdə, Sİ sistemlərinin daxili istifadəsi də nəzərə alınmalıdır. İstehlakçılar və xarici istifadəçilər tərəfindən Sİ sistemlərinin istifadəsinin izlənməsinə əqli mülkiyyətlə, müqavilə şərtlərilə və ya bazarla bağlı xüsusi məhdudiyyət qoyula bilər. Bu cür məhdudiyyətlər Sİ risklərinin idarə edilməsi prosesində nəzərə alınmalı və biznes şəraiti onlara yenidən baxılmasını tələb etdikdə yenilənməlidir.
g)	İnsan və mədəniyyət faktorları	İnsan davranışı və mədəniyyəti risklərin idarə edilməsinin bütün aspektlərinə hər səviyyədə və mərhələdə əhəmiyyətli dərəcədə təsir göstərir.	Sİ sistemlərinin layihələndirilməsi, işlənməsi və ya tətbiqi (yaxud onların hər hansı kombinasiyası) ilə məşğul olan təşkilatlar onların əhatə olunduğu insan və mədəniyyət

			landşaftını monitorinq etməlidirlər. Təşkilatlar obyektiv nəticələr, məxfilik, ifadə azadlığı, ədalətlilik, mühafizəlilik, təhlükəsizlik, məşğulluq, ətraf mühit və insan hüquqlarına geniş şəkildə təsir göstərən və əvvəlcədən mövcud olan ictimai modellərlə (obrazlarla) Sİ sistemlərinin və ya komponentlərinin qarşılıqlı əlaqəsinin müəyyənləşdirilməsinə diqqət yetirməlidirlər.
h)	Fasiləsiz təkmilləşmə	Risklərin idarə edilməsi öyrənmə və təcrübə vasitəsilə daim təkmilləşdirilir.	Sİ sistemlərinin istifadəsi ilə bağlı əvvəllər məlum olmayan risklərin identifikasiya edilməsi fasiləsiz təkmilləşmə prosesində nəzərə alınmalıdır. Sİ sistemlərinin və ya sistem komponentlərinin layihələndirilməsi, işlənməsi və ya tətbiqi, yaxud onların hər hansı kombinasiyası ilə məşğul olan təşkilatlar performans uğurları, çatışmazlıqlar və öyrənilmiş dərslər üçün Sİ ekosisteminə nəzarət etməli və yeni Sİ tədqiqat nəticələri və texnikaları (onları təkmilləşdirmə imkanları) haqqında məlumatlı olmalıdırlar.

5 RİSKLƏRİN İDARƏ EDİLMƏSİ ÇƏRÇİVƏSİ

5.1. Ümumi müddəalar

Risklərin idarə edilməsi çərçivəsinin məqsədi risklərin idarə edilməsini əhəmiyyətli fəaliyyətlərə və funksiyalara inteqrasiya etməkdə təşkilata kömək etməkdir.

AZS ISO 31000:2022 standartının 5.1-ci bəndində verilmiş təlimat tətbiq edilir.

Risklərin idarə edilməsi qərarların qəbul edilməsi və risklərin aradan qaldırılması məqsədilə təşkilat üçün münasib informasiyaların toplanmasını əhatə edir. İdarəedici orqan ümumilikdə, riskə meyillilik amillərini (“risk appetite”) və təşkilati məqsədləri müəyyən edir, risklərin identifikasiyası, qiymətləndirilməsi və aradan qaldırılması ilə bağlı qərar qəbuletmə prosesini isə təşkilatdaxili rəhbərliyə həvalə edir.

ISO/IEC 38507 [1] standartı təşkilatlar üçün Sİ sistemlərinin işlənməsi, satın alınması və ya istifadəsi ilə bağlı əlavə idarəçilik yanaşmalarını təsvir edir. Bu cür yanaşmalara yeni imkanlar, riskə meyillilik amillərində potensial dəyişikliklər, o cümlədən təşkilat tərəfindən Sİ-dən məsuliyyətli istifadəni təmin etmək məqsədi daşıyan yeni idarəetmə siyasətləri daxildir. Onlar AZS ISO 31000:2022 standartının 5.2-ci bəndində təsvir olunan dinamik və iterativ təşkilati inteqrasiyaya kömək məqsədilə bu sənəddə təsvir olunan risklərin idarə edilməsi prosesləri ilə birlikdə istifadə edilə bilər.

5.2. Liderlik və öhdəçilik

AZS ISO 31000:2022 standartının 5.2-ci bəndində verilmiş təlimat tətbiq edilir.

AZS ISO 31000:2022 standartının 5.2-ci bəndində verilmiş təlimata əlavə olaraq, aşağıdakılar da tətbiq edilir:

Sİ-nin işlənməsi və istifadəsi ilə bağlı etimad və hesabatlılığın xüsusilə zəruri olduğunu nəzərə alaraq, yuxarı səviyyəli rəhbərlik Sİ riskləri və bu risklərin idarə edilməsi ilə bağlı siyasət və bəyanatların maraqlı tərəflərə çatdırılması məsələlərini nəzərdən keçirməlidir.

Liderlik və öhdəçiliyin bu səviyyədə nümayiş etdirilməsi Sİ-nin məsuliyyətlə işlənməsi və istifadə edilməsinə maraqlı tərəflərin etimadını təmin etmək üçün əhəmiyyətli ola bilər.

Buna görə də, təşkilat maraqlı tərəflərin Sİ-dən istifadəyə etimadını artırmaq üçün Sİ risklərinin idarə edilməsinə dair öhdəlikləri ilə bağlı bəyanatlar verməyi nəzərdən keçirməlidir.

Yuxarı səviyyəli rəhbərlik, həmçinin Sİ risklərinin idarə edilməsi üçün ehtiyac duyulan xüsusiləşdirilmiş resurslar barədə məlumatlı olmalı və bu resursları aidiyyəti üzrə paylaşaraq istifadə etməlidir.

5.3. İnteqrasiya

AZS ISO 31000:2022 standartının 5.3-cü bəndində verilmiş təlimat tətbiq edilir.

5.4. Layihələndirmə

5.4.1. Təşkilat və onun kontekstini başa düşmə

AZS ISO 31000:2022 standartının 5.4.1-ci yarımbəndində verilmiş təlimat tətbiq edilir.

Cədvəl 2-də AZS ISO 31000:2022 standartının 5.4.1-ci yarımbəndində verilmiş təlimata əlavə olaraq, təşkilatın xarici kontekstinin başa düşülməsi zamanı nəzərə alınmalı olan əlavə faktorlar sadalanır.

Cədvəl 2 — Təşkilatın xarici kontekstini formalaşdırarkən nəzərə alınan məsələlər

AZS ISO 31000:2022 standartının 5.4.1-ci yarımbəndində verilmiş ümumi təlimat	Sİ ilə məşğul olan təşkilatlar üçün əlavə təlimat

Təşkilatlar xarici kontekstlərinin ən azı aşağıdakı elementlərini nəzərə almalıdırlar:	Təşkilatlar əlavə olaraq (müstəsna hal kimi deyil), aşağıdakı elementləri nəzərə almalıdırlar:
- Beynəlxalq, milli, regional və ya yerli səviyyəli sosial, mədəni, siyasi, hüquqi, tənzimləyici, maliyyə, texnoloji, iqtisadi və ekoloji faktorlar;	- Müvafiq qanunvericilik tələbləri (konkret olaraq Sİ ilə əlaqəli tələblər də daxil olmaqla) - Sİ sistemləri və avtomatlaşdırılmış sistemlərin etik istifadəsi və işlənməsi üzrə dövlət qurumlarında yaradılmış qruplar, tənzimləyicilər, standartlaşdırma qurumları, vətəndaş cəmiyyəti, akademik dairələr və sənaye assosiasiyaları tərəfindən hazırlanan (nəşr olunan) təlimatlar. - Konkret sahə üzrə Sİ ilə əlaqəli təlimatlar və çərçivələr.
- Təşkilatın məqsədlərinə təsir edən əsas faktorlar və trendlər;	- Sİ-nin müxtəlif sahələrində texnoloji tendensiyalar və irəliləyişlər. - Sİ sistemlərinin quraşdırılmasının ictimai və siyasi nəticələri (sosial elmlərə əsaslanan tövsiyələr də daxil olmaqla).
- Xarici maraqlı tərəflərin əlaqələri, rəyləri, dəyərləri, ehtiyacları və gözləntiləri;	- Sİ sistemlərinin qeyri-şəffaflıq və ya qərəzlilik kimi problemlərinin təsiri nəticəsində maraqlı tərəflərdə yarana bilən təsəvvürlər. - Konkret Sİ əsaslı həllərin əlçatanlığı və Sİ modellərinin əlçatan olduğu vasitələrlə (məsələn, istifadəçi interfeysi, proqram təminatının işlənməsi dəsti) bağlı maraqlı tərəflərin gözləntiləri.
- Müqavilə münasibətləri və öhdəliklər;	- Sİ-dən, xüsusilə də fasiləsiz öyrənmədən istifadə edən Sİ sistemlərinin tətbiqi təşkilatın müqavilə öhdəliklərini və təminatlarını yerinə yetirmək qabiliyyətinə təsir göstərə bilər. Nəticə etibarilə, təşkilatlar müvafiq müqavilələrin əhatə dairəsini diqqətlə nəzərdən keçirməlidirlər. - Sİ sistemlərinin və xidmətlərinin layihələndirilməsi və istehsalı müddətində müqavilə münasibətlərini ifadə edir. Məsələn, üçüncü şəxslər

	tərəfindən təmin edildikdə test və təlim verilənləri üzərində mülkiyyət və istifadə hüquqları nəzərə alınmalıdır.
- Şəbəkələrin və asılılıqların mürəkkəbliyi;	- Sİ-dən istifadə şəbəkələrin və asılılıqların mürəkkəbliyini artıra bilər.
- (AZS ISO 31000:2022 standartından başqa digər təlimat).	- Sİ sistemləri mövcud sistemi əvəz edə bilər. Belə olduğu halda, Sİ sistemlərinin tətbiqi ilə bağlı təhlükəsizlik, ekoloji, sosial, texniki və maliyyə məsələləri nəzərə alnmaqla, mövcud sistemə qarşı Sİ sistemlərinin risk faydaları və risk transferlərinin qiymətləndirilməsi həyata keçirilə bilər.

Cədvəl 3-də AZS ISO 31000:2022 standartının 5.4.1-ci yarımbəndində verilmiş təlimata əlavə olaraq, təşkilatın daxili kontekstinin başa düşülməsi zamanı nəzərə alınmalı olan əlavə faktorlar sadalanır.

