DOI: https://doi.org/10.36719/2789-6919/56/194-199

**Hüseyn Əliyev**
Azərbaycan Texniki Universiteti
https://orcid.org/0009-0003-6658-5144
huseynali1119@gmail.com

# Müəssisələrdə informasiya təhlükəsizliyi siyasətlərinin təkmilləşdirilməsində Data Classification və DLP inteqrasiyasının rolu

**Xülasə**

Rəqəmsal transformasiya proseslərinin sürətlənməsi ilə paralel olaraq müəssisələrdə məlumatların həcmi, müxtəlifliyi və biznes dəyəri kəskin şəkildə artmışdır. Bu artım informasiya resurslarının yalnız texnoloji aktiv kimi deyil, eyni zamanda, strateji və hüquqi məsuliyyət daşıyan obyektlər kimi idarə olunmasını zəruri edir. Müasir təşkilatlarda məlumat axınlarının bulud platformaları, mobil qurğular, korporativ şəbəkələr və üçüncü tərəf xidmətləri arasında sürətlə hərəkət etməsi məlumat sızmaları, icazəsiz ötürmələr və daxili təhlükələr kimi risklərin aktuallığını daha da artırır. Empirik araşdırmalar göstərir ki, məlumat sızması insidentlərinin əhəmiyyətli hissəsi texniki boşluqlarla yanaşı, siyasətlərin əməliyyat mühitində effektiv icra olunmaması və insan faktorunun təsiri ilə bağlıdır.

Bu kontekstdə Data Classification (məlumatların təsnifatı) və Data Loss Prevention (DLP) texnologiyalarının inteqrasiyası informasiya təhlükəsizliyi siyasətlərinin əməliyyatlaşdırılması üçün perspektivli yanaşma kimi çıxış edir. Data Classification məlumatın biznes dəyəri və həssaslıq səviyyəsinə görə strukturlaşdırılmış şəkildə identifikasiyasını təmin edərkən, DLP mexanizmləri bu kontekstə uyğun olaraq məlumat axınlarının nəzarətini, bloklanmasını və monitorinqini həyata keçirir. İnteqrasiya olunmuş yanaşma təhlükəsizlik siyasətlərinin risk-əsaslı, ölçülə bilən və auditə yararlı mexanizmlərə çevrilməsinə imkan yaradır.

***Açar sözlər:*** *Data Classification, DLP, informasiya təhlükəsizliyi siyasəti, risklərin idarə edilməsi, False positive, Metadata*

**Huseyn Aliyev**
Azerbaijan Technical University
https://orcid.org/0009-0003-6658-5144
huseynali1119@gmail.com

# The Role of Data Classification and DLP Integration in Improving Information Security Policies in Enterprises

**Abstract**

In parallel with the acceleration of digital transformation processes, the volume, diversity and business value of data in enterprises have increased dramatically. This growth necessitates the management of information resources not only as technological assets, but also as objects with strategic and legal responsibilities. In modern organizations, the rapid movement of data flows between cloud platforms, mobile devices, corporate networks, and third-party services further increases the relevance of risks such as data leaks, unauthorized transfers, and insider threats. Empirical studies show that a significant proportion of data leakage incidents are related to technical gaps, as well as ineffective implementation of policies in the operational environment and the influence of the human factor.

In this context, the integration of Data Classification and Data Loss Prevention (DLP) technologies acts as a promising approach for operationalizing information security policies.

While Data Classification provides structured identification of information according to business value and sensitivity level, DLP mechanisms control, block and monitor data flows in accordance with this context. An integrated approach allows security policies to be transformed into risk-based, measurable and auditable mechanisms.

