Azərbaycan Respublikası
Nazirlər Kabinetinin 2025-ci il
“ 25 ” dekabr tarixli
411 nömrəli Qərarı ilə
təsdiq edilmişdir.

İnformasiya təhlükəsizliyi riskləri reyestrinin aparılma

QAYDASI

1. Ümumi müddəalar

1.1. Bu Qayda informasiya təhlükəsizliyi riskləri reyestrinin (bundan sonra – risklər reyestri) həmin reyestrin sahibi tərəfindən aparılmasının hüquqi, texniki və təşkilati əsaslarını müəyyən edir.

1.2. İnformasiya təhlükəsizliyinə risklərin idarə edilməsi, o cümlədən qiymətləndirilməsi və emal edilməsi üçün zəruri olan strukturlaşdırılmış informasiya konfidensial informasiya hesab edildiyindən, həmin informasiya risklər reyestrinin sahibi tərəfindən məsul olduğu informasiya infrastrukturunda yaradılan risklər reyestrində toplanılır, mühafizə edilir və istifadə olunur.

1.3. Risklər reyestrinin aparılmasının məqsədləri aşağıdakılardır:

1.3.1. milli informasiya məkanında informasiya təhlükəsizliyi və kibertəhlükəsizlik risklərinin kateqoriyalarını müəyyən etmək və təsnifatlaşdırmaq;

1.3.2. risklər reyestri sahibinin məsul olduğu informasiya məkanında informasiya təhlükəsizliyinə və kibertəhlükəsizliyə təhdidlərin qarşısının alınması üzrə fəaliyyəti səmərəli təşkil etmək;

1.3.3. informasiya təhlükəsizliyi üzrə yarana biləcək təhdidləri və riskləri qiymətləndirmək, o cümlədən başvermə ehtimallarını və təsir dərəcələrini, riskə səbəb ola biləcək hadisələri əvvəlcədən müəyyən etmək və qeydiyyata almaq, həyata keçirilməli qabaqlayıcı tədbirləri proqnozlaşdırmaq, süni intellekt əsaslı və digər müvafiq həllərin işlənib hazırlanmasını və tətbiqini təşkil etmək.

1.4. Risklər reyestrindən xidməti fəaliyyətin səmərəliliyinə və davamlılığına, habelə informasiya təhlükəsizliyinin idarə olunmasında iştirak edən fəaliyyət sahələrinə (o cümlədən informasiya və kommunikasiya texnologiyaları (bundan sonra – İKT) layihələrinə, İKT xidmətlərə, “Risklər reyestri” rəqəmsal xidmətlərinə və sənədləşdirilmiş informasiya dövriyyəsinə, hüquqi dəstək xidmətlərinə, fiziki təhlükəsizliyə, kadrlarla təminata, mal və xidmətlərlə təchizata) olan risklərlə informasiya təhlükəsizliyinə olan risklər arasında asılılıq əlaqələrinin, o cümlədən ortaq olan risklərin müəyyən olunması, risklərin emalı həllərinin uzlaşdırılması və optimallaşdırılması üçün istifadə olunur.

1.5. Bu Qaydanın tələbləri dövlət orqanları (kəşfiyyat və əks-kəşfiyyat fəaliyyətinin subyektləri istisna olmaqla), dövlət adından yaradılan publik hüquqi şəxslər, dövlət mülkiyyətində olan və paylarının (səhmlərinin) nəzarət zərfi dövlətə məxsus olan hüquqi şəxslər və digər büdcə təşkilatları (bundan sonra – qurumlar) üçün məcburidir və onlarda Azərbaycan Respublikasının Xüsusi Rabitə və İnformasiya Təhlükəsizliyi

Dövlət Xidməti (bundan sonra – Xidmət) tərəfindən informasiya təhlükəsizliyi üzrə aparılan nəzarətin predmetini təşkil edir.

1.6. Hüquqi şəxslər və fərdi sahibkarlar tərəfindən risklər reyestri könüllülük əsasında aparılır. Bu Qaydanın tələbləri hüquqi şəxslər və fərdi sahibkarlar üçün tövsiyə xarakterlidir və risklər reyestri aparılan zaman nəzərə alına bilər.

1.7. Bu Qayda ilə tənzimlənməyən məsələlər Azərbaycan Respublikası Prezidentinin 2018-ci il 12 sentyabr tarixli 263 nömrəli Fərmanı ilə təsdiq edilmiş "Dövlət informasiya ehtiyatları və sistemlərinin formalaşdırılması, aparılması, inteqrasiyası və arxivləşdirilməsi Qaydaları"na uyğun olaraq həyata keçirilir.

1.8. Bu Qaydada nəzərdə tutulmuş risklər reyestrlərində, "Təhdidlər və həllər" kataloqunda yaradılan, əldə edilən, toplanılan informasiya və elektron sənədlər Azərbaycan Respublikasının mülkiyyətidir.

1.9. Kritik informasiya infrastrukturunda informasiya təhlükəsizliyi riskləri reyestrinin aparılması həmin sahəni tənzimləyən normativ hüquqi aktlara uyğun olaraq həyata keçirilir.

1.10. Risklər reyestrlərinin layihələndirilməsi, formalaşdırılması (təşkili, istehsalı), tətbiq edilməsi, aparılması, nəzarətdə saxlanılması (o cümlədən auditi, monitorinqi, ekspertizası) və davamlı inkişafı ilə bağlı zəruri xərclər hər il dövlət büdcəsində aidiyyəti orqanlar üzrə nəzərdə tutulmuş vəsaitlər və qanunla qadağan olunmayan digər mənbələr hesabına maliyyələşdirilir.

2. Əsas anlayışlar

2.1. Bu Qaydada istifadə olunan əsas anlayışlar aşağıdakı mənaları ifadə edir:

2.1.1. **informasiya təhlükəsizliyi riski** (bundan sonra – risk) – informasiya mühafizəsinin obyektlərinə aid mümkün təhdidlərin baş verməsinin, bu zaman həmin obyektlərdəki boşluqlardan, çatışmazlıqlardan, zəifliklərdən, nəzarətsizliklərdən və ya digər uyğunsuzluqlardan istifadə edilmənin və baş verə biləcək fəsadların birgə ehtimalı;

2.1.2. **informasiya təhlükəsizliyinə təhdid** (bundan sonra – təhdid) – informasiya təhlükəsizliyi hadisəsinə səbəb olan amil və ya vəziyyət;

2.1.3. **informasiya təhlükəsizliyi insidenti** (bundan sonra – insident) – xidməti fəaliyyətin davamlılığının pozulmasına və ya nüfuzdan salınmasına və informasiya təhlükəsizliyinin təhdid olunmasına əhəmiyyətli dərəcədə və ya mütəmadi (sistemli) şəkildə səbəb olan, yaxud gözlənilməz baş verən informasiya təhlükəsizliyi hadisəsi;

2.1.4. **informasiya təhlükəsizliyi həlləri** (bundan sonra – həllər) – risklərin emal olunmasını, o cümlədən təhdidlərin baş verməsinin qarşısının alınmasını və insidentlərə cavab verilməsini təmin etmək üçün nəzərdə tutulmuş, formalaşdırılan, tətbiq olunan qabaqlayıcı, nəzarətedici, təshihedici üsulu və vasitələri (təşkilati və texniki alətləri) müəyyən və təqdim edən biliklər;

