ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

Дослідження шляхів та розробка рекомендацій щодо захисту від витоку інформації з інформаційної системи організації на базі DLP-системи Symantec

Виконав студент 4 курсу, групи БСД-42
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Мрещук А.О.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

TCO - Total Cost of Ownership

DLP - Data Loss Prevention

HTTP - HyperText Transfer Protocol

ПЗ – програмне забезпечення

CSV - Comma-Separated Values

ІБ - інформаційна безпека

AD – Active Directory

VML - Vector Markup Language

ІТ - інформаційні технології

ВСТУП

Актуальність дослідження. У сучасному інформаційному суспільстві інформаційна безпека стала однією з ключових проблем для компаній і підприємств. У контексті швидкого розвитку технологій, все більше даних стає цифровими та потребує надійного захисту. Актуальність досліджуваної теми "Дослідження шляхів і розробка рекомендацій щодо застосування DLP-системи 'Symantec' як інструменту забезпечення інформаційної безпеки компанії та підприємств" випливає з низки чинників.

По-перше, зростання загроз інформаційній безпеці має значний вплив на успішність і діяльність компаній. Кібератаки, віруси, зломи, фішингові атаки та інші види кіберзагроз можуть призвести до витоку конфіденційної інформації, порушення роботи систем і серйозних фінансових втрат. Це особливо актуально для компаній, що зберігають конфіденційні дані клієнтів, банківську інформацію, комерційні секрети або інтелектуальну власність.

По-друге, законодавство і нормативні вимоги в галузі інформаційної безпеки стають дедалі суворішими. Багато галузей мають спеціальні правила і стандарти, яким необхідно відповідати. Порушення цих вимог може спричинити санкції, штрафи або навіть судові розгляди. Тому компанії та підприємства все більше звертають увагу на забезпечення інформаційної безпеки та впровадження відповідних систем та інструментів.

По-третє, зростаюча складність інформаційних систем і мереж вимагає використання спеціалізованих інструментів для виявлення та запобігання витоку інформації. DLP-системи (Data Loss Prevention) стають дедалі більш затребуваними для захисту конфіденційних даних, контролю передавання інформації та виявлення порушень політик безпеки. У цьому контексті DLP-система "Symantec" є одним із провідних рішень на ринку, пропонуючи широкий функціонал і можливості аналізу, контролю та захисту інформації.

Таким чином, дослідження шляхів застосування DLP-системи Symantec і розробка рекомендацій щодо її використання стають актуальними завданнями, що сприяють забезпеченню інформаційної безпеки компаній і підприємств. Це дасть змогу компаніям ефективно управляти ризиками, запобігати витоку даних і захищати свою інформацію від кіберзагроз, забезпечуючи надійну роботу та зберігаючи довіру клієнтів і партнерів.

Об’єкт дослідження – інформаційна система організації, яка схильна до ризику витоку конфіденційної інформації.

Предмет дослідження – DLP-система Symantec, як інструмент забезпечення інформаційної безпеки компанії та підприємств.

Мета роботи – аналіз DLP-системи Symantec, вивчення особливості цієї системи, її функціональність, можливості інтеграції з наявною інфраструктурою компаній і підприємств.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації.

Завдання бакалаврської роботи:

провести огляд наявних загроз і ризиків, з якими стикаються компанії та підприємства у сфері інформаційної безпеки;

вивчити концепцію DLP-систем та їхню роль у забезпеченні інформаційної безпеки;

провести аналіз DLP-системи Symantec; розробити рекомендації щодо застосування DLP-системи Symantec;

Практичне значення одержаних результатів: рекомендації для компаній і підприємств, які планують впровадити або поліпшити свої заходи інформаційної безпеки за допомогою DLP-системи Symantec, рекомендації налаштування.

1 ОГЛЯД DLP-СИСТЕМ ТА ЇХНЯ РОЛЬ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Визначення та методи функціонування DLP-системи

Система запобігання втрати даних (DLP) є комплексним програмним забезпеченням, розробленими для захисту конфіденційної та чутливої інформації в організаціях. Необхідність захисту інформації від внутрішніх загроз була очевидною на всіх етапах розвитку засобів інформаційної безпеки. Спочатку вважалося, що зовнішні загрози є найбільш небезпечними. Однак останніми роками стало проявлятися більше уваги до внутрішніх загроз, і в результаті збільшилася популярність DLP-систем. Термін DLP має кілька загальноприйнятих розшифровок та інтерпретацій:

- **Data Loss Prevention** - "запобігання втраті даних"
- **Data Leak Prevention** - "запобігання витоку даних"
- **Data Leakage Protection** - "захист від витоку даних"

Спочатку DLP системи з'явилися як засіб для запобігання небажаному розкриттю цінної інформації. Їхня основна мета полягала у виявленні та блокуванні передавання даних мережею.