***Keywords:*** *Data Classification, DLP, information security policy, risk management, False positive, Metadata*

## Giriş

Müəssisələrdə informasiya təhlükəsizliyi siyasətləri (ITS) praktikada iki əsas sualı cavablandırmalıdır:

1. Hansı məlumatı nə dərəcədə qoruyuruq?
2. Bu qorunmanı bütün kanallarda necə icra edirik?

Bu iki sualın ən ideal cavabı Data Classification (məlumatların təsnifatı) ilə DLP-nin (Data Loss/Leakage Prevention - məlumat itkisinin/sızmasının qarşısının alınması) inteqrasiyasından keçir. Data Classification müəssisə üçün məlumatın dəyərini, həssaslığını və risk səviyyəsini ölçülə bilən sxemə çevirir. ISO/IEC 27002:2022-də təsnifatın CIA tələblərinə əsaslanan sxem kimi qurulması vurğulanır (Alneyadi və b., 2016; Alneyadi və b., 2014). DLP isə həmin təsnifatın tələb etdiyi nəzarəti real əməliyyata çevirərək e-poçt, şəbəkə, endpoint, SaaS və s. kanallarda məlumatın icazəsiz istifadəsini və ötürülməsini aşkarlayıb dayandırmağı hədəfləyir.

İnteqrasiyanın rolunu anlamaq üçün hər bir komponentin fərdi funksiyasına nəzər salmaq lazımdır:

Data Classification (Məlumatların Təsnifatı): Məlumatların həssaslıq dərəcəsinə və biznes dəyərinə görə (məsələn: İctimai, Daxili, Məxfi, Ciddi Məxfi) etiketlənməsi prosesidir. Bu proses sənədlərin metadatasında (metadata) xüsusi izlər buraxaraq, həmin faylın kimliyini və dəyərini müəyyən edir.

DLP (Data Loss Prevention): Həssas məlumatların icazəsiz istifadəsini, ötürülməsini və ya sızmasını aşkar edən və qarşısını alan texnologiyalar toplusudur. DLP şəbəkə trafikini, son nöqtələri (endpoint) və bulud mühitlərini davamlı olaraq monitorinq edir.

*İnteqrasiyanın Mexanizmi: "Gözübağlı" DLP-dən "Ağıllı" DLP-yə Keçid.* Yalnız DLP sisteminə istinad etmək əksər hallarda yüksək həcmdə "yalançı pozitiv" (false positive) xəbərdarlıqların formalaşmasına gətirib çıxarır. Bunun əsas səbəbi ondan ibarətdir ki, təsnifat mexanizmi olmadıqda DLP həssaslığın kontekstini qiymətləndirmək qabiliyyətindən məhrum olur və əsasən açar sözlər, requlyar ifadələr (RegEx) və ya strukturlaşdırılmış məlumat şablonlarına (məsələn, kredit kartı nömrələrinin formatları, şəxsiyyət nömrələri və s.) əsaslanaraq reaksiya verir. Nəticədə, kontekstual olaraq risk daşımayan məlumat ötürmələri də təhlükə kimi qiymətləndirilir, bu isə həm təhlükəsizlik komandalarının üzərinə əlavə əməliyyat yükü yaradır, həm də real insidentlərin səs-küy içində "itməsi" riskini artırır. Data Classification ilə inteqrasiya olunduqda isə DLP qərarvermə mexanizmini yalnız sintaktik uyğunluqlara deyil, məlumatın biznes dəyərinə və həssaslıq səviyyəsinə əsaslandırır. Bu da həm yanlış "pozitivlərin" azalmasına, həm də real risklərin daha dəqiq prioritetləşdirilməsinə imkan verir.

**Tədqiqat**

İnteqrasiya necə işləyir? Data Classification mexanizmi sənədlərə həm vizual səviyyədə (məsələn, "Ciddi Məxfi" işarəsi, watermark və ya bannerlər), həm də texniki səviyyədə maşınoxunaqlı metadata əlavə edir. Bu metadata sənədin yaradıldığı andan etibarən onun bütün həyat dövrü (yaradılma, saxlanma, ötürülmə, paylaşılma və arxivləşdirmə mərhələləri) boyunca müşayiət olunur və təhlükəsizlik nəzarət mexanizmləri üçün kontekstual informasiya rolunu oynayır.