2.1.5. **informasiya təhlükəsizliyinə dair tələblər** – informasiyanın təhlükəsizlik vəziyyətinə, informasiya mühafizəsi fəaliyyətinə aid məqsədlər əsasında və mühafizə obyektləri üçün müəyyən edilən və sənədləşdirilən normalar;

2.1.6. **informasiya təhlükəsizliyi hadisəsi** – normativ hüquqi aktların, texniki normativ hüquqi aktların, informasiyanın təhlükəsizliyi üzrə siyasətin (bu siyasət üzrə

təyin edilmiş, habelə müqavilə, razılaşma və öhdəliklərdə sənədləşdirilən tələblərin, reqlamentlərin, prosedurların) həyata keçirilməsinin pozulmasının, idarəetmə alətlərinin çatışmazlığının və ya təhlükəsizlik baxımından əvvəl məlum olmayan halın yaranması;

2.1.7. **risklər reyestri** – risklərə və adekvat həllərə aid verilənlər bazalarından ibarət olan informasiya resursu;

2.1.8. **verilənlər bazası** – fəaliyyət proseslərinin informasiya təminatı üçün elektron daşıyıcıda əvvəlcədən nəzərdə tutulmuş təyinata və struktura uyğun toplanılan və saxlanılan, habelə xüsusiyyətləri və qarşılıqlı məntiqi əlaqələri müəyyən olunan, tələblərə uyğun qorunan və modellərə uyğun istifadə edilən verilənlərin nizamlanmış toplusundan ibarət elektron informasiya resursu;

2.1.9. **informasiya resursu** – fəaliyyət proseslərinin proqram təminatı vasitələri üçün lazım olan, bu vasitələrlə yaradılan sənədləşdirilmiş informasiyanın (sənədlərin, qeydlərin) elektron daşıyıcıda yerləşən və həmin fəaliyyət proseslərinə aid məntiqi əlaqələri olan verilənlər bazaları, fayl və ya digər formatlarda olan və identikləşdirilə bilinən informasiya ehtiyatı;

2.1.10. **risklər reyestrinin sahibi** (bundan sonra – sahib) – məsul olduğu informasiya məkanında informasiya təhlükəsizliyinə və kibertəhlükəsizliyə təhdidlərin qarşısının alınması üçün bu Qayda ilə, habelə digər aidiyyəti hüquqi aktlarla müəyyən edilmiş tədbirlər görməli olan qurumlar, həmçinin könüllülük əsasında digər hüquqi şəxs və ya fərdi sahibkar;

2.1.11. **risklər reyestrinin operatoru** (bundan sonra – operator) – sahib və ya onun bu sahədə fəaliyyətinin həyata keçirilməsi üzrə hüquq və vəzifələrini müəyyən edilən həcmdə və şərtlərlə həvalə etdiyi qurum;

2.1.12. **kibertəhlükəsizlik** – kiberməkanda informasiya və texnoloji resursların tamlığının, əlçatanlığının, konfidensiallığının və mötəbərliyinin təmin edilməsi vəziyyəti;

2.1.13. **kiberməkan** – insanların, proqram təminatı vasitələrinin internetdə (və digər qlobal şəbəkədə) ona qoşulmuş texniki qurğular və şəbəkələr vasitəsilə qarşılıqlı fəaliyyəti (ünsiyyət və kommunikasiyası) üçün yaradılan virtual mühit;

2.1.14. **“Risklər reyestri” rəqəmsal xidməti** – elektron qaydada nəzərdə tutulmuş, müvafiq alqoritmlərə və ya süni intellektə əsaslanan həllərdən və bu həllərə lazım olan verilənlərdən (onların ilkin mənbələrindən) istifadə olunaraq təqdim edilən, o cümlədən belə istifadə zamanı insan amilinin iştirakını minimallaşdıran İKT xidməti;

2.1.15. **İKT xidmət** – əvvəlcədən müəyyən olunan fəaliyyət proseslərinə birbaşa dəstək üçün İKT alətlərlə həyata keçirilən əsas kateqoriyalı xidmət;

2.1.16. **İKT qulluq** – proqram, proqram-texniki və texniki təminat vasitələrinə göstərilən köməkçi kateqoriyalı xidmət;

2.1.17. **risk ölçüsü** – ehtimal olunan informasiya təhlükəsizliyi hadisəsinin, yəni hadisəni mümkün edən təhdidin və təhdidi mümkün edən zəifliyin, habelə fəsadın ölçülərinin hasili;

2.1.18. **qalıq risk** – riskin emaldan sonra qalan və ölçülə bilinən hissəsi;

2.1.19. **informasiya təhlükəsizliyini idarəetmə sistemi** – informasiya mühafizəsinin obyektlərində bu mühafizənin məqsədlərini və gözləntilərini müvafiq risklərə, tələblərə və hədlərə uyğun həyata keçirmək üçün informasiya təhlükəsizliyinin

təşkilati və texniki alətlərindən, subyektlərindən ibarət olan, onlar arasında qarşılıqlı əlaqələri təmin edən çərçivə;

2.1.20. **fəaliyyətin davamlılığı** – fəaliyyət subyektinin fəaliyyət proseslərini və onlar arasında səbəb-nəticə əlaqələrini, bu proseslərin təminat infrastrukturlarının sistemli formalaşdırmasına, tətbiq etməsinə, nəzarətdə saxlamasına, habelə bu proseslərdə hər hansı pozulma, insident və fövqəladə hal baş verdikdə bu prosesləri, o cümlədən onların təminat infrastrukturlarını əvvəlcədən müəyyən edilmiş həddçərçivəsində bərpa və davam etdirə bilmə vəziyyəti;

2.1.21. **informasiya məkanı** – informasiya ehtiyatlarından, ehtiyat nüsxələrindən, onlarda olan informasiyanın həyat dövrü proseslərindən, bu proseslərdə istifadə olunan informasiya sistemlərindən və infrastrukturlarından, o cümlədən komponentlərindən və tərkibində olmadan həmin istifadəni təmin edən digər maddi və qeyri-maddi obyektlərdən, onlar arasında fiziki və məntiqi əlaqələrdən ibarət kompleks lokal mühit;

2.1.22. **kiber əks-kəşfiyyat** – milli informasiya təhlükəsizliyinə zərər vura biləcək mövcud və ya sonradan yaranan, hazırlanan təhdidlərin, o cümlədən bu təhdidlərlə əlaqədar olan hücumların, cəhdlərin, hazırlıqların, şəraitin və digər pozuculuq amillərinin aşkarlanması, qabaqlanması və qarşısının alınması məqsədilə İKT alətlərlə həyata keçirilən xüsusi fəaliyyət;

2.1.23. **milli informasiya məkanı** – Azərbaycan Respublikasının dövlət hakimiyyətinə və yerli özünüidarə orqanlarına, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq müəssisə, idarə və təşkilatlarına, vətəndaşlarına, Azərbaycan Respublikasının ərazisində daimi yaşayan vətəndaşlığı olmayan şəxslərə məxsus olan informasiya məkanlarının qarşılıqlı əlaqələrini təmin edən uzlaşdırılmış mühit.

2.2. Bu Qaydada istifadə olunan digər anlayışlar “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanunu və Azərbaycan Respublikasının digər normativ hüquqi aktları ilə müəyyən edilmiş mənaları ifadə edir.