Cədvəl 3 — Təşkilatın daxili kontekstini formalaşdırarkən nəzərə alınmalı olan məsələlər

AZS ISO 31000:2022 standartının 5.4.1-ci yarımbəndində verilmiş ümumi təlimat Təşkilatlar xarici kontekstlərinin ən azı aşağıdakı elementlərini nəzərə almalıdırlar:	**Sİ ilə məşğul olan təşkilatlar üçün əlavə təlimat** Təşkilatlar əlavə olaraq (müstəsna hal kimi deyil), aşağıdakı elementləri nəzərə almalıdırlar:
- Baxış, missiya və dəyərlər;	- AZS ISO 31000:2022 standartından başqa digər xüsusi təlimat yoxdur.
- İdarəçilik, təşkilati struktur, rollar və hesabatlılıqlər;	- AZS ISO 31000:2022 standartından başqa digər xüsusi təlimat yoxdur.
- Strategiya, məqsədlər və siyasətlər;	- AZS ISO 31000:2022 standartından başqa digər xüsusi təlimat yoxdur.
- Təşkilat mədəniyyəti;	- məsuliyyətləri, rolları və tapşırıqları dəyişdirilməklə və yenilərini tətbiq etməklə Sİ sistemlərinin təşkilatın mədəniyyətinə göstərə biləcəyi təsir.
- Təşkilatın qəbul etdiyi standartlar, təlimatlar və modellər;	- Sİ sistemlərinin istifadəsi ilə tətbiq edilən hər hansı əlavə beynəlxalq, regional, milli və yerli səviyyəli standartlar və təlimatlar.

- Resurslar və biliklər nöqteyi-nəzərindən başa düşülən imkanlar (məsələn, kapital, vaxt, insanlar, əqli mülkiyyət, proseslər, sistemlər və texnologiyalar);	- Sİ sistemlərinin şəffaflığı və izahlılığı ilə bağlı təşkilati biliklərə əlavə risklər. - Sİ sistemlərinin istifadəsi müəyyən imkanı (bacarığı) həyata keçirmək üçün lazım olan insan resurslarının sayının dəyişməsi ilə və ya ehtiyac duyulan resursların növünün dəyişməsi ilə nəticələnə bilər (məsələn, qərarvermə prosesinin getdikcə Sİ sistemləri tərəfindən daha çox dəstəkləndiyi sahələrdə insanlarda ixtisas və ya təcrübə itkisi). - Sİ sistemlərinin işlənməsi və istifadəsi üçün tələb olunan Sİ texnologiyaları və “data” elmi üzrə xüsusi biliklər. - Sİ alətləri, platformaları və kitabxanalarının mövcudluğu texnologiyanı, onun məhdudiyyətlərini və potensial “tələləri” tam başa düşmədən Sİ sistemlərinin işlənməsinə imkan verə bilər. - Konkret Sİ sistemləri üçün əqli mülkiyyətlə bağlı məsələləri həll etmək və imkanları artırmaq üçün Sİ potensialı. Təşkilatlar hər hansı addımın atılmasını müəyyən etmək üçün bu sahədəki əqli mülkiyyətlərini və əqli mülkiyyətin şəffaflığa, təhlükəsizliyə və maraqlı tərəflərlə əməkdaşlıq qabiliyyətinə təsir göstərə biləcəyi yolları nəzərdən keçirməlidirlər.
- Verilənlər, informasiya sistemləri və informasiya axınları;	- Sİ sistemləri verilənlərin emalını avtomatlaşdırmaq, optimallaşdırmaq və təkmilləşdirmək üçün istifadə edilə bilər. - Verilənlərin istehlakçıları olaraq, Sİ sistemləri tərəfindən verilənlərə və informasiyaya keyfiyyət və tamlıqla bağlı əlavə məhdudiyyətlər tətbiq edilə bilər.
- Daxili maraqlı tərəflərlə onların rəyləri və dəyərləri nəzərə alınmaqla münasibətlər;	- Sİ sistemlərinin qeyri-şəffaflığı və ya qərəzli Sİ sistemləri kimi məsələlərin təsir göstərdiyi maraqlı tərəflərin rəyləri. - Xüsusi SI sistemlərinin işlənməsi vasitəsilə maraqlı tərəflərin daha çox

	qarşılana bilən ehtiyacları və gözləntiləri. - Sİ sistemlərinin imkanları, uğursuzluq rejimləri və uğursuzluqların idarə edilməsi ilə bağlı maraqlı tərəflərin maarifləndirilməsinə ehtiyac.
- Müqavilə münasibətləri və öhdəlikləri;	- Sİ sistemləri ilə bağlı potensial qeyri-şəffaflıq və qeyri-obyektivlik kimi müxtəlif məsələlərin təsir göstərdiyi maraqlı tərəflərin rəyləri. - Maraqlı tərəflərin konkret Sİ sistemlərindən istifadə etməklə qarşılana bilən ehtiyacları və gözləntiləri. - Sİ sistemlərinin imkanları, uğursuzluq rejimləri və uğursuzluqların idarə edilməsi ilə bağlı maraqlı tərəflərin maarifləndirilməsinə ehtiyac. - Fərdi məlumatların mühafizəsi, əsas fərdi və kollektiv hüquq və azadlıqlarla bağlı maraqlı tərəflərin gözləntiləri.
- Qarşılıqlı asılılıqlar və əlaqələr;	- Sİ sistemlərinin istifadəsi qarşılıqlı asılılıqların və əlaqələrin mürəkkəbliyini artıra bilər.

AZS ISO 31000:2022 standartının 5.4.1-ci yarımbəndində verilmiş təlimata əlavə olaraq, təşkilatlar Sİ sistemlərindən istifadənin ixtisaslaşdırılmış təlimə ehtiyacı artıra bilməsi faktını nəzərə almalıdırlar.

5.4.2. Risklərin idarə edilməsi öhdəliyinin ifadə edilməsi

AZS ISO 31000:2022 standartının 5.4.2-ci yarımbəndində verilmiş təlimat tətbiq edilir.

5.4.3. Təşkilati rolların, səlahiyyətlərin, məsuliyyətlərin və hesabatlılığın müəyyən edilməsi

AZS ISO 31000:2022 standartının 5.4.3-cü yarımbəndində verilmiş təlimat tətbiq edilir.

AZS ISO 31000:2022 standartının 5.4.3-cü yarımbəndində verilmiş təlimata əlavə olaraq, yüksək səviyyəli idarəetmə və nəzarət orqanları mümkün hallarda resurslar ayırmalı və aşağıdakı səlahiyyətlərə malik fərdləri identifikasiya etməlidir:

— Sİ risklərinin aradan qaldırılması səlahiyyəti;
— Sİ risklərinin aradan qaldırılması üçün proseslərin yaradılması və monitorinqi üzrə cavbadehlik.

5.4.4. Resursların ayrılması

AZS ISO 31000:2022 standartının 5.4.4-ci yarımbəndində verilmiş təlimat tətbiq edilir.

5.4.5. Kommunikasiya və məsləhətləşmə əlaqələrinin qurulması

AZS ISO 31000:2022 standartının 5.4.5-ci yarımbəndində verilmiş təlimat tətbiq edilir.

5.5. İcra

AZS ISO 31000:2022 standartının 5.5-ci bəndində verilmiş təlimat tətbiq edilir.

5.6. Dəyərləndirmə

AZS ISO 31000:2022 standartının 5.6-cı bəndində verilmiş təlimat tətbiq edilir.

5.7. Təkmilləşmə

5.7.1. Adaptasiya

AZS ISO 31000:2022 standartının 5.7.1-ci yarımbəndində verilmiş təlimat tətbiq edilir.

5.7.2. Fəsiləsiz təkmilləşmə

AZS ISO 31000:2022 standartının 5.7.2-ci yarımbəndində verilmiş təlimat tətbiq edilir.

6 RİSKLƏRİN İDARƏ EDİLMƏSİ PROSESİ

6.1. Ümumi müddəalar

AZS ISO 31000:2022 standartının 6.1-ci bəndində verilmiş təlimat tətbiq edilir.

Təşkilatlar üzləşdikləri Sİ risklərini identifikasiya etmək, qiymətləndirmək və başa düşmək üçün riskə əsaslanan yanaşma tətbiq etməli və risk səviyyəsinə uyğun olaraq onu aradan qaldırmaq üçün müvafiq tədbirlər görməlidirlər. Təşkilatın ümumi Sİ risklərinin idarə edilməsi prosesinin uğuru strateji, fəaliyyətin təşkili (operational), proqram və layihələndirmə səviyyələrində mövcud olan risklərin idarə edilməsinin dar ixtisaslaşdırılmış proseslərinin identifikasiya edilməsi, yaradılması və uğurla həyata keçirilməsinə əsaslanır. Bəzi Sİ əsaslı texnologiyaların potensial mürəkkəbliyi, qeyri-şəffaflığı və gözlənilməzliyi ilə bağlı (lakin bununla məhdudlaşmayan) çətinliklər səbəbindən, Sİ sistemlərinin layihələndirmə səviyyəsində mövcud olan risklərin idarə edilməsi proseslərinə xüsusi diqqət yetirilməlidir. Bu cür layihələndirmə səviyyəli sistem prosesləri təşkilatın məqsədlərinə uyğunlaşdırılmalı və risklərin idarə edilməsinin digər səviyyələrinə informasiya ötürməli və qəbul etməlidir. Məsələn, Sİ sistemlərinin layihələndirmə səviyyəsində əldə olunmuş təcrübə və biliklər daha yüksək səviyyələrdə, məsələn, strateji, fəaliyyətin təşkili, proqram və digər müvafiq səviyyələrdə nəzərə alınmalıdır.

Layihələndirmə səviyyəsində risklərin idarə edilməsi prosesinin əhatə dairəsi, konteksti və meyarları layihələndirmə çərçivəsindəki Sİ sistemlərinin həyat dövrü mərhələlərindən birbaşa asılıdır. Əlavə C-də layihələndirmə səviyyəsində mövcud olan risklərin idarə edilməsi prosesi ilə Sİ sistemlərinin həyat dövrü arasındakı mümkün əlaqələr təsvir olunur (ISO/IEC 22989:2022-də müəyyən edildiyi kimi).

6.2. Kommunikasiya və məsləhətləşmə

AZS ISO 31000:2022 standartının 6.2-ci bəndində verilmiş təlimat tətbiq edilir.

Sİ sistemlərinin təsir göstərdiyi maraqlı tərəflər əhatəsi ilkin olaraq nəzərdə tutulduğundan daha geniş ola bilər, nəzərə alınmamış digər maraqlı tərəfləri əhatə edə və cəmiyyətin digər hissələrinə də yayıla bilər.

6.3. Əhatə dairəsi, kontekst və meyarlar

6.3.1. Ümumi müddəalar

AZS ISO 31000:2022 standartının 6.3.1-ci yarımbəndində verilmiş təlimat tətbiq edilir.

AZS ISO 31000:2022 standartının 6.3.1-ci yarımbəndində verilmiş təlimata əlavə olaraq, Sİ-dən istifadə edən təşkilatlar üçün Sİ risklərinin idarə edilməsinin əhatə dairəsi, Sİ risklərinin idarə edilməsi prosesinin konteksti və qərarların qəbulu proseslərinin dəstəklənməsi məqsədilə riskin əhəmiyyətinin dəyərləndirilməsi meyarları genişləndirilməlidir. Bu, təşkilatda Sİ sistemlərinin harada işlənildiyini və ya istifadə olunduğunu identifikasiya etmək üçün zəruridir. Sİ-nin işlənməsi və istifadəsi ilə bağlı bu cür siyahı sənədləşdirilməli və təşkilatın risklərin idarə edilməsi prosesinə daxil edilməlidir.