DLP sistemləri inteqrasiya mühitində faylı və ya məlumat axınını analiz edərkən yalnız məzmun səviyyəsində mürəkkəb və hesablama baxımından bahalı mətn analizi, RegEx uyğunluğu və ya şablon axtarışları aparmaq əvəzinə, birbaşa faylın metadata qatında mövcud olan təsnifat etiketlərini oxuyur. Bu yanaşma DLP-nin qərarvermə mexanizmini kontekstual məlumatla zənginləşdirir, performans yükünü azaldır və yanlış pozitivlərin (false positive) sayının minimallaşdırılmasına şərait yaradır.

Məsələn əgər istifadəçi tərəfindən bir sənəd "Ciddi Məxfi" (Strictly Confidential) kateqoriyası ilə etiketlənmişdirsə və həmin sənədin şəxsi e-poçt ünvanına ötürülməsi cəhdi baş verirsə, DLP sistemi ilkin mərhələdə sənədin metadata qatındakı təsnifat etiketini identifikasiya edir. Bu kontekstual göstəriciyə əsaslanaraq, məzmunun dərin semantik analizinə ehtiyac qalmadan əvvəlcədən müəyyən edilmiş təhlükəsizlik siyasətini işə salır və ötürülmə əməliyyatını avtomatik olaraq bloklayır (və ya alternativ olaraq şifrələmə, xəbərdarlıq və insident qeydi mexanizmlərini aktivləşdirir).

Bu cür inteqrasiya yanaşması təhlükəsizlik nəzarətinin reaktiv və məzmun-asılı mexanizmlərdən proaktiv və kontekst-əsaslı idarəetmə modelinə transformasiyasını təmin edir. Nəticədə, informasiya təhlükəsizliyi siyasətləri yalnız normativ sənəd səviyyəsində qalmır, real əməliyyat mühitində avtomatlaşdırılmış, ölçülə bilən və auditə yararlı nəzarət mexanizmlərinə çevrilir.

Data Classification və DLP inteqrasiyasının metodik olaraq əsaslandırılmış inteqrasiya siyasətləri praktiki tətbiqində yaranan boşluqların aradan qaldırılmasında həlledici rol oynayır. Doğru strukturlaşdırılmış inteqrasiya aşağıdakı "siyasət boşluqlarını" operasionallaşdıraraq aradan qaldırır:

- *Siyasət-texnologiya uyğunsuzluğu:* Siyasətdə "məxfi" kimi təsnifləndirilən məlumatın informasiya sistemlərində avtomatik identifikasiya olunmaması və vahid nəzarət qaydalarının bütün kommunikasiya kanallarında ardıcıl tətbiq edilməməsi nəticə etibarilə siyasət-icra uyğunsuzluğunu dərinləşdirir və məlumat sızması risklərini əhəmiyyətli dərəcədə artırır. NIST DLP yanaşmasının "proqram + siyasət" olması və idarəetmə komponentini vacib sayması bunu təsdiqləyir (Center for Internet Security, 2021; International Organization for Standardization, 2022).

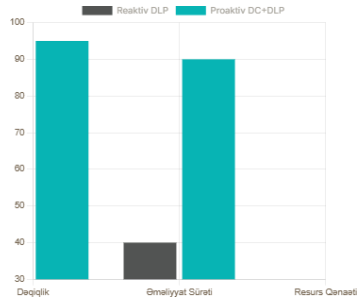
- *Komplayansın ölçülə bilməməsi:* Komplayansın ölçülə bilməməsi problemi ondan irəli gəlir ki, GDPR kimi tənzimləyici rejimlər riskə uyğun texniki və təşkilati tədbirlərin tətbiqini tələb etsə də, bu tələblərin əməliyyat səviyyəsində ölçülə bilən göstəricilərə çevrilməsi əksər hallarda təmin olunmur. Data Classification və DLP inteqrasiyası həmin tələbləri ölçülə bilən KPI-lar vasitəsilə operasionallaşdıraraq audit üçün obyektiv sübut bazasının formalaşdırılmasına imkan yaradır.

