КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.995
УДК 004.89

Гайдур Галина Іванівна
доктор технічних наук, професор,
завідувач кафедри систем та технологій кібербезпеки
Державний університет інформаційно-телекомунікаційних технологій, Київ, Україна
ORCID: 0000-0003-0591-3290
g.haidur@duikt.edu.ua

Марченко Віталій Вікторович
кандидат технічних наук, доцент,
доцент кафедри систем та технологій кібербезпеки
Державний університет інформаційно-телекомунікаційних технологій, Київ, Україна
ORCID: 0000-0003-4271-3132
v.marchenko@duikt.edu.ua

Борсуковський Юрій Володимирович
кандидат технічних наук, доцент,
доцент кафедри систем та технологій кібербезпеки
Державний університет інформаційно-телекомунікаційних технологій, Київ, Україна
ORCID: 0000-0003-1973-2386
BYurii@duikt.edu.ua

Дмітрієв В'ячеслав Євгенович
Старший викладач кафедри систем та технологій кібербезпеки
Державний університет інформаційно-телекомунікаційних технологій, Київ, Україна
ORCID: 0009-0001-6508-9945
v.dmitriev@duikt.edu.ua

Царьова Софія Валеріївна
студентка кафедри Систем та технологій кібербезпеки
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0004-9241-3730
tsaryovasofiya@gmail.com

DLP-СИСТЕМА ЯК КОМПОНЕНТ ПРОТИДІЇ ІНСАЙДЕРСЬКИМ ЗАГРОЗАМ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ

Анотація. Загрози інформаційної безпеки, зокрема витоки даних, що спричинені діями співробітників, з кожним роком лише зростають та становлять серйозний ризик для організацій. Наслідки реалізації таких загроз можуть бути руйнівними, оскільки вже надані доступи до інформаційних активів та знання співробітниками про наявні контролі безпеки ускладнюють виявлення та значно збільшують час реагування на інцидент безпеки. Одним із найвідоміших засобів запобігання внутрішнім загрозам інформаційної безпеки є Data Leak Prevention системи. Можливості тонкого налаштування правил відслідковування чутливих даних в мережі дозволяють запобігти випадкам, коли працівник поширює конфіденційні дані через неуважність або нестачу обізнаності. Тим не менш, DLP-рішення може виявитися неефективним для протидії вмотивованим інсайдерам, що здатні скористатися недоліками засобу безпеки, такими як неможливість перевірки зашифрованого файлу на наявність сенситивних даних. У статті досліджені шляхи покращення дієвості DLP-системи проти навмисного викрадення та розповсюдження інформації з обмеженим доступом. Це досягається шляхом постійної взаємодії Data Leak Prevention з іншими контролями безпеки, такими як управління доступом, аналітика активності користувачів та корпоративна культура організації, що націлена на забезпечення інформаційної безпеки. Було проведено аналіз сучасних DLP-систем та визначено критерії, за якими можливо обрати рішення, що найбільше охоплюватиме інформаційну інфраструктуру організації та забезпечуватиме комплексний підхід до захисту даних. Автор наголошує увагу на важливості інтеграції Data

Leak Prevention та User Activity Monitoring для своєчасного виявлення підозрілої поведінки користувачів та реагування на неї. Розглянуто практичну реалізацію поєднання DLP і UAM на прикладі програмного комплексу Teramind, функціонал якого забезпечує не тільки повноцінний контроль над використанням даних в мережі організації, а й спрощує процес реагування на інциденти витоку конфіденційної інформації. Результатами дослідження є розробка рекомендацій для підвищення ефективності DLP-системи у протидії інсайдерським загрозам.

Ключові слова: кібербезпека; загрози; інформаційна безпека; витік інформації; персональні дані; інсайтдерська атака; заходи захисту; DLP; UAM.

ВСТУП

Несанкціоновані дії з боку працівників залишаються серйозною загрозою для інформаційних активів організацій. Згідно зі звітом IBM середній збиток компаній від інсайдерських атак – 4,92 мільйонів доларів США [1]. Особливістю витоків даних, спричинених інсайдерами, є складність їх виявлення. Вже наявний доступ до внутрішньої мережі компанії, доступ до привілейованих облікових записів, знання організації інформаційної безпеки в компанії – все це дозволяє маскувати зловмисні дії під нормальну активність під час виконання робочих обов'язків. Як повідомляють Cybersecurity Insider у 93% випадках виявити та запобігти порушенням з боку співробітників складніше, ніж зовнішнім кібератакам через відсутність вже відомих й добре помітних індикаторів компрометації [2].