6.3.2. Əhatə dairəsinin müəyyən edilməsi

AZS ISO 31000:2022 standartının 6.3.2-ci yarımbəndində verilmiş təlimat tətbiq edilir.

Əhatə dairəsi təşkilatın müxtəlif səviyyələrinin xüsusi tapşırıq və məsuliyyətlərini nəzərə almalıdır. Bundan əlavə, təşkilat tərəfindən işlənən və ya istifadə olunan Sİ sistemlərinin məqsəd və hədəfləri də nəzərə alınmalıdır.

6.3.3. Xarici və daxili kontekst

AZS ISO 31000:2022 standartının 6.3.3-cü yarımbəndində verilmiş təlimat tətbiq edilir.

Sİ sistemlərinin potensial təsirlərinin maqnitudasına görə, təşkilatlar risklərin idarə edilməsi prosesinin kontekstini formalaşdırarkən və yaradarkən öz maraqlı tərəflərinin mühitinə xüsusi diqqət yetirməlidirlər.

Təşkilatlar aşağıdakılar daxil olmaqla (lakin bunlarla məhdudlaşmır), maraqlı tərəflərin siyahısını nəzərdən keçirməyə diqqət yetirilməlidir:

— təşkilat (özü);
— istehlakçılar, tərəfdaşlar və üçüncü tərəflər;
— təchizatçılar;

— son istifadəçilər;
— tənzimləyicilər;
— vətəndaş cəmiyyətləri (QHT, ictimai təşkilatlar, peşəkar assosiasiyalar, fondlar və s.);
— fiziki şəxslər;
— təsir dairəsində olan yerli icmalar;
— cəmiyyətin müəyyən qrupları.

Xarici və daxili kontekst üçün bəzi digər yanaşmalar aşağıdakılardır:

— Sİ sistemlərinin insanlara zərər verə bilməsi, zəruri xidmətlərdən (təmin edilmədiyi təqdirdə, həyat, sağlamlıq və ya şəxsi təhlükəsizlik üçün təhlükə yarana biləcək xidmətlərdən) imtina edə bilməsi, insan hüquqlarını poza bilməsi (məsələn, qeyri-obyektiv və qərəzli avtomatlaşdırılmış qərarlar qəbul etməsi) və ya ətraf mühitə zərər verə bilməsi ilə bağlı ehtimallar;
— təşkilatın sosial məsuliyyətinə dair xarici və daxili gözləntilər;
— təşkilatın ətraf mühitlə bağlı məsuliyyətinə dair xarici və daxili gözləntilər.

ISO 26000:2010 [2] standartında verilmiş sosial məsuliyyətin aspektlərini əks etdirən təlimatlar riskin başa düşülməsi və aradan qaldırılması üçün çərçivə (xüsusilə, təşkilati idarəetmə, insan hüquqları, əmək təcrübələri, ətraf mühit, ədalətli iş təcrübələri, istehlakçılarla bağlı məsələləri və cəmiyyətin iştirakı və inkişafı kimi mövzuları əhatə etməklə) kimi tətbiq edilməlidir.

Qeyd: Etimadı doğrultma xüsusiyyəti barədə əlavə məlumat ISO/IEC TR 24028:2020 [3] standartında verilmişdir.

6.3.4. Risk meyarlarının müəyyən edilməsi

AZS ISO 31000:2022 standartının 6.3.4-cü yarımbəndində verilmiş təlimat tətbiq edilir.

Cədvəl 4-də AZS ISO 31000:2022 standartının 6.3.4-cü yarımbəndində verilmiş təlimata əlavə olaraq, risk meyarlarını müəyyən edərkən nəzərə alınmalı olan faktorlara dair əlavə təlimat təqdim edilir:

Cədvəl 4 — Risk meyarlarının müəyyən edilməsi zamanı əlavə təlimat

AZS ISO 31000:2022 standartının 6.3.4-cü yarımbəndində verilmiş risk meyarlarının müəyyən edilməsi üzrə təlimat	Sİ sistemlərinin işlənməsi və istifadəsi kontekstində əlavə təlimat
- Nəticələrə və məqsədlərə təsir edə biləcək qeyri-müəyyənliklərin tipi (həm maddi, həm də qeyri-maddi) və növü;	- Təşkilatlar istifadə olunan verilənlər, proqram təminatı, riyazi modellər, fiziki genişlənmə və “insan-dövrdə” (verilənlərin toplanması və nişanlanması zamanı hər hansı insan fəaliyyəti) aspektləri daxil olmaqla, Sİ sistemlərinin bütün hissələrində qeyri-
- Risklərin təsirinin nəticələrinin (həm müsbət, həm də mənfi) və onların	

ehtimalının müəyyən edilməsi və ölçülməsi üsulu;	müəyyənliyi başa düşmək üçün ağlabatan addımlar atmalıdır.
- Zamanla əlaqəli faktorlar;	- AZS ISO 31000:2022 standartından başqa digər xüsusi təlimat yoxdur.
- Ölçmələrin istifadəsində mütəmadilik;	- Təşkilatlar Sİ-nin sürətlə inkişaf edən texnologiya sahəsi olduğunu nəzərə almalıdırlar. Sİ sistemlərinin istifadəsi üçün ölçmə metodlarının effektivliyi və yararlılığı baxımından onlar mütəmadi olaraq qiymətləndirilməlidir.
- Risk səviyyəsinin müəyyən edilməsi;	- Təşkilatlar risk səviyyəsini müəyyən etmək üçün ardıcıl yanaşma formalaşdırmalıdırlar. Bu yanaşma Sİ ilə bağlı müxtəlif məqsədlərə Sİ sistemlərinin potensial təsirini əks etdirməlidir (bax: Əlavə A).
- Çoxsaylı risk kombinasiyalarının və ardıcıllığının nəzərə alınması;	- AZS ISO 31000:2022 standartından başqa digər xüsusi təlimat yoxdur.
- Təşkilatın potensialı	- Sİ ilə bağlı risklərə meyillilik amilləri (“risk iştahı”) müəyyən olunarkən təşkilatın Sİ potensialı (imkanları), bilik səviyyəsi və reallaşan Sİ risklərini aradan qaldırma qabiliyyəti nəzərə alınmalıdır.

6.4. Risklərin qiymətləndirilməsi

6.4.1. Ümumi müddəalar

AZS ISO 31000:2022 standartının 6.4.1-ci yarımbəndində verilmiş təlimat tətbiq edilir.

Sİ riskləri identifikasiya edilməli, kəmiyyətcə və ya keyfiyyətcə təsvir edilməli və təşkilatın məqsədlərinə və risk meyarlarına əsasən prioritetləşdirilməlidir. Əlavə B-də Sİ ilə əlaqəli risk mənbələrinin kataloqunun nümunəsi təqdim edilir. Bu cür kataloq nümunəsi müfəssəl hesab edilə bilməz. Bununla belə, təcrübə göstərir ki, ilk dəfə risklərin qiymətləndirilməsini yerinə yetirən və ya Sİ risklərinin idarə edilməsini mövcud idarəetmə strukturlarına inteqrasiya edən hər hansı təşkilat üçün əsas kimi belə bir kataloqdan istifadə faydalıdır. Kataloq bu təşkilatlar üçün sənədləşdirilmiş əsas kimi çıxış edir.

Buna görə də, Sİ sistemlərinin işlənməsi, tətbiqi və ya onlarla təminat sahəsində fəaliyyət göstərən təşkilatlar risklərin qiymətləndirilməsi üzrə fəaliyyətlərini sistemin həyat dövrü ilə

uzlaşdırmalıdırlar. Sistemin həyat dövrünün müxtəlif mərhələlərində risklərin qiymətləndirilməsi üzrə fərqli metodlar tətbiq oluna bilər.

6.4.2. Risklərin identifikasiyası

6.4.2.1. Ümumi müddəalar

AZS ISO 31000:2022 standartının 6.4.2-ci yarımbəndində verilmiş təlimat tətbiq edilir.

6.4.2.2. Aktivlər və onların dəyərlərinin identifikasiyası

Təşkilatlar 6.3.2-ci yarımbənddə müəyyən edilmiş risklərin idarə edilməsi prosesinin əhatə dairəsinə daxil olan Sİ işlənməsi və istifadəsi ilə bağlı aktivləri identifikasiya etməlidir. Sözügedən əhatə dairəsinə daxil olan aktivlərin, onların nisbi kritikliyinin və ya dəyərinin müəyyənləşdirilməsi həmin aktivlərin bu prosesə təsirinin qiymətləndirilməsinin ayrılmaz tərkib hissəsidir. Bu zaman həm aktivlərin dəyəri, həm də tipi (maddi və ya qeyri-maddi) nəzərə alınmalıdır. Əlavə olaraq, Sİ-nin işlənməsi və istifadəsi ilə əlaqəli aktivlər aşağıdakı elementlər kontekstində nəzərdən keçirilməlidir (lakin bununla məhdudlaşmır):

— Aktivlər və onların təşkilatlar üçün dəyəri:

- Maddi aktivlər verilənlər, modellər və Sİ sistemlərini ehtiva edə bilər;
- Qeyri-maddi aktivlərə reputasiya və etimad daxil ola bilər.

— Aktivlər və onların fiziki şəxslər üçün dəyəri:

- Maddi aktivlər fiziki şəxsin fərdi məlumatlarını ehtiva edə bilər;
- Qeyri-maddi aktivlərə fiziki şəxsin sağlamlığı, təhlükəsizliyi və şəxsi həyatının toxunulmazlığı daxil ola bilər.

— Aktivlər və onların birlik və cəmiyyətlər üçün dəyəri:

- Maddi aktivlər ətraf mühiti ehtiva edə bilər;
- Qeyri-maddi aktivlər daha çox sosial-mədəni əqidələr, ictimaiyyətin əldə etdiyi biliklər, təhsilin əlçatanlığı və bərabərlik kimi dəyərlərə əsaslanır.

Aktivlər və onların təsirlərlə əlaqəsinin dəyərləndirilməsi üçün 6.4.2.6-cı və 6.4.3.2-ci yarımbəndlərə baxın.

Qeyd: Bu bölmədə “aktiv” sözünün illüstrativ nümunələrlə istifadə edilməsi heç bir hüquqi nəticələrə səbəb olmur.

6.4.2.3. Risk mənbələrinin identifikasiyası

Təşkilatlar müəyyən edilmiş əhatə dairəsi daxilində Sİ-nin işlənməsi və ya istifadəsi (yaxud hər ikisi) ilə bağlı risk mənbələrinin siyahısını identifikasiya etməlidir. Risk mənbələri aşağıdakı sahələr üzrə identifikasiya edilə bilər (lakin bunlarla məhdudlaşmır):

— təşkilatlar;
— proseslər və prosedurlar;

— idarəetmə rejimləri;
— heyət;
— fiziki mühit;
— verilənlər;
— Sİ sistemlərinin konfiqurasiyası;
— quraşdırılma mühiti;
— aparat (texniki təminat) və proqram təminatı, şəbəkə resursları və xidmətləri;
— xarici tərəflərdən asılılıq.