- *Bulud və uzaq iş mühitində parçalanma:* Müasir DLP yanaşmaları endpoint, bulud və şəbəkəni birlikdə əhatə etməlidir (cloud DLP, endpoint DLP, network DLP kimi) (ENISA, 2018; ENISA, 2016).

*Metodologiyaların Müqayisəsi: Reaktiv və Proaktiv Müdafiə.* Ənənəvi, "məzmun əsaslı" DLP (Data Loss Prevention) sistemləri əsasən mürəkkəb riyazi alqoritmlərə və əvvəlcədən müəyyən edilmiş şablonlara (pattern-based yanaşma) əsaslanır. Bu yanaşma konteksti tam nəzərə almadığı üçün yüksək səviyyədə "False Positive" halları yaradır. Nəticədə, təhlükəsizlik komandaları real riskləri müəyyənləşdirmək üçün artıq sayda insidenti manual şəkildə təhlil etməli olur və bu da əməliyyat yükünü artırır (National Institute of Standards and Technology, 2012; International Organization for Standardization, 2022).

DC (Domain Controller) ilə inteqrasiya olunmuş, "kontekst əsaslı" proaktiv DLP sistemləri isə istifadəçi davranışı, rol, cihaz, zaman və əməliyyat konteksti kimi əlavə faktorları analiz edərək daha dəqiq qərar mexanizmi formalaşdırır. Bu yanaşma:

- Yalançı həyəcanların sayını əhəmiyyətli dərəcədə azaldır;
- Real təhlükələrin prioritetləşdirilməsini təmin edir;
- Təhlükəsizlik əməliyyatlarının effektivliyini optimallaşdırır.




**Şəkil 1.** Metodoloji Müqayisə

Əsas göstəricilər:

- İnsident Analizi Sürəti: 4.5 dəfə artım;
- Resurs İsrafı (Triage Prosesi): 75% azalma.

Bu nəticələr göstərir ki, reaktiv, məzmun əsaslı modellərlə müqayisədə proaktiv və kontekst əsaslı yanaşma həm əməliyyat səmərəliliyini artırır, həm də təhlükəsizlik komandalarının vaxt və resurslarını daha effektiv idarə etməsinə imkan yaradır (Kumaresan, 2014; KPMG International, 2014).

*İnformasiya Təhlükəsizliyi Siyasətlərinə Təsiri və Təkmilləşdirilməsi.* Data Classification və DLP sistemlərinin inteqrasiyası müəssisələrdə informasiya təhlükəsizliyi siyasətlərinin normativ xarakterdən çıxarılaraq əməliyyat mühitində ölçülə bilən və icra oluna bilən mexanizmlərə çevrilməsinə şərait yaradır. Empirik tədqiqatlar göstərir ki, məlumat sızmalarının əhəmiyyətli hissəsi (təxminən 60-70%-i) ya yanlış konfiqurasiya, ya da insan səhvləri ilə əlaqədardır ki, bu da siyasət-icra uyğunsuzluğunun praktiki nəticələrini nümayiş etdirir. Bu baxımdan inteqrasiya olunmuş yanaşma təhlükəsizlik siyasətlərinin effektivliyini bir neçə fundamental istiqamətdə artırır:

*A. Siyasətlərin Dəqiqliyinin və Effektivliyinin Artması.* Ənənəvi olaraq açar sözlərə və sintaktik uyğunluqlara əsaslanan DLP qaydaları müxtəlif şöbələr və layihələr kontekstində fərqli semantik mənalar kəsb edir. Nəticədə, təhlükəsizlik mexanizmləri kontekstual həssaslığı düzgün qiymətləndirmir və yüksək həcmdə "yalançı pozitiv" (false positive) xəbərdarlıqları formalaşdırır. Praktiki müşahidələr göstərir ki, kontekstual təsnifat olmadan işləyən DLP sistemlərində yaranan insident bildirişlərinin 30-50%-i real təhlükə ilə əlaqəli olmur, bu isə təhlükəsizlik komandalarının resurslarını səmərəsiz şəkildə istifadə etməsinə gətirib çıxarır.