Найбільше занепокоєння викликає навмисні викрадення та оприлюднення конфіденційної інформації заради фінансової вигоди (50%), особистого інтересу працівника (47%), помсти та саботажу (45% і 40% відповідно), а також нанесення репутаційної шкоди (37%) [3].

Нещодавнім прикладом вмотивованих дій співробітників, що призвели до витоку чутливих даних, є інцидент, з яким стикнулася крипттовалютна біржа Coinbase у травні 2025 року. Підкуплені зовнішніми зловмисниками, група співробітників служби підтримки скористалася наданими правами доступу й скопіювала персональні дані клієнтів Coinbase для їх передачі третій стороні. Таким чином були викрадені, зокрема, імена та адреси електронної пошти користувачів, відомості про фінансову активність облікових записів (снапшоти балансів та історія транзакцій) тощо. Наслідками такого витоку були значні фінансові втрати, спричинені підривом довіри до компанії і, як наслідок, скороченням клієнтської бази та інвестицій, а також можливими штрафами через порушення законодавства у сфері захисту персональних даних [4], [5].

Зважаючи на високі ризики, пов'язані з доступом співробітників до корпоративної інформації, належні засоби захисту повинні бути впроваджені. Одним із таких рішень є Data Leak Prevention (DLP) система, що відслідковує взаємодію користувачів з даними в мережі відповідно до налаштованих політик виявлення, таких як певні символьні шаблони, regex-вирази або цифрові відбитки, та блокує їх несанкціоноване поширення у разі порушення правил використання.

Такий підхід є ефективним для запобігання витоку даних у результаті ненавмисних помилок користувачів. Наприклад, система за назвою конфіденційного файлу, яка записана в її сигнатурній базі, здатна заблокувати його випадкове пересилання поштою неправильному адресату. Але у випадку вмотивованої інсайдерської атаки, зловмисник, маючи навіть мінімальні технічні навички, здатен скористатися недосконалістю роботи

DLP-системи (наприклад, неможливість проаналізувати зашифрований файл) та обійти встановлені правила виявлення.

Аналіз останніх досліджень та публікацій. Роботи, присвячені системам запобігання витоку даних, зосереджені на важливості впровадження цього засобу захисту на підприємствах для забезпечення захищеності персональних даних та інтелектуальної власності. Досліджуються механізми контролю даних, що є в сучасних DLP-системах, а також порівнюються представлені на ринку рішення.

У роботі [6] розглядаються етапи впровадження DLP-системи. Автори наголошують на необхідності поступової інтеграції, що повинна складатися з первинної класифікації конфіденційної інформації, що обробляється в організації, оцінки ризиків та оцінки різних DLP-систем відповідно до визначених вимог та цілей. Перед впровадженням обраної DLP у роботу потрібно провести тестування її функціональності та впливу на бізнес-процеси. Для ефективного захисту конфіденційних даних DLP-система має проходити регулярний аудит на відповідність політик реагування наявним потребам, з їх подальшим оновленням за необхідністю. Розглядаються функції сучасних DLP-систем на прикладі Symantec-DLP.

Автори роботи [7] розглядають DLP-систему як компонент комплексного підходу до захисту корпоративних даних в умовах політики Bring Your Own Device. Архітектура DLP-системи в цьому випадку базується на встановленні центрального сервера, на якому налаштовуються політики, та клієнтських агентів на кінцеві пристрої працівників. При цьому, необхідним є додатковий захист мережного з'єднання та контроль доступу з допомогою таких засобів, як міжмережні екрани, IDS/IPS системи та Network Access Control (NAC).

Хоча в роботі [7] коротко описані можливі шляхи обходу DLP-системи та способи їх знешкодження, увага досліджень в основному зосереджена на аналізі базових можливостей DLP у контексті запобігання випадковим витокам чутливих даних. При цьому, майже не розглядаються недоліки Data Leak Prevention систем у протидії вмотивованим внутрішнім зловмисникам та способи їх пом'якшення.