3. Risklər reyestrinin fəaliyyət prinsipləri

3.1. Risklər reyestri Azərbaycan Respublikası Prezidentinin 2018-ci il 12 sentyabr tarixli 263 nömrəli Fərmanı ilə təsdiq edilmiş “Dövlət informasiya ehtiyatları və sistemlərinin formalaşdırılması, aparılması, inteqrasiyası və arxivləşdirilməsi Qaydaları”nın 2.1-ci bəndində nəzərdə tutulmuş prinsiplərə uyğun aşağıdakılar əsasında formalaşdırılır:

3.1.1. sistemli yanaşma – fəaliyyətin və infrastrukturun arxitekturasının, o cümlədən arxitektura komponentlərinin və onlar arasında asılılıq əlaqələrinin müəyyən olunması və nəzərə alınması;

3.1.2. vahid yanaşma – fəaliyyətin və infrastrukturun layihələndirilməsinin, formalaşdırılmasının, mühafizəsinin və istifadəsinin iyerarxiya üzrə məqsədləri, planları arasında uyğunsuzluğa, təzadlara yol verilməməsi və harmoniyanın təmin olunması;

3.1.3. konkret cavabdehlik – fəaliyyət proseslərinin müəyyən olunmasında, əlaqələndirilməsində, icrasında və infrastruktur komponentlərinin layihələndirilməsində, əldə olunmasında, tətbiqində, mühafizəsində iştirakçılar (qurumlar, struktur bölmələr, rollar, ştat vahidləri və qrup üzvləri) arasında məsuliyyət və səlahiyyət bölgüsünün təmin olunması;

3.1.4. icra və nəzarət arasında bölgü – fəaliyyətin icra üzrə proseslərinin icra rollarına (subyektlərinə), nəzarət üzrə proseslərinin nəzarət rollarına (subyektlərinə) həvalə olunması, hər hansı bir prosesin icrasının və ona nəzarətin eyni rola həvalə olunmasına yol verilməməsi;

3.1.5. nəticəyönümlülük, ölçüləbilənlik – fəaliyyət proseslərinin, onların məqsədlərinin keyfiyyət üzrə SMART (“Specific; Measurable; Achievable; Relevant; Timely”) (konkret; ölçüləbilən; nəticəli, mümkün; əhəmiyyətli, uyğun; vaxtında olma) meyarlarına uyğun olması;

3.1.6. risklərə preventivlik – fəaliyyətin və infrastrukturun layihələndirilməsində, formalaşdırılmasında, təhlükəsizliyində və istifadəsində risklərin əvvəlcədən nəzərə alınması.

4. Risklər reyestrinə aid informasiyanı müəyyən edən proseslər

4.1. Risklər reyestrinə toplanılan məlumatlar risklərin idarə edilməsi prosesləri ilə müəyyən olunur, yaradılır və istifadə edilir. Bu məqsədlə idarəetmənin kontekstinin və əhatə sahəsinin, o cümlədən aşağıdakı faktorların müəyyən edilməsi təmin olunmalıdır:

4.1.1. risklərin idarə edilməsi sahəsində məqsədlərin, prinsiplərin və digər meyarların müəyyən olunması;

4.1.2. riskləri idarəetmə sisteminin arxitekturasında və informasiya təhlükəsizliyini idarəetmə sisteminin (bundan sonra – İTİS), xidməti fəaliyyətin davamlılığını və keyfiyyətini idarəetmə sistemlərinin arxitekturalarında ortaq seqmentlərin müəyyən olunması;

4.1.3. İKT layihələrə, İKT xidmətlərə, sənədləşdirilmiş informasiya dövriyyəsinə, hüquqi məsləhət xidmətlərinə, fiziki təhlükəsizliyə, kadrlarla təminata, mal və xidmətlərlə təchizata, insidentlərin həllinə, fəaliyyətin auditinə, fəaliyyətin davamlı yaxşılaşdırılmasına tələblərin və hədlərin müəyyən olunması;

4.1.4. risklərin qiymətləndirilməsinə, risklərin emalının təşkilinə və təmin olunmasına aid proseslərin müəyyən olunması.

4.2. Risklərin qiymətləndirilməsi aşağıdakı prosesləri əhatə edir:

4.2.1. risklərin analizi üçün risklərin müəyyənləşdirilməsinə və risklərin ölçülməsinə aid proseslər müəyyən olunur;

4.2.2. risklərin müəyyənləşdirilməsi aşağıdakı proseslərlə təmin olunur:

4.2.2.1. risklərin idarə edilməsinin əhatə dairəsinə aid olan və mühafizə olunan ilkin və dəstəkləyici kateqoriyalı aktivlərin müəyyən olunması;

4.2.2.2. informasiya təhlükəsizliyinə əvvəlcədən məlum olan, sonradan yaranan və hazırlanan təhdidlərin, o cümlədən hücumların və onlara cəhdlərin müəyyən olunması;

4.2.2.3. mühafizənin mövcud və planlaşdırılan texnologiyalarının (üsul və vasitələrin) – informasiya təhlükəsizliyinin təşkilati və texniki idarəetmə alətlərinin, o cümlədən kiber əks-kəşfiyyat mexanizmlərinin və təhdid kəşfiyyatı alətlərinin müəyyən olunması;

4.2.2.4. təhdidlərin aktivlərdə istifadə edə biləcəyi boşluqların, çatışmazlıqların, zəifliklərin, nəzarətsizliklərin və digər uyğunsuzluqların müəyyən olunması;

4.2.2.5. təhdidlər nəticəsində yarana bilən informasiya təhlükəsizliyi hadisələrinin müəyyən olunması, o cümlədən insidentlərin aşkarlanması;

4.2.2.6. fəaliyyət davamlılığına, informasiya təhlükəsizliyinə və mühafizə olunan aktivlərə aid yarana bilən fəsadların müəyyən olunması;

4.2.3. risklərin ölçülməsi aşağıdakıları əhatə edir:

4.2.3.1. riskə səbəb olan infromasiya təhlükəsizliyi hadisəsinin təsiretmə ölçüsünün, o cümlədən təhdidin ehtimal və təsiretmə ölçüsünün və mühafizə olunan aktivdə istifadə edilə biləcəyi zəifliyin kritiklik ölçüsünün, həmçinin statistik məlumatlar əsasında başvermə ehtimalının (tezliyinin) müəyyən olunması;

4.2.3.2. riskin potensial texniki (konfidensiallığın, tamlığın, əlçatanlığın və hesabatlığın pozulması) və biznes nəticələri (maliyyə və nüfuz itkisi, uyğunluğun və məxfiliyin pozulması) əsasında təsirinin müəyyən olunması;

4.2.3.3. riskin təsirinə məruz qalan aktivin dəyəri əsasında risklərin prioritetləşdirilməsi;

4.2.3.4. keyfiyyət əsaslı risk qiymətləndirilməsi üçün “Risk dərəcəsi = aktivin dəyəri x başvermə ehtimalı (amillərin ortalaması və keçmiş statistik məlumatlar dəyərlərinin maksimumu) x təsir (texniki və biznes amilləri dəyərlərinin maksimumu)” mexanizmi əsasında risk dərəcəsinin müəyyən olunması;

4.2.3.5. kəmiyyət əsaslı risk qiymətləndirilməsi üçün “Risk qiyməti = aktivin dəyəri x başvermə tezliyi (faizlə ifadə edilmiş amillərin ortalaması və statistik məlumatlar dəyərlərinin maksimumu) x təsir (texniki və biznes amilləri dəyərlərinin maksimumu)” mexanizmi əsasında risk qiymətinin müəyyən olunması;

4.2.4. risklərin dəyərləndirilməsi üçün:

4.2.4.1. riskin analiz nəticələri və risklərin idarə edilməsinin kontekstində nəzərdə tutulmuş təsir meyarları arasında müqayisə aparılır;

4.2.4.2. riskin emal olunma imkanları və həlləri müəyyən olunur.