Sİ ilə bağlı risk mənbələrinə dair nümunələr Əlavə B-də göstərilmişdir.

6.4.2.4. Potensial hadisələrin və nəticələrin identifikasiyası

Təşkilatlar Sİ-nin işlənməsi və ya istifadəsi ilə bağlı və müxtəlif maddi və ya qeyri-maddi nəticələrə səbəb ola biləcək potensial hadisələri identifikasiya etməlidir.

Hadisələr aşağıdakı metod və mənbələrdən biri və ya bir neçəsinin köməyilə identifikasiya edilə bilər:

— nəşr edilmiş standartlar;
— nəşr edilmiş texniki spesifikasiyalar;
— nəşr edilmiş texniki hesabatlar;
— nəşr edilmiş elmi məqalələr;
— istifadədə olan oxşar sistemlər və ya tətbiqlər üzrə bazar verilənləri (“market data”);
— istifadədə olan oxşar sistemlər və ya tətbiqlər üzrə baş verən insidentlər barədə hesabatlar;
— istismar (sahə) sınaqları;
— istifadəyə yararlılıq tədqiqatları;
— müvafiq araşdırmaların nəticələri;
— maraqlı tərəflərin hesabatları;
— daxili və ya xarici ekspertlərlə müsahibələr və onların hesabatları;
— imitasiya modelləşdirməsi.

6.4.2.5. Nəzarət vasitələrinin identifikasiyası

Təşkilatlar Sİ-nin işlənməsi və ya istifadəsi (yaxud hər ikisi) ilə bağlı nəzarət vasitələrini identifikasiya etməlidir.

Nəzarət vasitələri risklərin idarə edilməsi fəaliyyətləri zamanı identifikasiya edilməli və sənədləşdirilməlidir (daxili sistemlərdə, prosedurlarda, audit hesabatlarında və s.).

Risk mənbələrini, hadisələrini və risklərin təsirinin nəticələrini “yumşaltmaqla” (aradan qaldırmaqla), nəzarət vasitələrindən ümumi riskə müsbət təsir göstərmək üçün də istifadə edilə bilər.

İdentifikasiya edilmiş nəzarət vasitələrinin effektivliyi, xüsusilə də bu vasitələrdəki nasazlıqlar nəzərə alınmalıdır.

6.4.2.6. Risklərin təsirinin nəticələrinin identifikasiyası

Təşkilatlar Sİ risklərinin qiymətləndirilməsinin bir hissəsi kimi risklərə səbəb ola biləcək risk mənbələrini, hadisələrini və ya risklərin təsirinin nəticələrini identifikasiya etməlidir. Onlar, həmçinin təşkilatın özü, fərdlər, birliklər, qruplar və cəmiyyətin məruz qalacağı bütün nəticələri də identifikasiya etməlidir. Təşkilatlar texnologiyaların üstünlüklərindən faydalanan qruplarla risklərin təsirinin mənfi nəticələri ilə qarşılaşan qruplar arasındakı fərqləri müəyyən etməyə xüsusi diqqət yetirməlidir.

Fərdlərə və cəmiyyətlərə münasibətdə təşkilatlar üçün risklərin təsirinin nəticələri zəruri dərəcədə bir-birindən fərqlənir.

Təşkilatlar üçün risklərin təsirinin nəticələrinə aşağıdakılar daxil ola bilər (lakin bunlarla məhdudlaşmır):

— araşdırma və bərpa vaxtı;
— qazanılmış və itirilmiş iş vaxtı;
— qazanılmış və ya itirilmiş imkanlar;
— fərdlərin sağlamlığına və ya təhlükəsizliyinə qarşı təhdidlər;
— zərərin aradan qaldırılması üzrə xüsusi bacarıqlara dair maliyyə xərcləri;
— işçilərin cəlb edilməsi, məmnuniyyəti və işdən ayrılmaması üçün şəraitin yaradılması;
— imic, reputasiya və xoşməramlılıq;
— cərimələr və cəzalar;
— istehlakçı çəkişmələri.

Kontekstdən, mühitdən asılı olaraq, fərdlər və cəmiyyət üçün risklərin təsirinin nəticələri daha ümumi ola bilər. Bu halda təşkilatlar hər bir fərd və ya cəmiyyət üçün ayrılıqda təsirləri dəqiq qiymətləndirməyə bilər.

Hər bir təsir növünü müəyyənləşdirmək əvəzinə, təsirlərin (məsələn, fərdlər üçün şəxsi həyatın toxunulmazlığına, ədalətliliyə, insan hüquqlarına və s., cəmiyyət üçün isə ətraf mühitə təsir) kritiklik dərəcəsi əsas element hesab olunduğundan, onlara ümumilikdə baxıla bilər.

Konkret nəticələr təşkilatın fəaliyyət göstərdiyi kontekstdən və Sİ sistemlərinin işləndiyi və istifadə olunduğu sahələrdən asılı ola bilər.

Qeyd 1: Risklərin təsirinin nəticələri müsbət və ya mənfi ola bilər. Təşkilatlar həm təşkilat, həm fərdlər, həm də cəmiyyət üçün risklərin təsirinin nəticələrini qiymətləndirərkən hər iki halı nəzərə ala bilər.

Qeyd 2: Fərdlər və cəmiyyət üçün risklərin təsirinin nəticələri adətən təşkilat üçün də eyni nəticələrə səbəb ola bilər. Məsələn, təşkilatın məhsulunun istifadəçisi ilə bağlı baş vermiş təhlükəsizlik insidenti təşkilata qarşı məsuliyyət iddiaları ilə nəticələnə, onun reputasiyasına və məhsul satışına mənfi təsir göstərə bilər.

6.4.3. Risklərin təhlili

6.4.3.1. Ümumi müddəalar

AZS ISO 31000:2022 standartının 6.4.3-cü yarımbəndində verilmiş təlimat tətbiq edilir.

Təhlil yanaşması kontekstin yaradılmasının bir hissəsi kimi işlənmiş risk meyarlarına uyğunlaşdırılmalıdır (6.3-cü bənd).

6.4.3.2. Risklərin təsirinin nəticələrinin qiymətləndirilməsi

Risklərin qiymətləndirilməsi zamanı əldə edilmiş nəticələri qiymətləndirərkən təşkilat biznesə təsirin qiymətləndirilməsi, fərdlərə təsirin qiymətləndirilməsi və cəmiyyətə təsirin qiymətləndirilməsi arasında fərq qoymalıdır.

Biznesə təsirin təhlili təşkilata göstərilən təsirin dərəcəsini müəyyən etməli və aşağıdakı elementlər nəzərə alınmalıdır (lakin bununla məhdudlaşmır):

— təsirin kritiklik dərəcəsi;
— maddi və qeyri-maddi təsirlər;
— ümumi təsirin müəyyən edilməsi üçün istifadə olunan meyarlar (6.3.4-cü yarımbənddə təyin edildiyi kimi).

Fərdlərə olan təsirin təhlili təşkilat tərəfindən Sİ-nin işlənməsi və ya istifadəsi (və ya hər ikisi) ilə bağlı fərdlərə göstərilən təsirin dərəcəsini müəyyən etməli və aşağıdakı elementlər (lakin bunlarla məhdudlaşmır) nəzərə alınmalıdır:

— istifadə edilən fərdi məlumatların növləri;
— Sİ-nin işlənməsi və ya istifadəsinin nəzərdə tutulan təsiri;
— qərəzliliyin fərdə potensial təsiri;
— fərd üçün maddi və qeyri-maddi zərərlə nəticələnə biləcək əsas hüquqların həyata keçirilməsinə potensial təsir;
— ədalətliliyin fərdə potensial təsiri;
— fərdin təhlükəsizliyi;
— arzuolunmaz qərəzlilik və ədalətsizliyin nəticələrinin azaldılması və onlardan qorunma vasitələri;
— fərdin hüquqi və mədəni mühiti (nisbi təsirin necə müəyyənləşməsinə təsir göstərə bilər)

Cəmiyyətə təsirin təhlili təşkilat tərəfindən Sİ-nin işlənməsi və ya istifadəsi (və ya hər ikisi) ilə bağlı cəmiyyətə göstərilən təsirin dərəcəsini müəyyən etməli və aşağıdakı elementlər nəzərə alınmalıdır (lakin bunlarla məhdudlaşmır):

— İctimai təsir dairəsi (Sİ sistemlərinin müxtəlif əhali qrupları üçün əhatə dairəsinin genişliyi), o cümlədən sistemdən kimlərin istifadə etdiyi və ya onun kimlər üçün nəzərdə tutulduğu (məsələn, özəl istifadədən daha çox hökumət tərəfindən istifadə cəmiyyətə potensial təsir göstərə bilər);
— Təsir dairəsində olan müxtəlif qruplar tərəfindən qorunan sosial və mədəni dəyərlərə Sİ sistemlərinin təsiri (Sİ sistemlərinin müxtəlif sosial qruplar üçün əvvəlcədən mövcud olan

zərər modelinin (nümunələrinin) gücləndirildiyi və ya məhdudlaşdırıldığı xüsusi üsullar daxil olmaqla).

6.4.3.3. Ehtimalın qiymətləndirilməsi

Mümkün hallarda, təşkilatlar risklərə səbəb olan hadisələrin baş vermə ehtimalını və nəticələrini qiymətləndirməlidir. Ehtimal keyfiyyət və ya kəmiyyət şkalası üzrə müəyyən edilə bilər və 6.3.4-cü yarımbəndə formalaşdırılmış meyarlara uyğun olmalıdır. Ehtimal aşağıdakılar (lakin bunlarla məhdudlaşmır) əsasında müəyyən edilə və onlardan asılı ola bilər:

— risk mənbələrinin növləri, əhəmiyyəti və sayı;
— təhdidlərin tezliyi, ciddiliyi və yayılma dərəcəsi;
— təşkilatın siyasət və prosedurlarının effektivliyi və daxili aktorların motivasiyası kimi daxili faktorlar;
— coğrafi və digər sosial, iqtisadi və ekoloji problemlər kimi xarici faktorlar;
— nəzarət vasitələrinin effektivliyi (“yumşaldılma” imkanı) və ya uğursuzluğu (6.4.2.5-ci yarımbənd).

Təşkilatlar ehtimal hesablamalarını yalnız onların risklərin aradan qaldırılması metodlarının əhatə dairəsinin müəyyən edilməsində tətbiq oluna bildiyi və faydalı olduğu hallarda aparmalıdır. Xüsusilə, ehtimalın hesablana bilmədiyi və ya hesablamanın böyük xətaya malik olduğu hallarda qərar qəbuletmə əsaslı ehtimallarla bağlı əhəmiyyətli texniki, iqtisadi və evristik problemlər yarana bilər.