Data Classification mexanizmlərinin tətbiqi ilə DLP siyasətləri məlumatın biznes dəyərinə və həssaslıq səviyyəsinə uyğun olaraq kontekstual əsasda icra olunur. Bu yanaşma yanlış pozitivlərin əhəmiyyətli dərəcədə azalmasına, real insidentlərin isə daha yüksək prioritetlə emal edilməsinə imkan verir (National Institute of Standards and Technology, 2020). Nəticədə, təhlükəsizlik siyasətləri "hamını və hər şeyi eyni qayda ilə yoxla" prinsipi əsasında deyil, riskə uyğunlaşdırılmış "etiketə əsaslanan nəzarət" modeli çərçivəsində tətbiq olunur ki, bu da siyasətlərin həm dəqiqliyini, həm də əməliyyat effektivliyini artırır.

*B. İstifadəçi Məsuliyyətinin və Təhlükəsizlik Mədəniyyətinin Formalaşması.* Məlumat sızmalarının əhəmiyyətli hissəsinin insan faktoru ilə əlaqəli olması informasiya təhlükəsizliyi siyasətlərində davranış yönümlü mexanizmlərin vacibliyini ön plana çıxarır. Müasir tədqiqatlar göstərir ki, kibertəhlükəsizlik insidentlərinin təxminən 70-80%-i birbaşa və ya dolayı yolla insan səhvləri (məsələn, yanlış paylaşım, zəif parol istifadəsi, diqqətsizlik) ilə bağlıdır. Data Classification prosesi istifadəçiləri yaratdıqları və paylaşdıqları məlumatın dəyəri və həssaslıq səviyyəsi barədə reflektiv düşünməyə təşviq edir və bu, təhlükəsizlik mədəniyyətinin formalaşmasında davranış dəyişikliklərinə səbəb olur.

DLP mexanizmləri isə yalnız məhdudlaşdırıcı texniki alət rolunu deyil, eyni zamanda, öyrədici və profilaktik funksiya daşıyır. Məsələn, istifadəçi məxfi kateqoriyaya aid sənədi USB daşıyıcıya köçürməyə cəhd etdikdə, sistemin yalnız əməliyyatı bloklaması deyil, həm də siyasəti izah edən kontekstual xəbərdarlıq (pop-up notification) göstərməsi istifadəçi davranışlarının tədricən korrektə olunmasına şərait yaradır. Davranış yönümlü təhlükəsizlik yanaşmaları ilə texniki nəzarətin sintezi uzunmüddətli perspektivdə təhlükəsizlik mədəniyyətinin institusionallaşmasına və insidentlərin sayının azalmasına töhfə verir (Microsoft, 2026; National Institute of Standards and Technology, 2018).

*C. Qanunvericiliyə və Standartlara Uyğunluq (Compliance).* GDPR, ISO/IEC 27001, PCI-DSS və digər beynəlxalq standartlar, habelə yerli normativ-hüquqi aktlar təşkilatlardan riskə uyğun texniki və təşkilati tədbirlərin tətbiqini, mütəmadi monitorinq və audit mexanizmlərinin qurulmasını tələb edir. Praktikada uyğunluq problemlərinin əsas səbəblərindən biri siyasətlərin ölçülə bilən göstəricilərə çevrilməməsidir. Statistik hesabatlara əsasən, böyük təşkilatlarda uyğunluq pozuntularının təxminən 40%-i adekvat monitorinq mexanizmlərinin olmaması ilə əlaqələndirilir.