4.3. Risklərin emalı risklərə qarşı aşağıdakıların təşkilini və təmin olunmasını ehtiva edir:

4.3.1. risklərin emal variantının müəyyən olunmasını (riskin qarşısının alınması, riskin təsirini azaltma, riski başqa tərəfə ötürmə və riski qəbuletmə (saxlama) üzrə növlərdən uyğun olanın seçilməsi);

4.3.2. risklərin emal variantına uyğun emal üsulunun müəyyən olunmasını;

4.3.3. risklərin emal üsuluna uyğun emal vasitəsinin müəyyən olunmasını;

4.3.4. risklərin reallaşma hallarına insidentlərə cavab tədbirlərinin müəyyən olunmasını.

5. Risklər reyestrinin strukturu və ona daxil edilən məlumatlar

5.1. Risklər reyestrinin strukturu ona daxil edilməli, saxlanılmalı, qorunmalı, istifadə və təqdim olunmalı olan məlumatların təyinatları, xüsusiyyətləri, zəruri və mümkün emal variantları nəzərə alınmaqla bu Qaydaya uyğun olaraq müəyyən edilir və bu zaman informasiya təhlükəsizliyinin, İKT xidmət və sistemlərin idarə edilməsinə aid beynəlxalq və milli standartlar, habelə Azərbaycan Respublikasında bu sahədə qəbul olunmuş normativ hüquqi aktlar və tətbiq edilə bilən ixtisaslaşdırılmış alətlər nəzərə alınır.

5.2. Risklər reyestrinin strukturu, paylanmış verilənlər bazaları modelinə uyğun qurulduqda aşağıdakı bölmələrdən ibarət müəyyən olunur:

5.2.1. risklər reyestrinin əsas verilənlər bazası;

5.2.2. risklər reyestrinin lokal mənbələri olan verilənlər bazaları – informasiya mühafizəsinin obyekti olan əsas və köməkçi aktivlərə aid kataloq və reyestrlərin (ilkin məlumatların) risklər reyestri ilə ortaq (inteqrativ) bölmələri;

5.2.3. risklər reyestrinin mərkəzi mənbələri olan verilənlər bazaları;

5.2.4. həllərə aid texnologiyaların inventar uçotu – informasiya mühafizəsinin obyekti olan aktivlərə aid kataloqların və reyestrlərin risklər reyestrinə aid xüsusi bölmələri.

5.3. Risklər reyestrinin əsas verilənlər bazasının strukturu onun əsas təyinatı və onda toplanılan məlumatların kateqoriyaları nəzərə alınmaqla müəyyən olunur və bu Qaydaya əlavəyə uyğun məlumatlar daxil edilir.

5.4. Risklər reyestrinin lokal mənbələri olan verilənlər bazalarına informasiya mühafizəsinin obyekti olan ilkin və dəstəkləyici aktivlər barədə və müvafiq səviyyədə (təhdidlərin bu aktivlərdə istifadə edə biləcəyi uyğunsuzluqların olduğu tərkib hissələrin və onların parametrlərinin müəyyənləşdirilməsini mümkün edə bilən səviyyədə) təfsilatlı məlumatlar daxil edilir.

5.5. Risklər reyestrinin mərkəzi mənbəyi olan məlumat cədvəlləri “Təhdidlər və həllər” kataloqunun tərkibində yaradılır. Risklər reyestrinin mərkəzi mənbəyinə aşağıdakı verilənlər bazaları daxildir:

5.5.1. informasiya təhlükəsizliyinə və kibertəhlükəsizliyə normativ tələblərin mərkəzləşmiş uçotu;

5.5.2. təhdidlərin kateqoriyalar üzrə təsnifatlaşdırılmış toplusu;

5.5.3. risklərin emalı və insidentlərə cavablar üzrə nümunəvi olan və ünvansızlaşdırılmış həllərin mərkəzləşmiş uçotu;

5.5.4. risklərin və insidentlərin siyahısı.

5.6. Risklər reyestrinin mərkəzi mənbəyinə aid verilənlər bazalarının strukturu aşağıdakılar istisna olmaqla, risklər reyestrinin əsas verilənlər bazalarının strukturlarına uyğun yaradılır:

5.6.1. informasiya təhlükəsizliyinə aid hədlər, reqlamentlər, vasitələr və kompetensiyalar;

5.6.2. informasiya təhlükəsizliyinə aid məsuliyyətlərin və səlahiyyətlərin rollar üzrə bölgü matrisaları;

5.6.3. təhdidlərin və həllərin vektorları olan obyektləri və bu obyektlərdə olan uyğunsuzluqları müəyyənləşdirmə rekvizitləri;

5.6.4. təhdidlərə və həllərə aid olan fəsadları müəyyənləşdirmə rekvizitləri.

5.7. Həllərə aid texnologiyaların inventar uçotunun strukturu həmin texnologiyaların əsas təyinatları və risklər reyestrinin lokal mənbələri olan verilənlər bazalarının strukturu nəzərə alınaraq yaradılır.

5.8. Risklər reyestrinin əsas verilənlər bazasına və həllərə aid texnologiyaların inventar uçotunun bazalarına daxil ediləcək məlumatlar risklərin idarə edilməsi prosesləri ərzində müəyyən olunur.

5.9. Risklər reyestrinin lokal və mərkəzi mənbələri olan verilənlər bazalarına daxil ediləcək məlumatlar risklərin idarə edilməsi proseslərindən əvvəl müəyyən olunur, bu proseslər ərzində aktuallığının təmin edilməsi üçün mütəmadi yenilənir.

6. Risklər reyestrinin aparılması qaydası

6.1. Risklər reyestri bu Qaydaya və bu sahədə qəbul olunmuş digər normativ hüquqi aktlara uyğun olaraq aparılır.

6.2. Risklər reyestrinin aparılması onun layihələndirilməsindən və formalaşdırılmasından (təşkilindən) yaranan nəticəni tətbiq etmək, nəzarətdə saxlamaq, davamlı təkmilləşdirmək üzrə idarəetmə mərhələlərindən və onlara aid proseslərdən ibarətdir.

6.3. Risklər reyestri sahibinin fəaliyyət hədəflərinə nail olunması, öhdəliklərinin və bununla əlaqədar zəruri informasiya təminatının həyata keçirilməsi məqsədilə sahibin özü və operatoru tərəfindən “Risklər reyestri” rəqəmsal xidməti vasitəsilə aparılır.

6.4. “Risklər reyestri” rəqəmsal xidmətinin əsas təyinatı bu reyestrin formalaşdırılmasının, tətbiqinin, mühafizəsinin və aktuallığının davamlı təmin edilməsidir. “Risklər reyestri” rəqəmsal xidməti bu Qaydaya, habelə sahib tərəfindən müəyyən edilən xüsusi tələblərə uyğun funksionallığa, konfiqurasiyaya və mühafizə alətlərinə malik olmalıdır.