6.4.4. Risklərin dəyərləndirilməsi

AZS ISO 31000:2022 standartının 6.4.4-cü yarımbəndində verilmiş təlimat tətbiq edilir.

6.5. Risklərin aradan qaldırılması

6.5.1. Ümumi müddəalar

AZS ISO 31000:2022 standartının 6.5.1-ci yarımbəndində verilmiş təlimat tətbiq edilir.

6.5.2. Risklərin aradan qaldırılması variantlarının seçilməsi

AZS ISO 31000:2022 standartının 6.5.2-ci yarımbəndində verilmiş təlimat tətbiq edilir.

Təşkilat tərəfindən müəyyən edilmiş risklərin aradan qaldırılması variantları risklərin təsirinin mənfi nəticələrini məqbul səviyyəyə endirmək və müsbət nəticələrə nail olmaq ehtimalını artırmaq üçün layihələndirilməlidir. Müxtəlif variantları tətbiq etməklə mənfi nəticələrin lazımi dərəcədə azaldılmasına nail olmaq mümkün olmadıqda, təşkilatlar qalıq risklər üçün risk-fayda təhlili aparmalıdır.

AZS ISO 31000:2022 standartının 6.5.2-ci yarımbəndinə uyğun olaraq, təşkilatlar aşağıdakıları nəzərə almalıdır:

— risklərin artmasına səbəb olan fəaliyyətə başlamamaq və ya davam etdirməmək qərarına gəlməklə risklərdən qaçmaq;
— fürsət əldə etmək üçün risk almaq və ya riskləri artırmaq;
— risklərin mənbəyini aradan qaldırmaq;
— ehtimalı dəyişdirmək;
— risklərin təsir nəticələrini dəyişdirmək;
— riskləri paylaşmaq (məsələn, müqavilələr və ya sığorta əldə etmək yolu ilə);
— əsaslandırılmış qərar qəbul etməklə riskləri “saxlamaq” (retain).

6.5.3. Risklərin aradan qaldırılması planlarının hazırlanması və həyata keçirilməsi

AZS ISO 31000:2022 standartının 6.5.3-cü yarımbəndində verilmiş təlimat tətbiq edilir.

Risklərin aradan qaldırılması planları sənədləşdirildikdən sonra 6.5.2-ci yarımbənddə göstərilən risklərin aradan qaldırılması üzrə seçilmiş tədbirlər həyata keçirilməlidir.

Risklərin aradan qaldırılması üzrə hər bir tədbirin həyata keçirilməsi və onların effektivliyi 6.7-ci bəndə uyğun olaraq verifikasiya edilməli və qeydə alınmalıdır.

6.6. Monitorinq və yenidən baxış

AZS ISO 31000:2022 standartının 6.6-cı bəndində verilmiş təlimat tətbiq edilir.

6.7. Sənədləşdirmə və hesabatlılıq

AZS ISO 31000:2022 standartının 6.7-ci bəndində verilmiş təlimat tətbiq edilir.

Təşkilatlar tətbiq və tətbiqdən sonrakı mərhələlərdə məhsullar və ya xidmətlər barədə məlumatların toplanması və verifikasiyası üçün sistem yaratmalı, qeydə almalı və dəstəkləməlidir. Təşkilatlar, həmçinin bazarda oxşar sistemlər haqqında ictimaiyyət üçün əlçatan olan məlumatları toplamalı və nəzərdən keçirməlidir.

Daha sonra həmin məlumatların Sİ sistemlərinin etimadı doğrultma xüsusiyyətinə uyğunluğunun mümkünlüyünün müəyyən edilməsi məqsədilə qiymətləndirilmə aparılmalıdır. Xüsusilə, bu qiymətləndirmə əvvəllər aşkar edilməmiş risklərin mövcudluğu və ya əvvəllər qiymətləndirilmiş risklərin artıq məqbul olub-olmadığını müəyyən etməlidir. Bu məlumatlar təşkilatın Sİ risklərinin idarə edilməsi prosesinə məqsədlərin, istifadə hallarının tənzimlənməsi və ya təcrübədə əldə edilmiş dərslərin uyğunlaşdırılması kimi daxil edilə və nəzərə alına bilər.

Bu şərtlərdən hər hansı biri tətbiq olunarsa, təşkilatlar aşağıdakıları yerinə yetirməlidir:

— risklərin idarə edilməsi üzrə əvvəlki fəaliyyətə təsirin qiymətləndirilməsi və bu qiymətləndirmənin nəticələrinin risklərin idarə edilməsi prosesinə daxil edilməsi.
— Sİ sistemləri üzrə risklərin idarə edilməsi fəaliyyətinin yenidən nəzərdən keçirilməsi. Əgər qalıq risklərin və ya onların məqbulluğunun dəyişməsi ehtimalı varsa, əvvəlki risklərə nəzarət tədbirlərinə təsirlər dəyərləndirilməlidir.

Qiymətləndirmənin nəticələri qeydə alınaraq sənədləşdirilməlidir. Risklərin idarə edilməsi qeydləri risklərin idarə edilməsi prosesləri boyu identifikasiya edilmiş hər bir riskin

izlənməsinə imkan verməlidir. Sənədləşmə (qeydlər) təşkilatlar tərəfindən razılaşdırılan ümumi şablon əsasında tərtib edilə bilər.

Əhatə dairəsi, kontekst və meyarlar (6.3-cü bənd), risklərin qiymətləndirilməsi (6.4-cü bənd) və risklərin aradan qaldırılması (6.5-ci bənd) ilə bağlı sənədləşdirməyə əlavə olaraq, qeydlər ən azı aşağıdakı məlumatları da əhatə etməlidir:

— təhlil edilmiş sistemin təsviri və identifikasiyası;
— tətbiq edilmiş metodologiya;
— Sİ sistemlərinin nəzərdə tutulan istifadəsinin təsviri;
— risklərin qiymətləndirilməsini həyata keçirmiş şəxs(lər)in və təşkilatların identifikasiyası;
— risklərin qiymətləndirilməsinin texniki tapşırığı və tarixi;
— risklərin qiymətləndirilməsinin nəşr edilmə statusu;
— məqsədlərə nail olunma dərəcəsi.

Əlavə A. Məqsədlər

(informativ məlumat)

A.1. Ümumi müddəalar

Sİ sistemlərinin riskləri identifikasiya edilərkən nəzərdən keçirilən sistemin mahiyyətindən və tətbiq edildiyi kontekstdən asılı olaraq, Sİ ilə əlaqəli müxtəlif məqsədlər nəzərə alınmalıdır. Nəzərə alınmalı olan Sİ ilə əlaqəli məqsədlərə A.2-A.12-ci bəndlərdə təsvir olunan məqsədlər (lakin bunlarla məhdudlaşmır) daxildir.

A.2. Hesabatlılıq

Hesabatlılıq həm təşkilatların xarakteristikalarına, həm də sistem xüsusiyyətlərinə aiddir:

— Təşkilati hesabatlılıq təşkilatların öz qərarlarına və fəaliyyətlərinə görə (onları izah etməklə) məsuliyyəti və rəhbər orqan, hüquqi orqanlar və daha geniş mənada maraqlı tərəflər qarşısında cavabdehlik daşıması mənasını ifadə edir.

— Sistem hesabatlılığı təşkilat tərəfindən həmin təşkilat çərçivəsindəki qərar və faəliyyətləri izləmək bacarığı ilə əlaqədardır.

Sİ-dən istifadə mövcud hesabatlılıq çərçivələrini dəyişə bilər. Əgər əvvəllər fərdlər məsuliyyət daşıdıqları fəaliyyətləri icra edirdilərsə, indi bu cür fəaliyyətlər Sİ sistemləri tərəfindən tam və ya qismən həyata keçirilə bilər. Bu halda kimin cavabdeh olacağı tənzimləyicilər tərəfindən davamlı olaraq nəzərdən keçirilir. Sİ sistemlərinin tərtibatçıları və istifadəçiləri həmin sistemlərin bazara çıxarıldığı və istifadə olunduğu ölkələrin müvafiq qanunvericilikləri barədə məlumatlı olmalıdırlar.

A.3. Sİ sahəsində təcrübə

Sİ sistemləri və onların işlənməsi Sİ ilə əlaqəli olmayan proqram həllərindən fərqlənir. Sİ sistemlərinin qiymətləndirilməsi, işlənməsi və quraşdırılması sahəsində fənlərarası bacarıqlara və təcrübəyə malik mütəxəssislərin seçilməsinə ehtiyac vardır.

Təşkilatlar bu cür təcrübəyə malik insanların Sİ sistemlərinin işlənməsi və spesifikasiyalarının müəyyən olunması prosesinə cəlb olunmasını təmin etməlidir.

SI sahəsində təcrübə Sİ sistemlərinin son istifadəçilərini əhatə etməlidir. İstifadəçilər Sİ sisteminin funksiyalarını kifayət qədər dəqiq anlamalı və səhv qərarları və ya nəticələri aşkar etmək və ləğv etmək səlahiyyətinə malik olmalıdırlar.

A.4. Təlim və test verilənlərinin əlçatanlığı və keyfiyyəti

ML-ə əsaslanan Sİ sistemləri nəzərdə tutulan davranışların (nəticələrin) əldə edilməsi məqsədilə sistemlərin təlimləndirilməsi və verifikasiyası üçün təlim və və test verilənlərinə ehtiyac duyur. Quraşdırılmış Sİ sistemləri produksiya verilənləri ilə işləyir. Təlim, test və produksiya verilənləri verilənlərin tipi və keyfiyyəti baxımından nəzərdə tutulan xüsusiyyətlərə uyğun olmalıdır.

Təlim və test verilənləri onların nəzərdə tutulan məqsədlər üçün aktuallığının və uyğunluğunun müəyyən edilməsi baxımından validasiya edilməlidir. Tələb olunan təlim və test verilənlərinin həcmi ətraf mühitin nəzərdə tutulan funksionallığı və mürəkkəbliyi əsasında dəyişə bilər. Təlim və test verilənləri Sİ sistemlərinin yüksək proqnozlaşdırma qabiliyyətini təmin etmək üçün kifayət qədər fərqli xüsusiyyətlərə malik olmalıdır. Bundan əlavə, mümkün olduqda, asılı olmayan verilənlər çoxluğundan istifadə etməklə təlim və test verilənləri arasında uyğunluq da təmin edilməlidir.

Təlim və test verilənlərinin təşkilat daxilində əlçatan olmaması və xarici mənbələrdən əldə edilməsi də mümkündür. Bu halda da verilənlərin lazımi keyfiyyəti təmin edilməlidir.

A.5. Ekoloji mühitə təsir

Sİ-dən istifadə ekoloji nöqteyi-nəzərdən də təsirlərə səbəb ola bilər. Sİ-dən istifadə ətraf mühitə müsbət təsir göstərə bilər. Məsələn, qaz turbinində azot oksidini azaltmaq üçün Sİ sistemlərindən istifadə edilə bilər. Sİ-nin tətbiqi resursların intensiv istifadəsi səbəbindən ətraf mühitə mənfi təsir də göstərə bilər. Məsələn, bəzi Sİ sistemlərinin təlim mərhələsi hesablama resursları tələb edir və əhəmiyyətli miqdarda elektrik enerjisi istehlak edə bilir. Buna görə də, ətraf mühitə bu kimi təsirlər nəzərə alınmalıdır.