Проблематика дослідження. Існуючі рішення DLP не завжди здатні ідентифікувати та попередити витік конфіденційних даних, спричинений навмисними діями співробітників. Наслідками цього недоліку серйозні фінансові та репутаційні збитки для організацій. Саме тому, для пом'якшення інсайдерських загроз та своєчасного й результативного реагування на вже існуючі інциденти, DLP має функціонувати як частина комплексної системи захисту.

Мета роботи. Дослідити можливості підвищення ефективності Data Leak Prevention системи у протидії навмисним витоками конфіденційної інформації, шляхом її взаємодії з іншими організаційними та технічними заходами захисту. Визначити принципи успішного застосування DLP як компоненту комплексної системи захисту чутливих даних всередині організації.

ОСНОВНА ЧАСТИНА

Важливість взаємодії DLP з іншими системами захисту

Хоча DLP-системи пропонують функціонал для відслідковування конфіденційних даних та блокування несанкціонованого розкриття, їх недостатньо для повного захисту від загроз з боку внутрішніх зловмисників при наявності в них відповідних знань та навичок. Наприклад, DLP-система не може розпізнати витік файлу за його цифровим відбитком, якщо було застосоване шифрування [8]. Найпростішим способом експлуатації цього

недоліку є збереження файлу, до якого застосовані політики DLP, в захищеному паролем архіві.

Більш обізнаний користувач може застосувати методи стеганографії, – техніки приховування інформації всередині іншого фалу (зображення, аудіо-файлу тощо), – з допомогою спеціальних програмних засобів, онлайн-сервісів або ручного редагування, наприклад у програмному комплексі Photoshop. Таким чином унеможливлюється ідентифікація чутливої інформації DLP-системою за ключовими словами або regex-шаблонами.

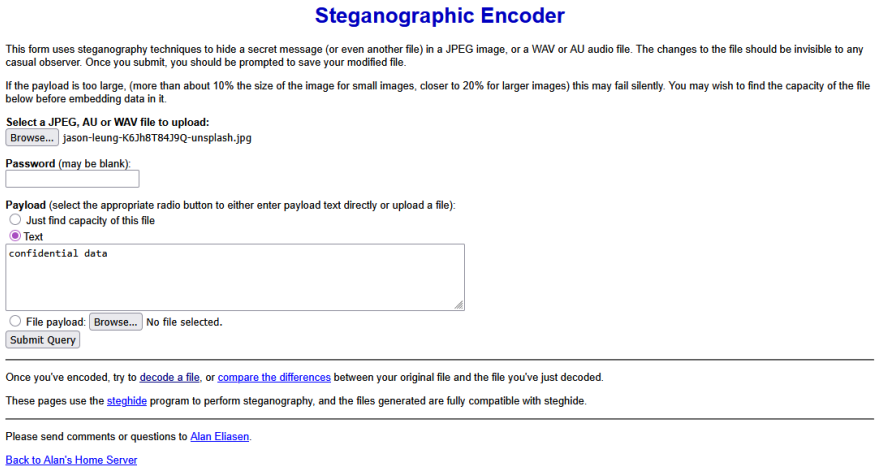

Рис. 1. Використання онлайн-сервісу Steganographic Encoder для приховування тексту в зображенні

Отже, для запобігання витоків необхідний комплексний підхід, що ґрунтується на постійному відслідковуванні не тільки самої критичної інформації, а також і користувачів, що взаємодіють з нею.

Базовим необхідним контролем доступу є запровадження рольової моделі та принципу найменших привілеїв, коли користувачу надаються мінімальні права доступу до ресурсів, необхідні для виконання робочих обов'язків. Особливо важливим є контроль адміністративних облікових записів, для яких необхідно впроваджувати двофакторну аутентифікацію та використання інструментів PAM (Privileged Access Management).

Оскільки людський фактор є найслабшою ланкою в системі захисту інформації, необхідно поєднувати технічні засоби з безпосереднім зв'язком з персоналом, зокрема, з допомогою регулярних тренінгів з безпечної роботи з інформацією з обмеженим доступом, під час яких до співробітників чітко доносяться можливі наслідки порушень політик безпеки компанії.