6.5. Risklər reyestrinin aparılmasına xüsusi tələblər sahib tərəfindən müəyyən olunur.

6.6. “Risklər reyestri” rəqəmsal xidmətinin funksionallıq imkanları, konfiqurasiya komponentləri və parametrləri risklərin və xidmətlərin idarə edilməsinə aid müvafiq standartlarda (ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 20000) və qabaqcıl təcrübələrdə (“ITIL, Information Technology Infrastructure Library”) nəzərdə tutulmuş, habelə bu Qaydaya və sahib tərəfindən müəyyən olunan xüsusi tələblərə uyğun müəyyən edilməlidir.

6.7. “Risklər reyestri” rəqəmsal xidmətinin texniki funksionallığı sahib tərəfindən müəyyən olunan İKT alətlər vasitəsilə təmin edilir.

6.8. “Risklər reyestri” rəqəmsal xidmətinin funksionallığı risklərin idarə edilməsini (qiymətləndirilməsini və emalını) əhatə etməlidir.

6.9. Risklər reyestrinə İKT qulluq müvafiq razılaşdırma sənədi ilə müəyyən olunmalı, o cümlədən aşağıda göstərilən tədbirləri təmin etməlidir:

6.9.1. risklər reyestrinin verilənlər bazalarının idarə edilməsi, strukturunun yaradılması, əlavələrin və dəyişikliklərin edilməsi, həmçinin əlaqəli ilkin mənbələrlə uzlaşdırılması;

6.9.2. informasiya təhlükəsizliyi hadisələrinə (təhdidin baş verməsinə, uyğunsuzluqdan istifadə olunmasına, fəsadın yaranmasına) dair qeydlərin müvafiq sistem jurnallarından real vaxt rejimində mərkəzləşmiş saxlanca toplanılması.

7. Sahibin və operatorun funksiyaları

7.1. Sahib və operator tərəfindən risklər reyestrinin aparılması ilə əlaqədar aşağıdakı funksiyalar yerinə yetirilir:

7.1.1. risklər reyestrinin bu Qaydaya və bu sahədə qəbul edilmiş digər normativ hüquqi aktlara uyğun olaraq aparılması təmin edilir;

7.1.2. “Risklər reyestri” rəqəmsal xidmətini formalaşdırılıb təqdim olunmasına, ondan istifadə və informasiya təhlükəsizliyinə nəzarət, habelə risklər reyestrinin aparılmasına aid olan prosesləri, bu proseslərə aidiyyəti olan rolları, proseslərlə həmin rollar arasında məsuliyyətin bölgüsü dəqiqləşdirilir və məsuliyyətin bölgüsü matrisaları tərtib edilir;

7.1.3. “Təhdidlər və həllər” kataloqundan təqdim olunan təhdidlər və həllər barədə informasiyanın risklər reyestrində toplanılması və mütəmadi olaraq yenilənməsi təmin edilir;

7.1.4. “Təhdidlər və həllər” kataloqunda qeydiyyata alınmaq üçün risklər reyestrində olan biliklər və yeni aşkar olunan təhdidlər barədə informasiyanın “Təhdidlər və həllər” kataloquna ötürülməsi təmin edilir;

7.1.5. “Risklər reyestri” rəqəmsal xidmətinin texniki funksionallığı üçün tətbiq edilən İKT alətlərin müəyyən olunması, layihələndirilməsi, təşkili və idarə edilməsi təmin olunur;

7.1.6. risklər reyestrinə aid və mühafizə obyekti olan proseslər üçün məlumatlara, texniki xidmətlərə, proqram, texniki və mühəndis təminatı vasitələrinə, habelə bu vasitələrin funksionallıq imkanlarına (modullarına) səlahiyyətlərin istifadəçi rolları arasında bölgüsü müəyyən edilir;

7.1.7. risklər reyestrinin informasiya təhlükəsizliyi təmin edilir;

7.1.8. “Risklər reyestri” rəqəmsal xidmətinin təkmilləşdirilməsi, o cümlədən funksional imkanlarının artırılması üzrə tədbirlər görülür.

7.2. Operator funksiyaları sahib tərəfindən həyata keçirilmədikdə, həmin funksiyalar sahiblə operator funksiyalarını həyata keçirəcək subyekt arasında müvafiq xidmət səviyyəsi barədə razılaşma sənədi ilə müəyyən olunur.

8. Xidmətin funksiyaları

8.1. Xidmət tərəfindən risklər reyestrinin aparılması ilə əlaqədar aşağıdakı funksiyalar yerinə yetirilir:

8.1.1. “Təhdidlər və həllər” kataloqunun sahibinin funksiyaları həyata keçirilir;

8.1.2. “Təhdidlər və həllər” kataloqunun mühafizəsi üçün tətbiq edilən İKT alətləri müəyyən olunur və idarə edilir;

8.1.3. “Təhdidlər və həllər” kataloqu mütəmadi olaraq yenilənir;

8.1.4. “Təhdidlər və həllər” kataloquna təqdim olunan təhdidlər və həllər barədə informasiya risklər reyestrlərindən və digər mənbələrdən toplanılır və mütəmadi olaraq yenilənir;

8.1.5. risklər reyestrlərində informasiya təhlükəsizliyinin müstəqil və mərkəzləşmiş ölçmələri (uyğunluğun qiymətləndirilməsi, səmərəliliyin dəyərləndirilməsi) aparılır və onların nəticələri, habelə təhdidlər və həllər barədə mərkəzləşmiş toplanılan məlumatlar aidiyyəti üzrə sahibə təqdim edilir;

8.1.6. aidiyyəti subyektlərə bu Qaydanın tələbləri ilə əlaqədar metodiki dəstək göstərilir;

8.1.7. qanunvericiliklə səlahiyyətlərinə aid edilmiş digər tədbirlər həyata keçirilir.

9. Risklər reyestrinin informasiya təhlükəsizliyi

9.1. Risklər reyestrinin informasiya təhlükəsizliyinə yönələn və texnologiyaların inkişafına paralel olaraq intensiv yenilənən təhdidlərlə, habelə aşağıdakılarla bağlı informasiya sahibi tərəfindən dəqiqləşdirmələr aparılır:

9.1.1. təhdidlərin risklər reyestrində və “Risklər reyestri” rəqəmsal xidmətində istifadə edə biləcəyi boşluqlar, çatışmazlıqlar, zəifliklər, nəzarətsizliklər və digər uyğunsuzluqlar;

9.1.2. təhdidlərdən xidməti fəaliyyətin səmərəliliyinə, davamlılığına və informasiya təhlükəsizliyinə yarana bilən fəsadlar;

9.1.3. təhdidlərin və fəsadların risklərin ehtimal və ciddilik dərəcələri;

9.1.4. risklərin emal edilməsi variantları, üsulları və vasitələri.

9.2. Hər bir risklər reyestrinin informasiya təhlükəsizliyinə həmin reyestrin sahibi cavabdehdir.

9.3. Fəaliyyət proseslərinə məsuliyyətlərin, proseslərə lazım olan məlumatlara, texniki xidmətlərə, proqram, texniki və mühəndis təminatı vasitələrinə, bu vasitələrin funksionallıq imkanlarına (modullarına) səlahiyyətlərin rollar arasında bölgüləri əvvəlcədən müəyyən olunur və cari fəaliyyət zamanı təmin edilir.