A.6. Ədalətlilik

Avtomatlaşdırılmış qərarların qəbulu üçün Sİ sistemlərindən istifadə konkret fərdlər və ya fərd qrupları üçün ədalətli olmaya bilər. Ədalətsiz nəticələrin bir çox səbəbləri (obyektiv funksiyalardakı qərəzlilik, balanssız verilənlər çoxluqları, təlim verilənləri və sistemlərə geridönüşün verilməsində insan qərəzlilikləri) mövcuddur. Ədalətsizlik, həmçinin məhsul konsepsiyasında qərəzlilik məsələləri, problemlərin formalaşdırılması və ya Sİ sistemlərinin nə vaxt və harada quraşdırılacağı ilə bağlı seçimlərdən də yarana bilər.

Sİ sistemlərində qərəzlilik və ədalətlilik barədə ətraflı məlumat ISO/IEC TR 24027 [4] standartında təqdim olunur.

A.7. İstismar prosesində dəstək

İstismar prosesində dəstək göstərmək imkanı səhvləri düzəltmək və ya yeni tələblərə uyğunlaşmaq üçün təşkilatın Sİ sistemlərindəki dəyişiklikləri idarə etmək qabiliyyəti ilə bağlıdır. ML əsaslanan Sİ sistemləri təlimlər əsasında öyrəndiyindən və qaydalara əsaslanan yanaşmalardan istifadə etmədiyindən, Sİ sistemlərinin müşayiət olunması, təşkilatın istismar prosesində onlara dəstək göstərmək imkanı və bunun nəticələri araşdırılmalıdır.

A.8. Konfidensiallıq

Şəxsi toxunulmazlıq fərdlər tərəfindən onlara aid hansı məlumatların toplanması, saxlanılması və işlənməsinə, bu məlumatların kimlər tərəfindən açıqlanmasına nəzarət edilməsi və ya təsir göstərilməsi qabiliyyəti ilə bağlıdır. ISO/IEC TR 24028:2020 [3]-standartında izah edildiyi kimi, "bir çox Sİ üsulları (məsələn, dərin öyrənmə) böyük həcmli verilənlərdən əhəmiyyətli dərəcədə asılıdır, çünki onların dəqiqliyi istifadə etdikləri verilənlərin həcminə əsaslanır. Bəzi məlumatların, xüsusilə də fərdi və xüsusi kateqoriyalı

(həssas) fərdi məlumatların (məsələn, sağlamlıq qeydləri) sui-istifadəsi və ya açıqlanması məlumat subyektlərinə zərər vura bilər.

Sİ sistemlərinin xüsusi kateqoriyalı (həssas) fərdi məlumatlar barədə nəticələr əldə edə bilməsi də müəyyən edilməlidir. Sİ sistemləri üçün konfidensiallığa Sİ sistemlərinin qurulması və istismarı üçün istifadə olunan məlumatların mühafizəsi, Sİ sistemləri tərəfindən onun verilənlərinə icazəsiz girişin əldə edilməsi üçün müraciətin təmin edilməməsi və şəxs üçün fərdiləşdirilmiş və ya oxşar şəxslərin məlumat və ya xarakteristikalarının əldə edilməsi üçün istifadə edilə bilən modellərə müraciətlərlə bağlı mühafizənin təşkili daxildir.

Fərdi məlumatların düzgün olmayan toplanması, istifadəsi və açıqlanması ayrı-seçkilik, fikir və söz, habelə məlumat azadlığı kimi fundamental insan hüquqlarına birbaşa təsir göstərə bilər. İnsani dəyərlərə və insan ləyaqətinə hörmət baxımından etik prinsiplərə təsirlər də nəzərə alınmalıdır.

Qeyd: ISO/IEC 29134:2017 [5] standartında qeyd olunan məlumatların mühafizəsinə təsirin qiymətləndirilməsi (çox vaxt konfidensiallığın pozulmasına yönələn təsirin qiymətləndirilməsi kimi istinad edilir) məlumatların toplanması, Sİ sistemlərinin təlimi və istifadəsi zamanı fərdi məlumatların istifadəsi ilə bağlı risklərin idarə edilməsi üçün faydalı alətdir.

A.9. Dayanıqlıq

Dayanıqlıq sistemin müxtəlif istifadə şəraitlərində öz performans səviyyəsini saxlamaq qabiliyyəti ilə bağlıdır. Sİ sistemlərinin və ya əlaqəli komponentlərin etibarsız girişlər olduqda və ya stresli ətraf mühit şəraitində düzgün işləyə bilmə dərəcəsi tədbir və nəticələrin təkrar istehsal qabiliyyəti ilə birlikdə nəzərdən keçirilməlidir.

Dayanıqlıq Sİ sistemləri kontekstində yeni çağırışlar yaradır. Neyron şəbəkəsinin arxitekturaları həm izah baxımından çətin, həm də mahiyyətcə “qeyri-xətti”, bəzən də gözlənilməz davranışa malik olduqları üçün xüsusi çətinliklər törədir. Neyron şəbəkələrinin dayanıqlığının xarakterizə edilməsi açıq tədqiqat sahəsidir və həm test, həm də verifikasiya yanaşmaları üçün məhdudiyyətləri mövcuddur.

Neyron şəbəkələrinin dayanıqlığı barədə əlavə məlumat ISO/IEC TR 24029-1 [6] standartında təqdim olunur.

A.10. Mühafizəlilik

Sİ sistemlərinin istifadəsi mühafizəliliyin təmini ilə bağlı yeni təhdidlər yarada bilər. Mühafizəlilik müəyyən edilmiş şərtlər daxilində sistemin insan həyatı, sağlamlığı, əmlakı və ya ətraf mühit üçün təhlükə yarada biləcəyi şəraitin yaradılmamasına dair gözləntilərlə əlaqəlidir. Avtomatlaşdırılmış nəqliyyat vasitələrində, istehsal qurğularında və robotlarda Sİ sistemlərinin istifadəsi mühafizəliliklə bağlı risklər yarada bilər. Bu sahələrdəki Sİ sistemləri üçün xüsusi tətbiq sahələri (məsələn, maşın, nəqliyyat və ya tibbi cihazların layihələndirilməsi) üzrə xüsusi standartlar nəzərə alınmalıdır.

Sİ sistemləri üzrə funksional mühafizəlilik barədə daha ətraflı məlumat ISO/IEC TR 5469 [7] standartında təqdim olunur.

A.11. Təhlükəsizlik

İnformasiya təhlükəsizliyi risklərinin idarə edilməsi ISO/IEC 27005:2022 [8] standartında müəyyən edilmişdir. Sİ kontekstində və xüsusən də, ISO/IEC TR 24028:2020 [3] standartında təsvir olunduğu kimi, ML yanaşmalarına əsaslanan Sİ sistemləri ilə bağlı bir neçə yeni məsələ (verilənlərin “zəhərlənməsi”, rəqabətli hücumlar və model oğurluğu) klassik informasiya və sistem təhlükəsizliyi ilə bağlı problemlər xaricində nəzərdən keçirilməlidir.

A.12. Şəffaflıq və izahlılıq

Şəffaflıq həm Sİ sistemlərini istismar edən təşkilatların xüsusiyyətləri, həm də həmin sistemlərin bilavasitə özü ilə bağlıdır. Təşkilatlar bəzən bu cür sistemləri necə tətbiq etdikləri, toplanmış məlumatlardan (məsələn, istehlakçı və istifadəçi məlumatları, ictimai məlumatlar, digər toplanmış məlumat dəstləri) necə istifadə etdikləri, Sİ sistemlərinin idarə edilməsi, risklərinin başa düşülməsi və onlara nəzarət edilməsi üçün hansı tədbirləri həyata keçirdikləri və s. barədə məsələlərdə şəffaf olurlar. Sİ sistemlərinin şəffaflığı maraqlı tərəfləri onların məqsədlərinə uyğun olaraq Sİ sistemlərinin işlənməsi, istismarı və istifadəsini qiymətləndirməyə imkan verən sistem barədə müvafiq məlumatla (məsələn, imkanlar və məhdudiyyətlər) təmin etməkdən ibarətdir. Sİ sistemlərinin izahlılığı və müəyyən bir sistem üçün nəticənin necə generasiya edildiyini anlamağa kömək etmək və rasionallaşdırmaq qabiliyyəti ilə bağlıdır.

Əlavə B. Risk mənbələri

(informativ məlumat)

B.1. Ümumi müddəalar

Sİ sistemlərinin risklərini identifikasiya edərkən, sözügedən sistemin mahiyyətindən və tətbiq kontekstindən asılı olaraq müxtəlif risk mənbələri də nəzərə alınmalıdır. Nəzərə alınmalı risk mənbələrinə B.2-B.8-ci bəndlərdə təsvir olunan məsələlər və imkanlar (lakin bunlarla məhdudlaşmır) daxildir.

B.2. Mühitin mürəkkəbliyi

Sİ sistemlərinin fəaliyyət göstərdiyi mühitin [9] mürəkkəbliyi bu sistemlərin öz fəaliyyət kontekstində dəstəkləməli olduğu potensial situasiyaların diapazonunu təyin edir.

ML kimi bəzi Sİ texnologiyaları mürəkkəb mühitləri tənzimləmək üçün xüsusilə uyğundur və buna görə də, çox vaxt nəqliyyatın avtomatlaşdırılmış idarə edilməsi kimi mürəkkəb mühitlərdə istifadə olunan sistemlər üçün tətbiq olunur. Bununla belə, layihələndirmə və işlənmə prosesləri zamanı sistemin həll edəcəyi gözlənilən bütün müvafiq situasiyaları müəyyən etmək, təlim və test verilənlərinin bütün bu situasiyaları əhatə etməsini təmin etmək böyük problemdir.

Beləliklə, mürəkkəb mühitlər sadə mühitlərlə müqayisədə əlavə risklərlə nəticələnə bilər. Sİ sistemlərinin mühitinin başa düşülmə dərəcəsinin müəyyən edilməsinə xüsusi diqqət yetirilməlidir:

— Mühitin hərtərəfli başa düşülməsi yalnız sadə proqnozlaşdırıla bilən və ya idarə olunan mühitlər üçün mümkündür ki, (bu zaman Sİ sistemi qarşılaşa biləcəyi ətraf mühitlə bağlı bütün mümkün situasiyaları nəzərə ala bilir) bu da risklərin daha yaxşı idarə edilməsinə imkan verir.

