ISSN 3060-4567

DLP TIZIMLARINING TASHKILOT XAVFSIZLIGIDAGI O'RNI

Andijon davlat texnika instituti talabasi

Tojmetov Adhambek Dilshod O'g'li

Andijon davlat texnika instituti ATT kafedrasi assisenti

Xoshimova Maftunabonu Xoshimjon Qizi

Andijon davlat texnika instituti talabasi

Dadajonov Baxodirjon Abdurahim O'g'li

Andijon davlat texnika instituti talabasi

Jo'rayev Biloliddin Sherali O'g'li

Anotatsiya: *Mazkur maqolada tashkilotlarda axborot xavfsizligini ta'minlashda DLP (Data Loss Prevention) tizimlarining tutgan o'rni nazariy manbalar asosida tahlil qilinadi. DLP texnologiyalari ruxsatsiz kirishlarning oldini olish, ma'lumotlar tarqalishini cheklash va axborot oqimini monitoring qilishda asosiy vosita hisoblanadi. Maqolada DLP tizimlarining asosiy komponentlari, ularning funktsional imkoniyatlari, joriy etish bosqichlari va ularni tashkilot infratuzilmasiga moslashtirish bo'yicha yondashuvlar yoritiladi. Xorijiy tajriba va xalqaro standartlar asosida olingan nazariy tahlillar DLP tizimlarining axborot xavfsizligi strategiyasidagi ahamiyatini ko'rsatadi.*

Abstract: *This article theoretically examines the role of Data Loss Prevention (DLP) systems in organizational information security. DLP technologies are considered a primary tool to prevent unauthorized access, restrict data leakage, and monitor the flow of information within networks. The paper outlines the core components of DLP systems, their functionalities, implementation stages, and approaches to integrating them into an organization's infrastructure. Through theoretical analysis based on international experience and global standards, the study highlights the significance of DLP systems in building a strong cybersecurity strategy.*

ISSN 3060-4567

Kalit so‘zlar:*DLP tizimi, Axborot xavfsizligi, Ma’lumotlarni himoya qilish, Ma’lumotlar oqimi monitoring, Ruxsatsiz kirishni oldini olish,Tashkilot xavfsizligi, Texnologik integratsiya,Xalqaro standartlar,DLP strategiyasi,O‘zbekiston tajribasi.*

Keywords:*DLP system,Information security,Data protection,Data flow monitoring,Unauthorized access prevention,Organizational security,Technological integration,International standards,DLP strategy,Uzbekistan experience.*

Raqamli transformatsiya zamonida tashkilotlar o‘z faoliyatini tobora ko‘proq axborot resurslariga tayanib amalga oshirmoqda. Bunda ma’lumotlar — eng muhim aktivga aylanmoqda. Ma’lumotlar sizib chiqishining oldini olish, ayniqsa moliyaviy, sog‘liqni saqlash, davlat boshqaruvi kabi sohalarda, nafaqat texnik, balki strategik muammoga aylangan. Shu nuqtayi nazardan, ma’lumotlarni yo‘qotishdan himoya qilish texnologiyalari — Data Loss Prevention (DLP) tizimlari — zamonaviy axborot xavfsizligi siyosatining ajralmas bo‘lagiga aylangan.Mazkur maqolada DLP tizimlarining nazariy asoslari, ularning texnologik imkoniyatlari, amaliy qo‘llanilishi va O‘zbekiston sharoitidagi ahamiyati xalqaro tajribalar asosida tahlil qilinadi. Ushbu yondashuv orqali mavzu chuqur va izchil tahlil etiladi.

DLP tizimining nazariy asosi: maqsad, ehtiyoj va rivojlanish sabablari.Axborot xavfsizligiga oid ilk yondashuvlar asosan perimetr (tashqi tahdid) xavfsizligini ta'minlashga yo‘naltirilgan edi. Ammo so‘nggi yillarda tahdidlar tabiati o‘zgardi: tashkilot ichidan chiqayotgan ma’lumotlar oqimi tahdidlarning asosiy manbai sifatida qaralmoqda. Aynan shunday ichki tahdidlar va ma’lumotlar sizib chiqishining oldini olish ehtiyoji DLP tizimlarining rivojlanishiga turtki bo‘ldi.DLP tizimi — bu nafaqat monitoring, balki proaktiv tarzda ma’lumotlarning harakatini boshqarish, siyosat asosida cheklash, xatti-harakatlarni analiz qilish va huquqbuzarliklarning oldini olish vositasidir. Bu tizim foydalanuvchining xatti-harakatlarini tahlil qilib, ma’lumotlar bilan qanday munosabatda bo‘layotganini aniqlaydi.

Shu nuqtada DLP konsepsiyasi ikki asosiy tamoyilga tayangan holda shakllanadi:

ISSN 3060-4567

1. Ma’lumot markaziga asoslangan yondashuv – Ma’lumotlar eng qimmat aktiv sifatida e’tirof etiladi.

2. Xatti-harakatga asoslangan yondashuv – Har qanday noan’anaviy harakat potentsial tahdid sifatida ko‘riladi.

DLP texnologiyalarining tuzilmasi va funktsional komponentlari: Tashkilotlar uchun samarali DLP tizimi quyidagi asosiy komponentlardan iborat:

- Ma’lumotlarni aniqlash va tasniflash: Ma’lumotlar turi (moliya, shaxsiy, tijorat sirlar) asosida identifikatsiya qilinadi.
- Monitoring va nazorat: Ma’lumotlar harakati (USB, email, bulutli servislar) doimiy nazoratda bo‘ladi.
- Qoidalar va siyosatlar: Avtomatlashtirilgan cheklovlar va ogohlantirishlar tizimi tuziladi.
- Hisobot va audit: Har bir harakat yozib boriladi va tahlil qilinadi.