9.4. Risklər reyestrinin aparılması üçün tətbiq olunan və təşkilati idarəetmə alətlərinə (proseslərə) ISO/IEC 15504 standartına uyğun olaraq, yetkinlik (“maturity”) üzrə ən azı 4-cü səviyyə (qurumun “biliklər bazasına” əsaslanan, təsdiqlənmiş meyarları olan, əvvəlcədən müəyyən olunan, qeydləri yetərli və nəticələri ölçülən səviyyə), texniki idarəetmə alətlərinə, ISO/IEC 15408 standartına uyğun olaraq, etimadlılıq (“Evaluation Assurance Level, EAL”) üzrə 6-cı səviyyə (verifikasiya, validasiya və nüfuzetmə testləri keçirilən, test ssenariləri və nəticələri sənədləşdirilən səviyyə) təyin və təmin olunur, bu səviyyələrə uyğunluq mütəmadi audit olunur. İnformasiyanın mühafizəsi üçün istifadə olunan alətlər sertifikatlaşdırılır.

9.5. İnformasiya məkanlarında risklər reyestrinin əsas verilənlər bazasının mərkəz cədvəli, uyğunsuzluqların ünvanı, mühafizə üsul və vasitələrinin təyinatları və obyektləri, habelə uzlaşdırma barədə məlumatlar informasiyanı mühafizə vasitələri ilə qorunur. Bu məlumatların və risklərin emalının təşkilati və texniki idarəetmə alətlərinə aid biliklər bazaları yalnız informasiya məkanlarına məsul olan subyektlərin sahib olduqları informasiya resurslarında toplanıla, saxlanıla və istifadə oluna bilər. Bu

məlumatların mərkəzləşmiş kataloqa və ya digər informasiya məkanlarına köçürülməsinə yol verilmir.

9.6. Hər bir risklər reyestrinin konfiqurasiyasının və funksionallığının informasiya təhlükəsizliyi tələblərinə uyğunluğunun qiymətləndirilməsi və səmərəliliyinin dəyərləndirilməsi həmin reyestrin sahibi və Xidmət tərəfindən təmin olunur.

9.7. “Təhdidlər və həllər” kataloqundakı məlumatlara sahib üçün əlçatanlıq Xidmət tərəfindən təmin olunur.

10. Risklər reyestrinin səmərəliliyinin dəyərləndirməsi

10.1. Risklər reyestrinin səmərəlilik səviyyəsi onun idarəetmə aləti olan “Risklər reyestri” rəqəmsal xidmətinin təyinatı üzrə yetərlilik və yararlılıq dərəcələrinin xidmət səviyyəsini müvafiq razılaşdırma sənədində təyin olunan məqbul hədlərə uyğunluğundan, bu hədlərin qurumun informasiya məkanının informasiya təhlükəsizliyini idarəetmə hədəflərinə uyğunluğundan asılıdır.

10.2. Risklər reyestrinin səmərəliliyini dəyərləndirmə üçün aşağıdakı əsas indikatorlar üzrə ölçmə parametrləri (“metrics”) formalaşdırılaraq tətbiq olunur:

10.2.1. konfiqurasiyanın uyğunluğunun qiymətləndirilməsi üzrə:

10.2.1.1. mühafizə obyektləri olan aktivlərin siyahısı və informasiya təhlükəsizliyini idarəetmənin əhatə sahəsi arasında uyğunluq dərəcələri;

10.2.1.2. tələblər toplusu və mühafizə obyektləri olan aktivlərin kataloqu (reyestri) arasında uyğunluq dərəcələri;

10.2.1.3. informasiya təhlükəsizliyinin baza vəziyyəti və tələblər toplusu, habelə informasiya təhlükəsizliyini idarəetmə hədəfləri, prinsipləri və hədləri arasında uyğunluq dərəcələri;

10.2.1.4. təhdidlərin uçotu və informasiya təhlükəsizliyinin baza vəziyyəti arasında uyğunluq dərəcələri;

10.2.1.5. risklər reyestri və təhdidlər uçotu arasında uyğunluq dərəcələri;

10.2.1.6. risklərin emal variantlarının risklər reyestrinə uyğunluq dərəcələri;

10.2.1.7. risklərin emalına aid qabaqlayıcı, nəzarətedici və təshihedici üsulların (tədbirlərin, proseslərin) risklərin emal variantlarına uyğunluq dərəcələri;

10.2.1.8. risklərin emalına aid qabaqlayıcı, nəzarətedici və təshihedici vasitələri (proqram, texniki və mühəndis təminatı vasitələrinin) və risklərin emal üsulları arasında uyğunluq dərəcələri;

10.2.1.9. ehtimal olunan fəsadlarla əlaqədar zərər vurulan aktivlərdə risklərin emalına aid bərpaedici üsullar (tədbirlər, proseslər), o cümlədən insidentlərə cavab sxemləri (ssenariləri), alqoritmik iş kitabçaları və risklərin emal üsulları arasında uyğunluq dərəcələri;

10.2.1.10. risklərin emalına aid bərpaedici vasitələr (proqram, texniki və mühəndis təminatı vasitələri), o cümlədən alqoritmik iş kitabçalarını avtomatik tətbiqetmə əsasında kompüterləşdirilmiş həllər və risklərin emal üsulları arasında uyğunluq dərəcələri;

10.2.2. funksionallığın səmərəliyinin dəyərləndirilməsi üzrə:

10.2.2.1. risklər reyestrinin müvafiq mənbələrdən məlumatlara əlçatanlığının və onların tamlığının təmin olunma dərəcələri;

10.2.2.2. risklər reyestrində risklərin qiymətləndirilməsi və emal edilməsi üçün nəzərdə tutulmuş üsulların, vasitələrin yeni texnologiyalara, intensiv yenilənən təhdidlərə və həllərə uyğunluq dərəcələri;

10.2.2.3. risklərin emalına aid həllər kataloquna (“biliklər bazası”na), o cümlədən alqoritmik iş və tətbiqetmə kitabçalarına informasiya məkanlarına məsul olan subyektlər üçün informasiya əlçatanlığının və tamlığının təmin edilmə dərəcələri;

10.2.2.4. risklər reyestrində risklərin emalı üçün nəzərdə tutulmuş üsulların, vasitələrin tətbiqindən sonra qalıq risklərin qurumun riskgötürmə qabiliyyəti daxilində qəbul edə biləcəyi riskin ölçüsündən yuxarı səviyyədə yaranmasının qarşısının alınma dərəcələri;

10.2.2.5. risklərin reallaşması – insidentlərin baş vermə və təsir hallarının risklər reyestrindəki həmin risklər üzrə nəzərdə tutulmuş qalıq risk dərəcəsinə uyğunluq səviyyəsi.

10.3. Hər bir risklər reyestrinin səmərəlilik səviyyəsi sahib tərəfindən mütəmadi, Xidmət tərəfindən isə ildə 1 (bir) dəfədən az olmayaraq dəyərləndirilməlidir.

“İnformasiya təhlükəsizliyi riskləri
reyestrinin aparılma Qaydası”na

əlavə

Risklər reyestrinin əsas verilənlər bazasına daxil edilən məlumatlar

1. Risklər reyestrinin mərkəz cədvəlinə daxil edilən məlumatlar:

1.1. risk, riskin kateqoriyası və mahiyyəti;
1.2. risk faktoru olan təhdid, təhdid sxemi, təhdidin ehtimal və ciddilik dərəcələri;
1.3. təhdidin ünvanlandığı obyektdə (aktivdə) istifadə etdiyi uyğunsuzluq və ya uyğunsuzluqlar zənciri, uyğunsuzluğun ciddilik dərəcəsi;
1.4. təhdiddən yarana bilən informasiya təhlükəsizliyi hadisəsi və ciddilik dərəcəsi;
1.5. təhdiddən yarana bilən fəsad, fəsadın ehtimal və ciddilik dərəcələri;
1.6. riskin ehtimal və ciddilik dərəcələri;
1.7. riskin emal variantı, üsulu və həlli;
1.8. riskin reallaşma faktı (insident);
1.9. insidentə cavab variantı, üsulu və həlli;
1.10. risklər reyestrində qarşılıqlı əlaqəli olan, həmçinin bu reyestrə ilkin mənbə olan cədvəllər ilə risklər reyestrinin mərkəz cədvəli arasında uzlaşdırma məlumatları.