— Mühitin yüksək mürəkkəbliyi və ya qeyri-müəyyənliyi səbəbindən, Sİ sistemlərinin bütün mümkün situasiyaları (məsələn, nəqliyyatın avtonom idarə edilməsində) proqnozlaşdıra bilmədiyi qismən başa düşülmə hallarında bütün müvafiq situasiyaların nəzərə alındığını fərz etmək olmaz. Bu, risk mənbəyi olan qeyri-müəyyənliklə nəticələnə bilər və buna görə də, sistemlərin layihələndirilməsi zamanı nəzərə alınmalıdır.

B.3. Qeyri-şəffaflıq və qeyri-izahlılıq

Şəffaflıq təşkilatın müvafiq fəaliyyət və qərarlarını (məsələn, siyasətlər, proseslər) və Sİ sistemləri barədə müvafiq məlumatları (məsələn, qabiliyyət, performans, məhdudiyyətlər, layihələndirmə seçimləri, alqoritmlər, təlim və test verilənləri, verifikasiya və validasiya prosesləri və nəticələri) müvafiq maraqlı tərəflərə kommunikasiya etməsidir. Bu, maraqlı tərəflərə Sİ sistemlərinin işlənməsi, istismarı və istifadəsini öz gözləntilərinə uyğun olaraq qiymətləndirməyə imkan verə bilər. Müvafiq məlumatların növü və səviyyəsi maraqlı tərəflərdən, istifadə hallarından, sistem növündən və qanunvericilik tələblərindən əhəmiyyətli dərəcədə asılıdır. Təşkilatların müvafiq maraqlı tərəflərə lazımi məlumatları təqdim edə bilməməsi təşkilatın və Sİ sistemlərinin etimadı doğrultma xüsusiyyətinə və hesabatlılığına mənfi təsir göstərə bilər.

İzahlılıq Sİ sistemlərinin elə xüsusiyyətidir ki, qərarların qəbul edilməsinə təsir göstərən mühüm faktorlar insanların başa düşəcəyi şəkildə ifadə oluna bilir. ML modeli (xüsusilə dərin öyrənmə hallarında) onu təlimləndirmək üçün istifadə olunan modeli və ya alqoritmi araşdırmaqla başa düşülməsi çətin olan davranışa malik ola bilər. Bu cür vacib faktorların ifadə (izah) edilməsinin mümkün olmadığı hallar Sİ sistemlərinin validasiyasına və insanların sistemə olan güvəninə mənfi təsir göstərir, çünki sistemin niyə bu vəya digər qərarı verəcəyi və ya bütün hallarda düzgün qərar verə biləcəyi aydın olmur. Bu cür qeyri-müəyyənlik bir çox risklərlə nəticələnə bilər, həmçinin etimadı doğrultma və hesabatlılıq kimi ümumi məqsədlərə və mühafizəlilik, təhlükəsizlik, ədalətlilik və dayanıqlıq kimi xüsusi məqsədlərə güclü təsir göstərə bilər. Buna görə də. izahlılıq Sİ sistemlərinin şəffaflığının bir hissəsi kimi yalnız maraqlı tərəflər üçün deyil, həm də Sİ sistemlərinin validasiyası və verifikasiyası məqsədilə təşkilatın özü üçün də aktualdır.

Həddindən artıq şəffaflıq və izahlılıq, həmçinin şəxsi toxunulmazlıq, təhlükəsizlik, konfidensiallıq tələbləri və əqli mülkiyyətlə bağlı risklərə səbəb ola bilər.

B.4. Avtomatlaşdırma səviyyəsi

Sİ sistemləri müxtəlif avtomatlaşdırma səviyyələrində fəaliyyət göstərə bilər. Onlar operatorun sistemə tam nəzarət etdiyi avtomatlaşdırılmamış sistemlərdən tam avtomatlaşdırılmış sistemlərə qədər diapazonda işləyə bilər. Ümumiyyətlə, Sİ sistemləri avtomatlaşdırılmış sistemlərdir. Konkret istifadə hallarından asılı olaraq, bu cür sistemlərin avtomatlaşdırılmış qərarları mühafizəlilik, ədalətlilik və ya təhlükəsizlik kimi müxtəlif sahələrə təsir göstərə bilər.

Zəruri hallarda xarici agentin iştirakı tələb edilən avtomatlaşdırma səviyyələrində funksiyaların sistemdən agentə ötürülmə prosesi risk mənbəyi ola bilər (məsələn, vaxt məhdudiyyətləri, agentin diqqətliliyi).

Avtomatlaşdırma səviyyələri haqqında əlavə məlumat ISO/IEC 22989:2022 standartının 5.2-ci bəndində təqdim olunur.

B.5. Maşın öyrənməsi ilə bağlı risk mənbələri

Sİ sahəsində nailiyyətlərin əksəriyyəti ML və onun dərin öyrənmə kimi altsahələri ilə bağlıdır. ML sistemlərinin davranışı yalnız istifadə olunan alqoritmlərdən deyil, həm də ML modellərinin təlim keçdiyi verilənlərdən əhəmiyyətli dərəcədə asılıdır. Beləliklə, Sİ xarakteristikalarına aşağıdakı mümkün təsirlər daxildir:

— Verilənlərin keyfiyyəti: Təlim və test verilənlərinin keyfiyyəti sistemin funksionallığına birbaşa təsir göstərir. Verilənlərin tələblərə uyğun keyfiyyətə cavab verməməsi ədalətlilik, mühafizəlilik və dayanıqlıq kimi müxtəlif məqsədlərə təsir edə bilər.

— ML-dən istifadə edən Sİ sistemləri üçün məlumatların toplanması məqsədilə istifadə olunan proseslər diaqnoz qoymaq və aşkar etmək kimi xüsusilə çətin olan risk mənbələrinə aiddir. Məsələn:

  — Verilənlərin tətbiq sahəsi üçün reprezentativ olmaması biznes məqsədləri üçün risklərə səbəb ola bilər.

  - Verilənlərin müxtəlif mənbələrdən əldə olunması (data sourcing) və saxlanması əhəmiyyətli dərəcədə etik və hüquqi risklərə məruz qala bilər. Verilənlərin toplanması prosesinin təhlükəsizliyinin təmin edilməməsi rəqabətli hücumlar, verilənlərin “zəhərlənməsi” və ya digər manipulyasiyalarla bağlı risklərə səbəb ola bilər.

— Fasiləsiz öyrənən Sİ sistemləri təkmilləşən produksiya verilənlərinə əsaslanan sistemlərin inkişaf etdirilməsi niyyətini daşıyır. Eyni zamanda, onlar istifadə zamanı istismara verildiyi zaman nəzərdə tutulmadığı şəkildə davranışlarını dəyişə bildiyi üçün riskləri artıra bilər.

B.6. Sistemin texniki təminat problemləri

Texniki təminat problemləri ilə bağlı risk mənbələrinə aşağıdakılar (lakin bunlarla məhdudlaşmır) daxildir:

— Nasaz komponentlərin səbəb olduğu texniki təminatla bağlı xətalar. Nümunələrə bir və ya daha çox yaddaş hücrələrində qısa qapanmalar və ya kəsilmələr, nasaz şin xətləri, ossillyatorların dreyf etməsi, “ilişmə” nacazlıqları (stuck-at faults) və ya inteqral sxemlərin giriş və ya çıxışlarında “arzuolunmaz rəqslər” (parasitic oscillations) daxildir.

— Çox vaxt yüksək enerji radiasiyası nəticəsində yaranan, yaddaş hücrələrinin və ya məntiq komponentlərinin arzuolunmaz müvəqqəti vəziyyət dəyişiklikləri kimi “yumşaq” xətalar.

— Təlim keçmiş ML modellərinin müxtəlif sistemlər arasında transferi emal gücü, yaddaş və xüsusi Sİ aparat sürətləndiricilərinin mövcudluğu baxımından sistemlərin fərqli texniki imkanlarına görə məhdudlaşdırıla bilər.

— Sİ sistemi məsafədən emal və verilənlərin saxlanmasını tələb etdiyi zaman şəbəkə resursları məhdud və paylaşılan xüsusiyyətlərə malik olduğu üçün şəbəkə xətaları, ötürücülük imkanlarının məhdudiyyətləri və gecikmələrin artması meydana çıxır.

B.7. Sistemin həyat dövrünə dair problemlər

Uyğun və ya rasional olmayan metodların, proseslərin Sİ sistemlərinin həyat dövrü boyu istifadəsi risklərə səbəb ola bilər. Belə risklərə misal olaraq aşağıdakıları göstərmək olar:

— Layihələndirmə və işlənmə: Nöqsanlı layihələndirmə prosesi Sİ sistemlərinin hansı kontekstlərdə istifadə olunduğu proqnozlaşdıra bilmədiyi üçün bu kontekstlərdə Sİ-dən istifadə gözlənilməz uğursuzluğa səbəb ola bilər.

— Verifikasiya və validasiya: Sİ sistemlərinin yenilənmiş versiyalarının tətbiqi üçün qeyri-adekvat verifikasiya və validasiya prosesi təsadüfi reqressiyalara və ya keyfiyyət, etibarlılıq və ya mühafizəlilik baxımından nəzərdə tutulmayan deteriorasiya (pisləşməyə) və ya deqradasiyaya səbəb ola bilər.

— Quraşdırılma: Düzgün olmayan quraşdırma konfiqurasiyası yaddaş, hesablama, şəbəkə, saxlanma, izafilik və ya balanslaşdırılmış yük ilə bağlı resurs problemlərinə səbəb ola bilər.

— Texniki dəstək, yenilənmə və yoxlama: Tərtibatçı tərəfindən artıq dəstəklənməyən və ya xidmət göstərilməyən, lakin hələ də istifadə olunan Sİ sistemləri təşkilat üçün uzunmüddətli risklər və ya məsuliyyət yarada bilər.

— Yeni məqsədlə istifadə: İstismarda olan Sİ sistemləri ilkin olaraq nəzərdə tutulmadığı kontekstdə istifadə oluna bilər, bu da layihələndirmə və faktiki istifadə mərhələlərində irəli sürülən fərqli tələblər səbəbindən yeni problemlər yarada bilər. Məsələn, sosial şəbəkələrdə paylaşılan fotoşəkillərdə üzlərin identifikasiya edilməsi üçün layihələndirilmiş sistem müşahidə kameralarının görüntülərində cinayətdə şübhəli bilinən şəxslərin üzlərini identifikasiya etməyə cəhd etmək üçün istifadə oluna bilər, lakin bu zaman ilkin istifadə halından fərqli olaraq daha yüksək dərəcədə dəqiqlik tələb olunur.

— İstismardan çıxarılma: Müəyyən Sİ sistemlərinin və ya Sİ texnologiyalarına əsaslanan komponentin istifadəsini sonlandıran təşkilatlar istismardan çıxarılan sistem tərəfindən təmin edilmiş informasiya və ya qərar qəbuletmə sahəsində bilikləri “itirə” bilər. Bundan əlavə, istismardan çıxarılan sistemi əvəz etmək üçün başqa bir sistem istifadə edilərsə, təşkilatda informasiya emalı və qərar qəbuletmə üsulu da dəyişə bilər.