У випадку інсайдерських загроз, передумовою часто можуть бути соціальні та психологічні фактори, такі як фінансові труднощі, різні види залежності, домашнє насилля або тиск з боку керівництва. Важливо звертати увагу на поведінкові індикатори таких проблем – погана соціальна взаємодія або соціальна ізоляція, непередбачувана агресія, небажання дотримуватися встановлених правил і політик організації та їх повторні порушення, погана концентрація, зростання кількості помилок тощо, – та надавати підтримку співробітникам у вигляді, зокрема, професійної психологічної допомоги та вибудовування корпоративної культури, що базується на встановленні чітких меж для

лідерів організації, відповідальності кожного співробітника за свою поведінку та вчинки й заохоченні повідомляти про неприйнятну поведінку без страху перед наслідками [9].

Оскільки важливим є безперервний моніторинг активності користувачів для своєчасного виявлення внутрішніх загроз, сучасні DLP часто є інтегрованими в системи управління активністю користувачів (User Activity Monitoring або UAM) [3]. Функції DLP реалізуються через налаштування політик, а саме відслідковування конфіденційної інформації за шаблонами з можливістю автоматичного реагування у разі несанкціонованого пересилання – надсилання попередження, блокування облікового запису. Окрім цього UAM-рішення пропонують різноманітні способи відслідковування активності користувачів – перехоплення даних з клавіатури, команд у терміналі, буферу обміну, перегляд запису з екранів робочих станцій працівників, створення правил для виявлення підозрілої активності, такої як запис інформації на змінні носії, створення знімків екрану, віддалене підключення до інших хостів тощо [10].

Аналіз сучасних DLP-систем

Наразі на ринку існує багато DLP-рішень. Важливими критеріями при виборі DLP-системи є: можливість контролю підключених до робочих станцій USB-пристроїв, щоб уникнути витоку даних через копіювання на змінні носії; підтримка всіх популярних операційних систем для захисту всієї інформації, що обробляється в мережі організації; можливість передачі сповіщень безпеки до SIEM-системи для централізованого адміністрування подій безпеки. В таблиці 1 наведено порівняння характеристик деяких з сучасних DLP-систем.

Таблиця 1

Порівняння функціоналу сучасних DLP-систем

DLP-система / Функціонал	Manage Engine DLP Plus	Endpoint Protector DLP	Teramind DLP	Safetica DLP
Контроль USB-пристроїв	Так	Так	Так	Так
Підтримка MacOS та Linux	Ні	Так	Частково (підтримка MacOS)	Частково (підтримка MacOS)
Інтеграція з іншими засобами безпеки	Ні	Так (інтеграція з SIEM-системою)	Так (інтеграція з SIEM-системою та UAM)	Так (інтеграція з SIEM-системою)

Прикладом DLP-системи, яка пропонує комплексний підхід до захисту інформації від внутрішніх загроз, поєднуючи функціонал DLP та UAM є Teramind DLP. Контроль роботи співробітників з конфіденційними даними відбувається за допомогою програмних агентів, що збирають інформацію про активність користувачів, та надсилають її до керуючого сервера. Використовуючи DLP-сервер, адміністратор безпеки налаштовує політики реагування.

Перевагою Teramind DLP, як було зазначено раніше, є впровадження DLP як частини UAM-системи, що дозволяє централізовано здійснювати контроль над захистом від витоків конфіденційних даних, відслідковувати підозрілі дії співробітників та запобігати несанкціонованому викриттю даних у тих випадках, коли базового функціоналу DLP недостатньо.