2. İnformasiya təhlükəsizliyinə tələblərə və məqbul hədlərə aid daxil edilən məlumatlar:

2.1. İnformasiya təhlükəsizliyinə tələblərə daxil edilməli məlumatların kateqoriyaları:
2.1.1. tələb, tələbin kateqoriyası və mahiyyəti:
2.1.2. tələbin mənbəyi (normativ hüquqi akt, standart, müqavilə, öhdəlik, qabaqcıl təcrübə və praktik tələbat);
2.1.3. tələbin qoyulduğu fəaliyyət sahəsi (fəaliyyətin keyfiyyətinə və davamlılığına, risklərin emalına, İTİS üzrə əməkdaşlıq və koordinasiyaya, İKT layihələrə, rəqəmsal xidmətlərə, sənədləşdirilmiş informasiya dövriyyəsinə, hüquqi məsləhət xidmətlərinə, fiziki təhlükəsizliyə, kadrlarla təminata, mal və xidmətlərlə təchizata, insidentlərin həllinə, fəaliyyətin auditinə və fəaliyyətin davamlı yaxşılaşdırılmasına);
2.1.4. informasiya təhlükəsizliyinə dair tələblər;
2.1.5. informasiya təhlükəsizliyi üzrə prinsiplər;
2.1.6. İTİS-nin əhatə sahələri üzrə tələblər, o cümlədən:
2.1.6.1. informasiya məkanlarında İTİS-yə aid təşkilati idarəetmə (o cümlədən planlaşdırma, təminetmə, nəzarət və təkmilləşdirmə) alətlərinə tələblər;
2.1.6.2. İTİS-yə aid texniki idarəetmə (texniki xidmət, İKT sistem, proqram, texniki və mühəndis təminatı) alətlərinə tələblər;

2.1.6.3. insan kapitalına aid təhlükəsizlik tələbləri;

2.1.6.4. fiziki təhlükəsizliyə dair tələblər;

2.1.7. normativ hüquqi aktlar üzrə tələblər, o cümlədən:

2.1.7.1. ölkədə qəbul olunan beynəlxalq normativ hüquqi aktların tələbləri;

2.1.7.2. milli normativ hüquqi aktların tələbləri;

2.1.7.3. lokal (qurumdaxili) normativ aktların tələbləri;

2.1.8. standartlardan, texniki normativ hüquqi aktlardan irəli gələn tələblər və qabaqcıl təcrübələr:

2.1.8.1. beynəlxalq, regional və milli standartların tələbləri;

2.1.8.2. beynəlxalq, regional, milli və lokal (qurumdaxili) qabaqcıl təcrübələr;

2.1.8.3. beynəlxalq, regional və milli elmi-texniki nailiyyətlərdən irəli gələn innovativ həllər;

2.1.8.4. infrastrukturdan, konfiqurasiya vahidlərindən irəli gələn xüsusi (spesifik) tələblər (istehsalçı, təchizatçı və istifadəçi tərəfindən təqdim olunan).

2.2. İnformasiya təhlükəsizliyi üzrə məqbul hədlərə aid daxil edilməli məlumatlar kateqoriyaları:

2.2.1. İTİS-nin əhatə sahəsinə aid olan xidməti fəaliyyətin davamlılığı (“business continuity”) üçün bu fəaliyyətin hər bir prosesinə (xüsusilə, prioritetlik və kritiklik dərəcələri yuxarı olan proseslərə) maksimal məqbul dayanma (“maximum acceptable outage, MAO”) hədləri və fəaliyyətin davamlılığı üçün minimal məqsədlərə (“minimum business continuity objective, MBCO”) aid hədlər;

2.2.2. İTİS-yə aid, onun əhatə hüduduna daxil olan fəaliyyət sahələrində, menecment sistemlərində təhlükəsizliyə aid proseslər üçün yetkinlik (“maturity”) üzrə hədlər;

2.2.3. İTİS-nin əhatə sahəsinə aid olan informasiyanın fəaliyyət sahəsi, mərhələsi və prosesi üçün prioritetlik, kritiklik hədləri, tamlıq (dəqiq, səlis, aktual və bütöv olma), əlçatanlıq (müraciət və əldə etmə, nəzarətdə saxlamanın mümkün olması), konfidensiallıq (yalnız səlahiyyəti olan istifadəçilər və proseslər üçün məlum olması) və mötəbərlilik (adekvat, obyektiv, faydalı olması) hədləri;

2.2.4. fəaliyyət proseslərinə xidmət və onların təminat vasitələrinə qulluq səviyyələrinin müvafiq razılaşdırma (“SLA/ OLA, Service/ Operational Level Agreements”) sənədində təyin olunan hədləri, o cümlədən bu xidmətlər və qulluqlar üçün məqbul imkan hədləri, onların tətbiqi üçün səmərəlilik hədləri;

2.2.5. fəaliyyət proseslərinin proqram, texniki və mühəndis təminatı sistemlərinə, vasitələrinə fəaliyyət davamlılığı (“business continuity”) və informasiya təhlükəsizliyi üçün yetərlilik və yararlılıq üzrə hədlər, o cümlədən imkan hədləri, etimad qiyməti səviyyəsi üzrə hədlər (“Evaluation Assurance Level – EAL”);

2.2.6. fəaliyyət sahələrində və menecment sistemlərində iş rejimlərinə, reqlamentlərə aid hədlər;

2.2.7. rəhbərlik, idarəetmə, inzibatçılıq (“governance, management, administration”), icraçılıq və digər kateqoriyalı rollar, menecment sistemləri və struktur bölmələri, layihə və işçi qrupları arasında, sistemlərdə iştirakçı rollar, ştat vahidləri arasında məsuliyyət və səlahiyyət bölgüsünün bu sadalanan laylar üzrə matrisaları, vəzifə və hüquq hədləri;

2.2.8. fəaliyyət proseslərinin subyektləri (qurumlar, struktur bölmələr və ştat vahidləri) üçün məqsədlərə, hədəflərə, vəzifələrə faktiki uyğunluq və səmərəlilik hədləri;

2.2.9. fəaliyyət proseslərinin proqram, texniki və mühəndis təminatı sistemlərindən, vasitələrindən istifadə edən subyektlərə (qurumlara, struktur bölmələrə və ştat vahidlərinə) bu sistemlər, vasitələr üzrə nəzərdə tutulmuş səmərəlilik hədləri;

2.2.10. fəaliyyət proseslərində lazım olan və təqdim olunan sənədləşdirilmiş informasiya (sənədlərin, qeydlərin) resurslarının və onların reyestrinin mühafizə hədləri.