B.8. Texnoloji hazırlıq səviyyəsi

Texnoloji hazırlıq səviyyəsi hər hansı texnologiyanın verilmiş tətbiq kontekstində nə qədər “yetkin” (mature) olduğunu göstərir. Sİ sistemlərinin işlənməsi və tətbiqində istifadə edilən və yetkinlik səviyyəsi daha aşağı olan texnologiyalar təşkilata məlum olmayan və ya qiymətləndirməsi çətin olan risklər yarada bilər. “Yetkin” texnologiyalar üçün risklərin identifikasiyasını və qiymətləndirilməsini asanlaşdıran daha geniş həcmli müxtəlif təcrübə verilənləri əlçatan ola bilər. Bununla belə, “yetkin” texnologiyalardan istifadə “arxayınlıq” və “texniki borc” (technical debt) kimi risklər də yarada bilər.

Əlavə C. Risklərin idarə edilməsi və Sİ sistemlərinin həyat dövrü

(informativ məlumat)

Cədvəl C.1-də ISO/IEC 22989:2022 standartında verilmiş risklərin idarə edilməsi prosesləri ilə Sİ sistemlərinin həyat dövrü arasındakı xəritəyə dair nümunə təqdim edilir:

Cədvəl C.1 — Risklərin idarə edilməsi və Sİ sistemlərinin həyat dövrü

<table>
<tr><td>→

Risklərin idarə edilməsi</td><td rowspan="2">Sİ risklərinin idarə edilməsi çərçivəsi

(Bölmə 5)</td><td colspan="5">Sİ risklərinin idarə edilməsi prosesi (Bölmə 6)</td></tr>
<tr><td>Sİ sistemləri-nin həyat dövrü ↓</td><td>Əhatə dairəsi, kontekst və meyarlar</td><td>Risklərin qiymətləndiril-məsi</td><td>Risklərin aradan qaldırılması</td><td>Monitorinq və yenidən baxış</td><td>Qeydəalın-ma və hesabatla-rın hazırlan-ması</td></tr>
<tr><td rowspan="2">Risklərin idarə edilməsi ilə bağlı təşkilati səviyyəli fəaliyyətlər</td><td rowspan="2">İdarəedici orqan Sİ risklərinin idarə edilməsi ilə bağlı istiqamətlər müəyyən edir.

Yuxarı idarəetmə orqanı üzərinə öhdəliklər götürür.

Yüksək səviyyəli risklərin idarə edilməsi meyilləri və ümumi meyarlar müəyyən edilir.</td><td colspan="5">Sİ sistemlərinin risklərinin idarə edilməsi prosesləri barədə geridönüş rəylərinə dair hesabatlar qəbul edilir və emal olunur.

Nəticə etibarilə, təşkilatın risklərin idarə edilməsi alətlərinin genişləndirilməsi və yaxşılaşdırılması ilə təşkilati risklərin idarə edilməsi çərçivəsi təkmilləşdirilir:</td></tr>
<tr><td>Risk meyarları üzrə kataloq</td><td>Potensial risk mənbələri üzrə kataloq;

Risk mənbələrinin qiymətləndiril-məsi və ölçülməsi texnikaları üzrə kataloq</td><td>Risklərin aradan qaldırılması üzrə məlum və ya həyata keçirilmiş tədbirlər üzrə kataloq</td><td>Sİ sistemlərinin monitorinqi və idarə edilməsi məqsədilə məlum və ya tətbiq edilmiş texnikalar üzrə kataloq;</td><td>Sİ sistemləri barədə məlumatı izləmək, qeydə almaq, hesabatlılı-ğı təmin etmək, daxili və xarici maraqlı tərəflərlə paylaşmaq üçün yaradılmış metodlar və müəyyən edilmiş formatlar üzrə kataloq</td></tr>
</table>

İlkin mərhələ	İdarəedici orqan Sİ sistemlərinin məqsədlərini təşkilatın və maraqlı tərəflərin prinsipləri və dəyərləri kontekstində təhlil edir; Təhlilə (adətən çoxmərhələli təhlilə) əsaslanaraq, Sİ sisteminin həyata keçirilməsinin mümkünlüyünü və təşkilatın həll etməyə çalışdığı problemləri həll edə biləcəyini müəyyən edir.	Sİ sistemlərinin risklərinin idarə edilməsi prosesi və sistemin risk meyarları təşkilatın risklərin idarə edilməsi çərçivəsinin fərdiləşdirilməsi yolu ilə formalaşdırılır.	Konkret SI sistemi ilə bağlı risk mənbələri identifikasiya edilir (potensial olaraq, çoxmərhələli şəkildə) və ətraflı formada təsvir edilir.	Risklərin aradan qaldırılmasına dair hərtərəfli plan qurulur. Potensial olaraq, “konseptin isbatı” metodları müəyyən edilir.	“Konseptin isbatı”na dair zəruri metodlar tətbiq edilir, test edilir və qiymətləndirilir.	Təhlillər və onların nəticələri, habelə tövsiyələr qeydə alınır və yüksək səviyyəli idarəetmə səviyyəsinə təqdim edilir.
Layihələndirmə və işlənmə Verifikasiya və validasiya	İdarəedici orqan qəbul edilən rəylərə dair hesabatlar əsasında sistemin məqsədlərini, effektivliyini və həyata keçirilməsinin mümkünlüyünü müntəzəm olaraq yenidən	Potensial olaraq, Sİ sistemlərinin risk meyarları rəylərə dair hesabatların nəticələrinə uyğun modifikasiya edilir.	Risklərin qiymətləndirilməsi müntəzəm olaraq həyata keçirilir (potensial olaraq, çoxmərhələli şəkildə).	Risklərin aradan qaldırılmasına dair plan həyata keçirilir. Risklərin aradan qaldırılması və risklərin (qalıq) qiymətləndirilməsi prosesi təyin edilmiş risk meyarlarına cavab	Testləşdirmə, verifikasiya və validasiya zamanı sistemin komponentləri, eləcə də bütün sistem üçün risklərin aradan qaldırılması planı qiymətləndirilir və tənzimlənir.	Nəticələr qeydə alınır və müvafiq risklərin idarə edilməsi prosesinə ötürülür (geri qaytarılır). Zəruri hallarda, nəticələr idarəetmə zəncirinin iştirakçılarına və

	qiymətləndirir.			verənə qədər davam etdirilir.		idarəedici orqana təqdim edilir.
Quraşdırılma	İdarəedici orqan qəbul edilən rəylərə dair hesabat əsasında sistemin məqsədlərini və mümkünlüyünü müntəzəm olaraq yenidən qiymətləndirir.	Sİ sistemlərinin risk meyarları və risklərin idarə edilməsi prosesi zəruri "konfiqurasiya" dəyişikliklərinə uyğun tənzimlənir.	Risklərin qiymətləndirilməsi müntəzəm olaraq həyata keçirilir (potensial olaraq, çoxsəviyyəli şəkildə).	Risklərin aradan qaldırılmasına dair plan "konfiqurasiya" dəyişiklikləri səbəbindən potensial olaraq yenilənir və həyata keçirilir. Risklərin aradan qaldırılması və risklərin (qalıq) qiymətləndirilməsi prosesi təyin edilmiş risk meyarlarına cavab verənə qədər davam etdirilir.	Zəruri tənzimləmələrə icazə vermək üçün Sİ sistemlərinin risklərin aradan qaldırılmasına dair planı yenidən qiymətləndirilir.	
İstismar və monitorinq Müntəzəm validasiya	İdarəedici orqan qəbul edilən rəylərə dair hesabat əsasında sistemin məqsədlərini, effektivliyini və mümkünlüyü	Potensial olaraq, Sİ sistemlərinin risk meyarları rəylərə dair hesabatın nəticələrinə uyğun modifikasiya edilir.	Sistemin risklərin qiymətləndirilməsi planı risk meyarlarındakı dəyişikliklər əsasında potensial olaraq tənzimlənir.	Sistemin risklərin aradan qaldırılması planı risklərin qiymətləndirilməsi nəticələrinə uyğun risk dəyişiklikləri	Sistemin komponentləri üçün risklərin aradan qaldırılmasına dair plan qiymətləndirilir və tənzimlənir.	

	nü davamlı olaraq yenidən qiymətləndirir.			əsasında potensial olaraq tənzimlənir.		
Təkrar qiymətləndirmə	İdarəedici orqan Sİ sistemlərinin məqsədlərini təşkilatın və onun maraqlı tərəflərinin prinsipləri və dəyərlərinə uyğunluğunu yenidən təhlil edir; Təhlilə əsaslanaraq, Sİ sistemlərinin mümkünlüyünü müəyyən edir.	Sİ sistemlərinin risklərinin idarə edilməsi prosesi və sistemin risk meyarları Sİ sistemlərinin xüsusi məqsədləri və əhatə dairəsindəki mümkün dəyişikliklər, istismar mərhələsinin monitorinqinin nəticələri və yeni tənzimləyici tələblər əsasında təkrar qiymətləndirilir.	Konkret Sİ sistemləri ilə bağlı mövcud risk mənbələrinin siyahısı uyğunluğun və mümkün boşluqların müəyyən edilməsi üçün təhlil edilir.	Risklərin aradan qaldırılmasına dair plan potensial olaraq yenilənir. Risklərin aradan qaldırılması və risklərin (qalıq) qiymətləndirilməsi prosesi müəyyən edilmiş risk meyarlarına cavab verənə qədər davam etdirilir.	Zəruri tənzimləmələrə icazə vermək üçün Sİ sistemlərinin risklərinin aradan qaldırılması planı yenidən qiymətləndirilir.	
İstismardan çıxarılma və ya əvəzetmə Yeni məqsədlər, risklər və onların aradan qaldırılması yolu ilə yeni	İdarəedici orqan təhlillər əsasında Sİ sistemlərinin məqsədlərinə yenidən baxılır, Sİ sistemlərinin istismardan çıxarılması və ya əvəzedilməsinin	Sİ sistemlərinin istismardan çıxarılmasının idarə edilməsi prosesi və sistemin istismardan çıxarılmasına dair risk meyarları formalaşdırılır.	Konkret Sİ sistemləri ilə bağlı risk mənbələri identifikasiya edilir və ətraflı formada təsvir edilir.	Risklərin aradan qaldırılmasına dair hərtərəfli plan qurulur.	“Konseptin isbatı”na dair zəruri metodlar tətbiq edilir, test edilir və qiymətləndirilir.	

risklərin idarə edilməsi prosesi başladılır	mümkünlü-yünü müəyyən edir.					

ƏDƏBİYYAT

[1] ISO/IEC 38507:2022, *Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations*

[2] ISO 26000:2010, *Guidance on social responsibility*

[3] ISO/IEC TR 24028:2020, *Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence*

[4] ISO/IEC TR 24027:2021, *Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making*

[5] ISO/IEC 29134:2017, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[6] ISO/IEC TR 24029-1:2021, *Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview*

[7] ISO/IEC TR 54692), *Artificial intelligence — Functional safety and AI systems*

[8] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[9] Russell S. J., Norvig P., Artificial intelligence: a modern approach. 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2010