УДК 004.056.5

Т.В. Німченко, к.т.н.,
Т.В. Мелешко,
Л.І. Моржова
Національний авіаційний університет, Київ

СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

На сьогодні інформація є найціннішим ресурсом. Тому перед організаціями та підприємствами гостро постає завдання збереження інформації, у тому числі відомостей, що становлять комерційну або державну таємницю [1].

Ефективність бізнесу в багатьох випадках залежить від збереження конфіденційності, цілісності та доступності інформації. В даний час однією з найбільш актуальних загроз у сфері інформаційної безпеки є витік конфіденційних даних від несанкціонованих дій користувачів [2]

Як показують опубліковані дані опитування Deloitte провідних світових фінансових компаній, 49% респондентів зафіксували внутрішні інциденти (пов'язані з IT-безпекою). У 31% випадків інсайдери занесли віруси зсередини корпоративної мережі, а з інсайдерськими шахрайством зіткнулися 28% респондентів. 18% організацій стали жертвами витоку приватної інформації клієнтів, а 10% виявили, що інсайдери скомпрометували корпоративну мережу [2-3].

Широке застосування для захисту інформаційних ресурсів знайшли системи DLP. Системи DLP це технології, що дозволяють запобігти витоку конфіденційної інформації. У перебігу останніх декількох років використовувалася велика термінологія: Information Leakage Protection (ILP), Information Leak Protection (ILP), Information Leakage Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), Extrusion Prevention System (EPS) та ін. Але остаточним і найбільш точним терміном прийнято вважати Data Leak Prevention (DLP, запропонований агентством Forrester в 2005 р.).

В рамках створення таких систем вирішуються завдання: запобігання витоків конфіденційної інформації по основних каналах передачі даних; витікаючий веб-трафік (HTTP, FTP, P2P та ін.); вихідна електронна пошта, внутрішня електронна пошта; системи миттєвого обміну повідомленнями, мережевий та

локальний друк; контроль доступу до пристроїв і портів введення-виведення до яких відносяться: дисководи, CD-ROM, USB - пристрої, інфрачервоні, принтерні (LPT) і модемні (COM) порти.

Для запобігання витоку інформації системи DLP мають вбудовані механізми ступеню конфіденційності перехопленого документа: шляхом аналізу вмісту документа або шляхом аналізу спеціальних маркерів (грифів). Вони наділені можливостями аналізу за словником, лінгвістичного аналізу, аналізу транслітерації.

У DLP-системах зазвичай використовуються три методи ідентифікації: імовірнісний, детерміністський та комбінований.

Системи, засновані на першому методі, основним чином використовують лінгвістичний аналіз контенту та «цифрові відбитки» даних. Такі системи прості в реалізації, але недостатньо ефективні і характеризуються високим рівнем помилкових спрацювань. Системи, що використовують детермінований підхід (мітки файлів), дуже надійні, але їм невистачає гнучкості.

Комбінований підхід поєднує обидва методи з аудитом середовища зберігання та обробки даних, що дає можливість досягти оптимального вирішення проблеми захисту конфіденційності інформації [4].

Звісно, гарантувати абсолютний захист від наслідків діяльності працівників не може жодна DLP-система, однак вона дозволить значно мінімізувати ризики та наслідки людських помилок. Отже, використання систем DLP є одним з ефективних варіантів захисту конфіденційної інформації.

ВИКОРИСТАНІ ДЖЕРЕЛА

1.ohttps://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf

2.ohttps://ua.ikmj.com/isms-access-control/

3.ohttp://integritysys.com.ua/security/dlp/

4. О.В. Богуславський, Д.А. Кирилюк. DLP системи як засіб виявлення інсайдера. Міжнародна науково-практична конференція Інформаційні технології та взаємодії. – 2018. – С. 249.