

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

Забезпечення заходів інформаційної безпеки (ІБ) стає все більш важливим питанням для багатьох банків. Усвідомлення масштабів можливих ризиків та загроз, а також вимог НБУ банки не тільки створюють письмову документацію про комплексну політику інформаційної безпеки, але й забезпечують усім необхідним для ефективної роботи системи управління ІБ.

Правильний підхід до організації системи ІБ передбачає розмежування права на допуск, розуміння співробітників відповідальності за виток даних, своєчасне оновлення програмного забезпечення, контроль виконання всіх правил та інструкцій. При цьому ключовою задачею являється навчання персоналу інформаційної безпеки.

Для реалізації даної задачі широке застосування отримала DLP-система (англ. Data Loss Prevention). DLP-система повинна забезпечувати моніторинг поточного стану захисту й оповіщати про витоки, а також надати засоби активного аналізу вразливих місць і інструменти для швидкого розслідування інцидентів. Правильний вибір DLP-рішення залежить перед усім від розуміння, які ресурси потрібно захищати і де вони знаходяться.

Практично усі DLP-рішення в своїй основі містять технологію морфологічного аналізу даних. І цієї технології частіш за все достатньо для забезпечення захисту наявної інформації від витоку при відправленні поштових листів, месенджерів або публікацій у соціальних мережах. Більш складні системи включають у себе технологію цифрових відбитків або маркування даних. Такі технології в поєднанні з морфологічним аналізом істотно підвищують безпеку конфіденційної інформації.

Ефективне застосування технічних засобів захисту буде можливим тільки після реалізації наступних організаційних заходів:

- розробка політики інформаційної безпеки;
- аналіз загроз і оцінки ризиків;
- розробка критеріїв класифікації інформації;
- інвентаризація інформаційних ресурсів, котрі підлягають захисту.

Таким чином розгортання DLP-систем – достатньо складний процес, який потребує значних трудових затрат на початкових стадіях комплексу організаційних заходів, але впровадження DLP-системи виправдає усі затрачені ресурси.

Науковий керівник – к.т.н., доц., А.О. Краснопольський