Bu modullar o‘zaro uzviy bog‘langan: aniqlash moduli orqali tan olingan ma’lumotlar kuzatuv moduliga o‘tadi, u esa siyosat moduliga signal yuboradi. Bu orqali real-time xavfsizlik ta’minlanadi.

DLP tizimlarining turlari: texnologik ko‘rinishlar:DLP tizimlarining asosiy 3 turi mavjud:

- Tarmoq DLP (Network DLP) – Ma’lumotlarning tashqi tarmoqqa chiqishini monitoring qiladi (email, internet, FTP).
- Endpoint DLP – Har bir foydalanuvchi qurilmasidagi harakatlar ustidan nazorat (fayl nusxalash, USB, ekran surati).
- Bulut DLP – SaaS xizmatlaridagi ma’lumotlar (Google Drive, OneDrive, Dropbox) bilan ishlovchi modullar.

Bu turlar birgalikda ishlaganda kompleks DLP yechimi shakllanadi. Zero, faqat tarmoq darajasida emas, balki foydalanuvchi darajasida ham xavfsizlikni ta’minlash talab etiladi.

DLP tizimlarining afzalliklari: xavfsizlikdan strategiyaga

DLP tizimlarining asosiy afzalliklari quyidagilardan iborat:

- Axborot oqimlarini shaffoflashtiradi – Qayerga, kim, qanday ma’lumot jo‘natayotganini ko‘rsatadi.
- Tahdidlarni oldindan aniqlaydi – Ma’lumotlarni noqonuniy tarqatish urinishlarini proaktiv aniqlaydi.
- Huquqiy javobgarlikdan himoya qiladi – Ma’lumotlar xavfsizligi qonunlariga (masalan, GDPR) moslikni ta’minlaydi.
- Ishonchli korporativ madaniyat shakllantiradi – Foydalanuvchilar ongli va ehtiyotkor bo‘lishga odatlanadi.

Demak, DLP tizimlari faqat xavfsizlik vositasi emas, balki tashkilot ichki siyosatini shakllantiruvchi vositaga aylanmoqda.O‘zbekiston tajribasi: imkoniyatlar va muammolar.O‘zbekistonda DLP texnologiyalariga bo‘lgan ehtiyoj ayniqsa bank sektori, davlat xizmatlari va ta’lim muassasalarida sezilmoqda. Bir qancha yirik banklar xorijiy DLP yechimlarini (Symantec, McAfee, Fortinet) joriy qilgan. Biroq quyidagi muammolar mavjud:

- Mahalliy mutaxassislarning yetishmasligi;
- Texnologik infrastrukturada uzilishlar;
- Maxfiylik siyosatining yetarli darajada huquqiy kafolatga ega emasligi.

Shunga qaramay, Raqamli texnologiyalar vazirligi tashabbuslari va "Raqamli O‘zbekiston — 2030" strategiyasi doirasida bu tizimlarni milliylashtirish, mahalliylashtirish bo‘yicha chora-tadbirlar olib borilmoqda.

Xulosa va tavsiyalar. Mazkur maqolada DLP tizimlarining tashkilot xavfsizligidagi o‘rni ilmiy-nazariy asosda tahlil qilindi. Quyidagi xulosalarga kelindi:

- DLP — bu faqat texnik vosita emas, balki tashkilot xavfsizlik strategiyasining markaziy komponentidir;
- Tashkilot ichida DLP tizimlari orqali xodimlarning axborotga munosabati shakllantiriladi;
- O‘zbekiston uchun DLP tizimlari kelajakda davlat va xususiy sektor axborot xavfsizligining kafolati bo‘lib xizmat qiladi.

Tavsiyalar:

1. DLP tizimlarini milliy qonunchilikka integratsiya qilish;

2. Mahalliy IT-kadrlar tayyorlashni kuchaytirish;
3. Har bir yirik tashkilotda individual DLP siyosatini ishlab chiqish.

FOYDALANILGAN ADABIYOTLAR:

1. Andress, J. (2020). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Burlington: Syngress Publishing.
2. Gartner Research. (2023). *Market Guide for Data Loss Prevention*. Stamford: Gartner Inc.
3. Symantec Enterprise. (2022). *Understanding DLP: Why Data Loss Prevention Is Crucial in Modern Enterprises*. Mountain View: Symantec Corporation.
4. Chapple, M., & Seidl, D. (2022). *CISSP Official (ISC)² Practice Tests*. Indianapolis: Wiley Publishing.
5. Kaspersky Lab. (2021). *Data Loss Prevention (DLP) Technologies: Overview and Practical Implementation*. Moscow: Kaspersky Press.
6. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi. (2024). *"Raqamli O‘zbekiston – 2030" strategiyasi*. Toshkent: MITC nashriyoti.
7. Badriddinov, A.X., & Yusupov, Sh.A. (2022). *Axborot xavfsizligi asoslari*. Toshkent: Iqtisod-Moliya nashriyoti.