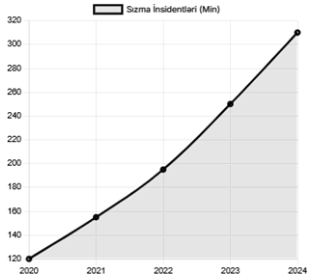
Nəzəri olaraq inteqrasiyanın faydalarını və siyasətlərə müsbət təsirini müzakirə etdikdən sonra, gəlin bunun gündəlik əməliyyatlarda necə fərq yaratdığına baxaq. İnformasiya təhlükəsizliyi komandasının iş yükünü və qərarvermə prosesini daha aydın qavramaq üçün, ənənəvi olaraq təsnifat

olmadan işləyən "tənha" DLP sistemi ilə bu iki həlqənin birləşdiyi inteqrasiya olunmuş mühitin birbaşa müqayisəsinə nəzər salaq. Bu fərqlər, doğru texnoloji sinergiyanın vaxta və resurslara necə qənaət etdiyini konkretləşdirir:

**Cədvəl 1.**
Təsnifatsız və İnteqrasiya Olunmuş Sistemlərin Müqayisəsi

| Xüsusiyyət | Yalnız DLP (Təsnifat olmadan) | Data Classification + DLP İnteqrasiyası |
|---|---|---|
| Qərarvermə Əsası | Məzmun analizi, açar sözlər, RegEx | Sənədin metadatası və istifadəçi etiketi |
| Yalançı Pozitivlər | Çox yüksək (əməliyyat yükü yaradır) | Minimum (dəqiq hədəfləmə təmin edilir) |
| Sistem Performansı | Ağır (davamlı mətn skan edilməsi tələb olunur) | Yüngül (yalnız metadata oxunur) |
| İstifadəçi Təcrübəsi | Passiv (istifadəçi nəyin səhv olduğunu bilmir) | Aktiv (istifadəçi sənədi təsnif edir və qaydaları öyrənir) |

Müasir rəqəmsal ekosistemlərdə korporativ şəbəkə sərhədlərinin aradan qalxması (de-seqmentasiya) və hibrid infrastruktur modellərinin geniş yayılması ənənəvi təhlükəsizlik yanaşmalarının effektivliyini əhəmiyyətli dərəcədə azaldıb. Mövcud təhlükə mühitində məlumat mərkəzli təhlükəsizlik (Data-Centric Security) modeli strateji əhəmiyyət daşıyır (Ross və b., 2020). Tədqiqatlar göstərir ki, DLP (Data Loss Prevention) həllərinin aşağı effektivliyi əksər hallarda texnoloji çatışmazlıqlardan deyil, korporativ məlumat taksonomiyasının düzgün müəyyən edilməməsindən qaynaqlanır. Məlumatların sistemli şəkildə təsnif edilmədiyi mühitlərdə DLP mexanizmləri "kor nöqtələr" formalaşdırır ki, bu da kritik aktivlərin qeyri-qanuni ekzfiltrasiyası riskini əhəmiyyətli dərəcədə artırır.




**Şəkil 1.** Qlobal məlumat sızması insidentlərinin dinamik analizi

Aparılmış nəzəri təhlil və praktik tətbiq ssenarilərinin müqayisəli qiymətləndirilməsi Data Classification və Data Loss Prevention (DLP) texnologiyalarının inteqrasiyasının müəssisələrdə informasiya təhlükəsizliyi siyasətlərinin effektivliyinə əhəmiyyətli müsbət təsir göstərdiyini nümayiş etdirmişdir. Tədqiqatın nəticələri göstərir ki, inteqrasiya olunmuş yanaşma siyasətlərin normativ xarakterdən çıxarılaraq əməliyyat səviyyəsində avtomatlaşdırılmış nəzarət mexanizmlərinə çevrilməsinə imkan yaradır və bununla da siyasət-icra uyğunsuzluğunu əhəmiyyətli dərəcədə azaldır.