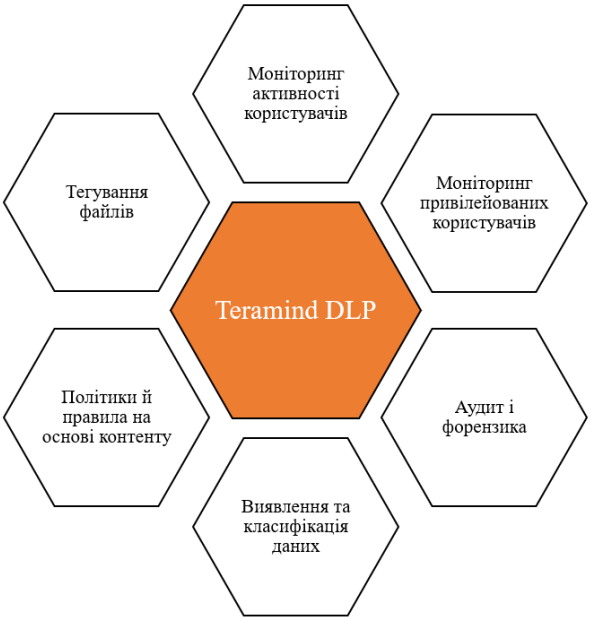

Рис. 2. Функціональні можливості Teramind DLP для протидії інсайдерським загрозам

Наприклад, можливість ідентифікації програмного забезпечення, яке було запущене на робочих станціях, дозволяє усунути ризик витоку чутливої інформації через додатки, які не відповідають вимогам безпеки організації. Виявивши порушення, команда інформаційної безпеки може своєчасно ініціювати процес видалення забороненого програмного забезпечення з кінцевих точок та застосування дисциплінарного покарання до співробітника, що порушив політики безпеки.

Записи з екранів корпоративних комп'ютерів можуть бути корисними під час реагування на сповіщення від DLP-системи – від того, чи подія відбулася в результаті помилкових дій співробітника, навмисного зловживання доступом або ексфільтрації даних зловмисником з скомпрометованої системи, залежатимуть подальші дії для усунення загрози.

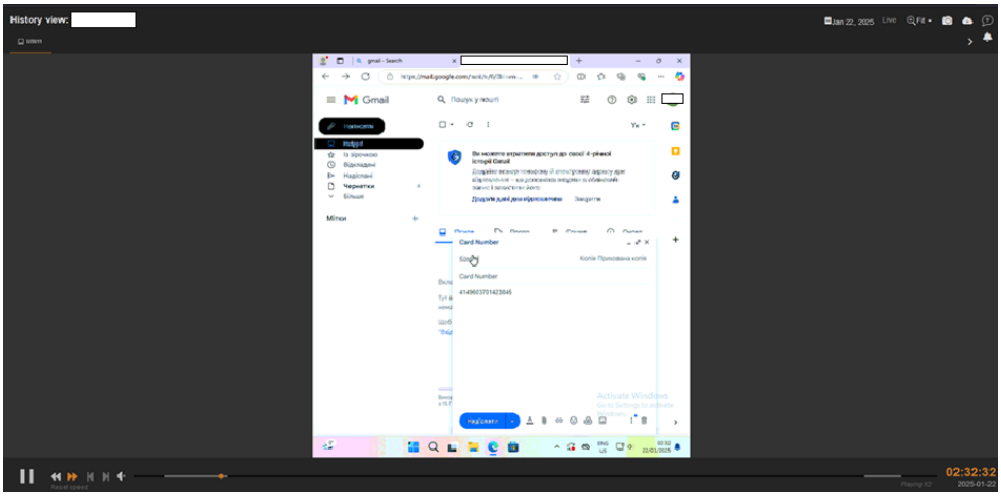

Рис. 3. Приклад запису екрану, зробленого з допомогою Teramind DLP, на якому зафіксоване несанкціоноване поширення чутливої інформації

Рішення пропонує як ручне розгортання віртуального сервера на фізичному обладнанні (on-premise), так і хмарну версію, доступну через веб-браузер. Вона дозволяє полегшити процес впровадження DLP-системи в інформаційно-комунікаційну систему організації та зменшити фінансові витрати.

Конфіденційність при використанні on-premise версії Teramind можна забезпечити шляхом асиметричного шифрування даних, що передаються від програмних агентів до сервера. Таким чином, доступ до записів, що можуть містити інформацію з обмеженим доступом, можливо отримати лише з допомогою паролю, пов’язаного з особистим ключем.

