УДК 004.056.5

# СИСТЕМИ МОНІТОРИНГУ ТА АУДИТУ ЗАДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВІД ВТРАТИ ДАНИХ

Бринза І.Ю., Желєзнякова В.В.
e-mail: iryna.brynza@nure.ua, e-mail: viktoriia.zheliezniakova@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна

Modern corporate data loss prevention (DLP) systems are becoming increasingly in demand as organizations need to process larger amounts of their clients' information. DLP systems are based on the creation of policies and rules for filtering outbound traffic. Their goal is to minimize the number of successful data transmissions. It has been established that the most effective protection is provided by comprehensive security systems that prevent data leaks through various channels, including email, web resources, USB devices, third-party applications, and printers.

Питання забезпечення конфіденційності, цілісності та доступності завжди залишається актуальним. Проблема захисту інформації від витоку корпоративних даних включає в себе різноманітність каналів витоку, людський фактор, інсайдерські загрози, обхід захисту та контроль доступів до обмежених даних. З кожним роком все гостріше постає питання вдосконалення систем для налаштувань обмежень та контролю.

Системи запобігання втраті даних (Data Loss Prevention, DLP) – це комплексні технологічні рішення, розроблені для захисту конфіденційної та чутливої інформації. Вони забезпечують контроль і обмеження передачі даних відповідно до заданих організацією правил і політик. DLP-рішення можуть включати аудит, моніторинг та блокування відправки інформації через електронну пошту, веб-ресурси, месенджери, файлообмінники та інші канали комунікації. Крім того, такі системи здатні ідентифікувати та запобігати несанкціонованим діям з даними, наприклад, копіюванню на зовнішні носії або завантаженню у хмарні сервіси.

Рішення про впровадження DLP базується передусім на оцінці ризиків втрати критичних даних та вимогах регуляторів. Окрім нормативних вимог, компанії усвідомлюють високу ціну витоку даних: інциденти можуть призвести до фінансових втрат, втрати довіри клієнтів і пошкодження ділової репутації.

Залежно від характеру даних, що обробляються, система має забезпечувати контроль доступу, моніторинг руху конфіденційної інформації та автоматичне блокування потенційних загроз. DLP повинна бути інтегрована в існуючу IT-інфраструктуру, охоплюючи робочі станції, сервери, мережеві шлюзи та хмарні середовища. Успішне впровадження передбачає попередній аналіз інформаційних активів та класифікацію даних

відповідно до рівня чутливості.

Аналіз системи DLP демонструє значні зміни у показниках безпеки після її впровадження. У звітах DLP фіксується кожен випадок спрацювання політики, наприклад, коли хтось намагається відправити назовні файл із номерами кредитних карт, система це виявляє і блокує.

Таким чином, кількість блокувань чутливих даних слугує метрикою результативності: її зростання порівняно з базовим рівнем свідчить, що тепер витоки не проходять непоміченими. DLP дозволяє виміряти частку або обсяг конфіденційної інформації, що залишає межі організації усупереч політикам безпеки. Після впровадження DLP очікується суттєве зниження цього показника, оскільки система здатна відфільтрувати більшість несанкціонованих передач.

Система вважається ефективною, якщо виконуються такі умови:

1. Забезпечення контролю за всіма потенційними каналами витоку.
2. Точність і своєчасність виявлення.
3. Мінімальний вплив на користувачів.
4. Відповідність законодавчим вимогам.

Впроваджуючи DLP, організація отримує чітку картину, де саме зберігаються її чутливі дані і як вони рухаються. До уваги береться можливість інтеграції системи з іншими засобами кібербезпеки, такими як SIEM, IAM та засоби управління доступом.

Отже, на сьогоднішній день впровадження DLP-систем є важливим кроком у забезпеченні інформаційної безпеки організацій, оскільки вони дозволяють мінімізувати ризики витоку конфіденційних даних через різні канали. Аналіз показує, що ефективність DLP залежить від правильного налаштування політик безпеки, інтеграції з іншими захисними інструментами та постійного моніторингу загроз.

Список використаних джерел:

1. Sheela Gowr. P, Kumar. N. Data Leakage Prevention System: A Systematic. International Journal of Recent Technology and Engineering (IJRTE). 2019. DOI: https://www.ijrte.org/wp-content/uploads/papers/v8i4/D690411841 9.pdf(дата звернення: 22.02.2025)
2. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014.
3. Плюси та мінуси запобігання втраті даних. URL: https://www.digitalguardian.com/blog/pros-cons-data-loss-prevention (дата звернення: 25.02.2025).