## Nəticə

Empirik müşahidələr və mövcud tədqiqatların nəticələrinin ümumiləşdirilməsi əsasında müəyyən edilmişdir ki, təsnifat etiketləri ilə zənginləşdirilmiş DLP mexanizmlərinin tətbiqi "yalançı pozitiv" insident bildirişlərinin sayını əhəmiyyətli dərəcədə azaldır, real risklərin isə daha yüksək prioritetlə aşkar olunmasına şərait yaradır. Bu, təhlükəsizlik komandalarının əməliyyat yükünü optimallaşdırır

və resursların daha səmərəli bölüşdürülməsinə imkan verir. Eyni zamanda, kontekst-əsaslı nəzarət mexanizmləri məlumat axınlarının daha dəqiq monitorinqini təmin etməklə insidentlərin erkən mərhələdə aşkarlanması ehtimalını artırır.

Tədqiqat nəticələri həmçinin göstərir ki, inteqrasiya olunmuş model informasiya təhlükəsizliyi mədəniyyətinin formalaşmasına töhfə verir. Data Classification prosesində istifadəçilərin məlumatın həssaslıq səviyyəsini şüurlu şəkildə qiymətləndirməsi və DLP mexanizmlərinin kontekstual xəbərdarlıqlar vasitəsilə davranışları korrektə etməsi insan faktoru ilə bağlı risklərin azalmasına səbəb olur. Bu yanaşma uzunmüddətli perspektivdə təhlükəsizlik siyasətlərinin yalnız texniki nəzarət mexanizmi deyil, təşkilati davranış modeli kimi qəbul olunmasına şərait yaradır.

Ümumilikdə, əldə olunan nəticələr göstərir ki, Data Classification və DLP inteqrasiyası informasiya təhlükəsizliyi siyasətlərinin effektiv icrası üçün texnoloji və metodoloji baxımdan əsaslandırılmış, praktik dəyəri yüksək olan yanaşmadır. Bu yanaşmanın tətbiqi müəssisələrin kibertəhlükəsizlik risklərinə qarşı dayanıqlığını gücləndirir, tənzimləyici uyğunluq səviyyəsini artırır və məlumatların strateji aktiv kimi qorunmasını təmin edən davamlı təhlükəsizlik arxitekturasının formalaşmasına töhfə verir.

## Ədəbiyyat

1. Alneyadi, S., Sithirasenan, E. & Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. *Journal of Network and Computer Applications, 62*, 137–152.
2. Alneyadi, S., Sithirasenan, E. & Muthukkumarasamy, V. (2014). *A semantics-aware classification approach for data leakage prevention*. In W. Susilo, Y. Mu (Eds.), Information Security and Privacy (ACISP 2014) (pp. 413–421). Springer.
3. Center for Internet Security. (2021). *CIS Critical Security Controls (v8): Control 3 - Data Protection*.
4. European Union Agency for Cybersecurity (ENISA). (2016). *Guidelines for SMEs on the security of personal data processing*.
5. European Union Agency for Cybersecurity (ENISA). (2018). *Handbook on security of personal data processing*.
6. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security management systems — Requirements*.
7. International Organization for Standardization. (2022). *ISO/IEC 27002:2022 — Information security controls*.
8. International Organization for Standardization. (2022). *ISO/IEC 27005:2022 — Guidance on managing information security risks*.
9. KPMG International. (2014). *Data loss prevention: Protecting your data from enemy lines*.
10. Kumaresan, N. (2014). Key considerations in protecting sensitive data leakage using data loss prevention tools. *ISACA Journal*.
11. Microsoft. (2026). *Use sensitivity labels as conditions in DLP policies*. Microsoft Learn.
12. National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (SP 800-30 Rev. 1).
13. National Institute of Standards and Technology. (2018). *Risk Management Framework for information systems and organizations* (SP 800-37 Rev. 2).
14. National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (SP 800-53 Rev. 5).
15. Ross, R., Pillitteri, V., Dempsey, K., Riddle, M. & Guissanie, G. (2020). *Protecting controlled unclassified information in nonfederal systems and organizations* (SP 800-171 Rev. 2).

Daxil oldu: 04.12.2025
Qəbul edildi: 06.03.2026