Недоліком цієї DLP-системи є те, що пробний період триває всього 7 днів, що може бути недостатнім для того, щоб провести повноцінне тестування засобу безпеки та вирішити, чи відповідає він вимогам організації [10-13].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Для того, щоб DLP-система була ефективною у зменшенні ризику витоку конфіденційних даних, під час її впровадження та експлуатації необхідно дотримуватись наступних рекомендацій:

– DLP-система має бути частиною комплексної системи захисту інформації та працювати разом з іншими засобами захисту, такими як антивірусне програмне забезпечення, міжмережні екрани, SIEM та UAM системи тощо. Мають бути прописані чіткі політики безпеки даних та інструкції, що визначатимуть правила експлуатації DLP-системи та відповідальних осіб;

– організація повинна провести оцінку своїх інформаційних активів, щоб визначити, яка інформація потребує захисту, і в майбутньому правильно налаштувати політики для DLP-системи. Ці вимоги можуть зокрема регулюватися законодавством та галузевими стандартами, такими як PCI DSS;.

– повинна підтримуватися ефективна комунікація зі співробітниками, наприклад, з допомогою регулярних опитувань щодо залучення;

– мають проводитись регулярні навчання співробітників для збільшення рівня обізнаності про загрози інформаційної безпеки та правила безпечної роботи з конфіденційними даними. Співробітники повинні чітко усвідомлювати наслідки порушення політик безпеки організації;

– політики, налаштовані для DLP-системи, мають регулярно переглядатися на відповідність актуальним потребам та редагуватися у разі зміни типу інформації з обмеженим доступом, що обробляється в організації.

Data Leak Prevention система є необхідним компонентом захисту від інсайдерських загроз, що захищають критичну для організації інформацію від несанкціонованого розповсюдження. Тим не менш, цей засіб захисту є дієвим проти внутрішніх зловмисників лише у випадку інтеграції з іншими організаційними та технічними заходами запобігання витоку даних.

З точки зору подальших досліджень контролю доступу користувачів до конфіденційних даних з метою протидії навмисним витокам даних та застосування для цього DLP та UAM систем актуальним залишається питання етичності. Увага має бути приділена проблемі одночасного забезпечення приватності користувачів, зокрема права на таємницю кореспонденції, та надійного захисту конфіденційної інформації від розголошення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cost of a data breach 2025 | IBM. (2025). IBM. https://www.ibm.com/reports/data-breach.
2. 2025 Insider Risk Report [Cogility]. (2025). Cybersecurity Insiders. https://www.cybersecurity-insiders.com/portfolio/2025-insider-risk-report-cogility/.
3. Holger, S. (2024). New Report Reveals Insider Threat Trends, Challenges, and Solutions. Cybersecurity Insiders. https://www.cybersecurity-insiders.com/2024-insider-threat-report-trends-challenges-and-solutions/.
4. Protecting Our Customers - Standing Up to Extortionists. (2025, 15 May). Coinbase. https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists.
5. Verrion, W. (2025, 31 July). What the Coinbase Breach Says About Insider Risk. Dark Reading. https://www.darkreading.com/vulnerabilities-threats/coinbase-breach-insider-risk.
6. Polotai, O., & PuzyrA. (2024). Analysis of Means of Preventing the Leakage of Confidential Information iN Enterprises, Using the DLP System as an Example. Bulletin of Lviv State University of Life Safety, 30, 134-144. https://doi.org/https://doi.org/10.32447/20784643.30.2024.13.
7. Vovchanskyi, P. P., & Demchynskyi, V. V. (2020). Architecture of DLP systems in the context of BYOD policy. Theoretical and applied problems of physics, mathematics, and computer science. https://www.researchgate.net/publication/347525260_Arhitektura_DLP-sistem_v_umovah_politiki_BYOD.
8. Insider Threat Mitigation Guide. (2020). Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide.
9. About document fingerprinting. (2025, 31 March). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/purview/sit-document-fingerprinting?tabs=purview.
10. Arik. (2025). Usage & Deployment Guides | Teramind Knowledge Base. Teramind Knowledge Base. https://kb.teramind.co/en/collections/7798686-usage-deployment-guides.
11. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
12. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
13. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). Enterprise information and cyber security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.