3. İnformasiya təhlükəsizliyinə təhdidlərə aid və təhdid sxeminə uyğun daxil edilən məlumatlar:

3.1. təhdid, təhdidin kateqoriyası və mahiyyəti;

3.2. təhdidin pozduğu tələb (norma, mühit) və prinsip;

3.3. təhdidin pozduğu tələbin mənbəyi (normativ hüquqi akt, standart, müqavilə, öhdəlik, qabaqcıl təcrübə və praktik tələbat);

3.4. təhdidin pozduğu tələbin qoyulduğu fəaliyyət sahəsi (fəaliyyətin keyfiyyətinə və davamlılığına, risklərin emalına, İTİS üzrə əməkdaşlıq və koordinasiyaya, İKT layihələrə, rəqəmsal xidmətlərə, sənədləşdirilmiş informasiya dövriyyəsinə, hüquqi məsləhət xidmətlərinə, fiziki təhlükəsizliyə, kadrlarla təminata, mal və xidmətlərlə təchizata, insidentlərin həllinə, fəaliyyətin auditinə və fəaliyyətin davamlı yaxşılaşdırılmasına);

3.5. milli informasiya məkanında təhlükəsizliyə yönələn təhdidlər;

3.6. informasiyanın təhlükəsizlik (tamlıq, əlçatanlıq, konfidensiallıq və mötəbərlilik) xassələrinin pozulmasına yönələn təhdidlər;

3.7. qurumların informasiya məkanlarında İTİS-yə aid təşkilati idarəetmə (planlaşdırma, təminetmə, nəzarət, təkmilləşdirmə) alətlərinin mükəmməlliyinə və davamlılığına yönələn təhdidlər;

3.8. xidməti fəaliyyətin səmərəliliyinə, davamlılığına və informasiya təhlükəsizliyinə tətbiq olunan ümumi və xüsusi prinsiplərin pozulmasına yönələn təhdidlər;

3.9. İTİS-yə aid texniki idarəetmə (texniki xidmətlərə, İKT sistemlərə, proqram, texniki və mühəndis təminatı) alətlərinin etimadlığına, yetərliyinə və yararlığına yönələn təhdidlər;

3.10. insan kapitalına yönələn təhdidlər;

3.11. fiziki mühafizənin texniki idarəetmə alətlərinin yetərliyinə və yararlığına yönələn təhdidlər;

3.12. təhdidin mənbəyi (kənardan, daxildən);

3.13. təhdidin ciddilik dərəcəsi (çox aşağı, aşağı, orta, yüksək, kritik);

3.14. təhdidin ehtimal dərəcəsi (çox aşağı: 01–20 faiz, aşağı: 21–40 faiz, orta: 41–60 faiz, yüksək: 61–80 faiz, kritik: 81–99 faiz);

3.15. təhdidin məqsədi, təyinatı (təhrifetmə, oğurluq, açıqlama, mane olma, müdaxilə, nasazlıq, səlahiyyəti aşma və s.);

3.16. təhdidin ünvan obyekti (struktur, infrastruktur komponenti, konfiqurasiya parametri, proses və subyekt);

3.17. təhdidin məqsədyönlülük xarakteri (qərəzli, təsadüfi, axın üzrə və s.);

3.18. təhdidin ünvanlandığı obyektdə (aktivdə) istifadə olunan uyğunsuzluq;

3.19. uyğunsuzluğun ciddilik dərəcəsi (az, orta, yüksək, çox yüksək, kritik, fövqəladə);

3.20. təhdidin reallaşma texnologiyası (üsulu, vasitəsi);

3.21. təhdiddən yarana bilən fəsad.

4. İnformasiya təhlükəsizliyinə fəsadlara aid daxil edilən məlumatlar:

4.1. fəsad, fəsadın mahiyyəti;

4.2. fəsadın kateqoriyası (qərarvermə, icraetmə, nəzarətetmə, yaxşılaşdırma);

4.3. fəsadın növü (fəaliyyət davamlılığının pozulması, reputasiyanın azalması, normativ tələbin pozulması, öhdəliyin pozulması, işçi heyətə zərər, texnoloji gerilik, maliyyə zərəri və aktivin itkisi);

4.4. fəsadın ciddilik dərəcəsi (çox aşağı, aşağı, orta, yüksək, kritik);

4.5. fəsadın ehtimal dərəcəsi (çox aşağı: 01–20 faiz, aşağı: 21–40 faiz, orta: 41–60 faiz, yüksək: 61–80 faiz, kritik: 81–99 faiz).

5. İnformasiya təhlükəsizliyinə uyğunsuzluqlara aid daxil edilən məlumatlar:

5.1. uyğunsuzluq, uyğunsuzluğun mahiyyəti;

5.2. uyğunsuzluğun kateqoriyası (boşluq, nəzarətsizlik, zəiflik və s.);

5.3. uyğunsuzluğun ünvan obyekti (struktur, infrastruktur komponenti, konfiqurasiya parametri, proses və subyekt);

5.4. uyğunsuzluğun ciddilik dərəcəsi (çox aşağı, aşağı, orta, yüksək, kritik).

6. Risklərin emal variantlarına uyğun mühafizə üsullarına və vasitələrinə aid məlumatlar:

6.1. risklərin emalı üzrə üsullara aid məlumatlar:

6.1.1. təhdiddə istifadə oluna bilən uyğunsuzluqlara yol verməyərək uyğunsuzluqları aşkarlayıb aradan qaldırmaq, təhdidin ünvanı olan aktivi bloklamaq üsulları;

6.1.2. təhdiddə istifadə oluna bilən uyğunsuzluqları qurumun riskgötürmə qabiliyyəti daxilində qəbul edə biləcəyi riskin ölçüsünə uyğun səviyyəyədək azaltmaq, fəsadlar yaranan aktivləri həmin səviyyəyə uyğun bərpa etmək və ehtiyat resurslarla əvəzləmək üsulları;

6.1.3. təhdidin təsirini, fəsadların aradan qaldırılmasını, məqbul vəziyyətin bərpasını başqa tərəfə, ünvana ötürmək və fəsadlar yaranan aktivlərin digər resurslarla əvəzlənməsini sığortaya yönləndirmək üsulları;

6.1.4. təhdid və fəsadla barışmaya aid üsullar;

6.1.5. reallaşmış risklərə – insidentlərə cavabvermə üzrə “aşkarlama”, “bildiriş, xəbərvermə”, “müşahidə, izləmə”, “qiymətləndirmə”, “bloklama”, “bərpaetmə”, “dəyişiklik aparılma”, “yeniləmə”, “təkmilləşdirmə”, “ehtiyat varianta keçmə”, “əvvəlki vəziyyətə geri qaytarılma”, “sübut - dəlil toplama”, “anti-böhran” variantlara uyğun olan üsullar və alqoritmlər.

6.2. Risklərin emalı üzrə vasitələrə aid məlumatlar:

6.2.1. risklərin emal üsullarının proqram, proqram-texniki və texniki təminat vasitələri, o cümlədən bu vasitələrin funksional təyinatları, konfiqurasiya komponentləri və parametrləri, onlara aid imkan və etimadlıq hədləri;

6.2.2. risklərin emalının təminat vasitələri üçün yeni və “ağıllı” texnologiyalar, o cümlədən süni intellektə əsaslanan həllər (“big data”, “threat intelligence” , “link analysis”, “E2E: End-to-end”, “UEBA: User and Entity Behavior Analytics”, “deep learning”, “DLP: Data Leak Prevention”, “corpus linguistics”, “SIEM: Security information and event management”, “OODA loop: demand, Observe, Orient, Decide, Act, delivery”, “SOAR: Security Orchestration, Automation and Response” və s.), onların tətbiq sahələri, onlara aid texniki şərtlər və tələblər.

_____