КІБЕРБЕЗПЕКА: освіта, наука, техніка № 2 (30), 2025
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
Спеціальний випуск ISSN 2663 – 4023
Special issue

Halyna Haydur
Doctor of Technical Sciences, Professor, Head of the Department of Cybersecurity Systems and Technologies
State University of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-0591-3290
g.haidur@duikt.edu.ua

Vitalii Marchenko
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Cybersecurity Systems and Technologies
State University of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-4271-3132
v.marchenko@duikt.edu.ua

Yurii Borsukovskyi
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Cybersecurity Systems and Technologies
State University of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-1973-2386
BYurii@duikt.edu.ua

Viacheslav Dmitriiev
Senior Lecturer, Department of Cybersecurity Systems and Technologies
State University of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0009-0001-6508-9945
v.dmitriev@duikt.edu.ua

Sofiia Tsarova
Student of the Department of Cybersecurity Systems and Technologies,
State University of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0009-0004-9241-3730
tsaryovasofiya@gmail.com

DLP SYSTEM AS A COMPONENT OF COUNTERING INSIDER THREATS TO INFORMATION CONFIDENTIALITY

Abstract. Information security threats, particularly data leaks caused by employee actions, are increasing every year and pose a serious risk to organizations. The consequences of such threats can be devastating, as employees' existing access to information assets and their knowledge of security controls complicate detection and significantly increase the time required to respond to a security incident. One of the most well-known means of preventing internal information security threats is Data Loss Prevention (DLP) systems. The capability to fine-tune rules for tracking sensitive data across the network helps prevent instances where an employee disseminates confidential data due to carelessness or a lack of awareness. Nevertheless, a DLP solution may prove ineffective against motivated insiders who can exploit security control flaws, such as the inability to inspect an encrypted file for sensitive data. This article explores ways to enhance the efficacy of DLP systems against the intentional theft and distribution of restricted information. This is achieved through the continuous interaction of Data Loss Prevention with other security controls, such as access management, user activity analytics, and an organizational corporate culture focused on ensuring information security. An analysis of modern DLP systems was conducted, and criteria were defined for selecting a solution that would best cover the organization's information infrastructure and ensure a comprehensive approach to data protection. The author emphasizes the importance of integrating Data Loss Prevention and User Activity Monitoring (UAM) for the timely detection of and response to suspicious user behavior. The practical implementation of combining DLP and UAM is examined using the example of the Teramind software suite, whose functionality provides not only full control over data usage within the organization's network but also simplifies the process of responding to confidential information leakage incidents. The research results include the development of recommendations for increasing the effectiveness of DLP systems in countering insider threats.

Keywords: cybersecurity; threats; information security; information leakage; personal data; insider attack; protection measures; DLP; UAM.

REFERENCES

1. Cost of a data breach 2025 | IBM. (2025). IBM. https://www.ibm.com/reports/data-breach.
2. 2025 Insider Risk Report [Cogility]. (2025). Cybersecurity Insiders. https://www.cybersecurity-insiders.com/portfolio/2025-insider-risk-report-cogility/.
3. Holger, S. (2024). New Report Reveals Insider Threat Trends, Challenges, and Solutions. Cybersecurity Insiders. https://www.cybersecurity-insiders.com/2024-insider-threat-report-trends-challenges-and-solutions/.
4. Protecting Our Customers - Standing Up to Extortionists. (2025, 15 May). Coinbase. https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists.
5. Verrion, W. (2025, 31 July). What the Coinbase Breach Says About Insider Risk. Dark Reading. https://www.darkreading.com/vulnerabilities-threats/coinbase-breach-insider-risk.
6. Polotai, O., & PuzyrA. (2024). Analysis of Means of Preventing the Leakage of Confidential Information iN Enterprises, Using the DLP System as an Example. Bulletin of Lviv State University of Life Safety, 30, 134-144. https://doi.org/https://doi.org/10.32447/20784643.30.2024.13.
7. Vovchanskyi, P. P., & Demchynskyi, V. V. (2020). Architecture of DLP systems in the context of BYOD policy. Theoretical and applied problems of physics, mathematics, and computer science. https://www.researchgate.net/publication/347525260_Arhitektura_DLP-sistem_v_umovah_politiki_BYOD.
8. Insider Threat Mitigation Guide. (2020). Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide.
9. About document fingerprinting. (2025, 31 March). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/purview/sit-document-fingerprinting?tabs=purview.
10. Arik. (2025). Usage & Deployment Guides | Teramind Knowledge Base. Teramind Knowledge Base. https://kb.teramind.co/en/collections/7798686-usage-deployment-guides.
11. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
12. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
13. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). Enterprise information and cyber security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.