Головною метою DLP-систем, що очевидно, є запобігання передачі конфіденційної інформації за межі інформаційної системи. Ця передача, або витік, може бути як навмисною, так і ненавмисною. Значна частина відомих випадків витоків (приблизно 3/4) відбувається не зі злого наміру, а внаслідок помилок, неуважності, недбалості та недбалої поведінки співробітників. Виявлення таких витоків більш просте. Частина, що залишилася, пов'язана зі злим умислом операторів і користувачів інформаційних систем. Крім основного завдання, перед DLP-системою можуть стояти і додаткові другорядні завдання. Деякі з них включають:

- запобігання передаванню небажаної інформації не тільки зсередини назовні, а й зовні всередину інформаційної системи;
- запобігання передаванню назовні не тільки конфіденційної, а й іншої небажаної інформації (образливих виразів, спаму, еротики, надмірних обсягів даних тощо);
- архівування повідомлень, що пересилаються, на випадок можливих у майбутньому розслідувань інцидентів;
- подання співробітникам заборони на використання державних інформаційних ресурсів в особистих інтересах;
- оптимізація завантаження каналів, економія трафіку;
- контроль присутності працівників на робочому місці;
- відстеження благонадійності співробітників, їхніх політичних поглядів, переконань, збір компромату.

У більшості країн законом захищається право на особисте життя та конфіденційність. Використання DLP-систем може суперечити місцевим законам у певних випадках або вимагати спеціального регулювання відносин між роботодавцем і співробітниками. Тому при впровадженні DLP-системи необхідно звернутися за допомогою до юриста на ранніх етапах проєктування.

Наразі розробники DLP-систем активно приділяють увагу розширенню охоплення потенційних джерел витоку інформації та розвитку аналітичних інструментів для розслідування й аналізу інцидентів. Сучасні DLP-продукти здатні перехоплювати перегляд, друк і копіювання документів на зовнішні носії, а також контролювати запуск додатків на робочих станціях і підключення зовнішніх пристроїв. Та більше того, за допомогою сучасного аналізу мережевого трафіку можна виявити витік даних, навіть якщо він здійснюється через зашифровані та тунельні протоколи.

У DLP-системах розпізнавання конфіденційної інформації здійснюється двома методами: аналізом формальних ознак, як-от грифи документів, спеціальні мітки або порівняння хеш-функцій, і аналізом контенту. Перший метод допомагає уникнути помилкових спрацьовувань (помилок першого роду), але вимагає попередньої класифікації документів, упровадження міток і збору сигнатур тощо. Однак при використанні цього методу можливі пропуски конфіденційної інформації (помилки другого роду), якщо документ не був попередньо класифікований як конфіденційний.

Другий метод може спричиняти помилкові спрацьовування, але водночас дає змогу виявляти пересилання конфіденційної інформації не тільки в документах із грифами. Щоб забезпечити ефективну роботу, DLP-система повинна містити компоненти обох зазначених методів, а також модуль для централізованого управління.

DLP системи розрізняють за способом виявлення витоку даних:

- у процесі використання даних (Data-in-Use) - на робочій станції користувача;
- під час передачі (Data-in Motion) - у мережі компанії;
- під час зберігання (Data-at Rest) - на серверах і робочих станціях компанії.

DLP-системи включають компоненти (модулі) на мережевому рівні та на рівні хоста. Мережеві компоненти контролюють трафік, який перетинає межі інформаційної системи. Зазвичай вони розміщені на проксі-серверах і серверах електронної пошти. Компоненти на рівні хоста, у свою чергу, встановлені на персональних комп'ютерах співробітників і контролюють такі канали, як запис інформації на компакт-диски, флеш-накопичувачі та інші пристрої. Хостові компоненти також стежать за зміною мережевих налаштувань, друком документів

на локальні та мережеві принтери, передаванням інформації через Wi-Fi і Bluetooth, встановленням програм для тунелювання та іншими можливими способами обходу контролю. Крім того, деякі DLP-системи можуть записувати всі натискання клавіш (key logging) і зберігати знімки екрана (screen shots).

Сучасна система захисту від витоку інформації зазвичай являє собою розподілений програмно-апаратний комплекс, що складається з безлічі модулів різного призначення. Деякі модулі функціонують на виділених серверах, інші - на робочих станціях співробітників компанії, а деякі - на робочих місцях співробітників служби безпеки.

Виділені сервери можуть знадобитися для таких модулів як база даних і, іноді, для модулів аналізу інформації. Ці модулі, по суті, є ядром і без них не обходиться жодна DLP система.

База даних необхідна для збереження різноманітної інформації, включно з правилами контролю, детальними даними про інциденти і всі документи, виявлені системою в певний період часу. У певних випадках, система може навіть зберігати копію всього мережевого трафіку компанії, який був перехоплений за певний період часу.

Як правило, у DLP-системі присутній модуль управління, який відповідає за моніторинг та адміністрування системи. Цей модуль дає змогу відстежувати роботу всіх інших модулів системи, а також виконувати їх налаштування.

Модулі аналізу інформації виконують завдання аналізу текстів, які були витягнуті іншими модулями з різних джерел всередині компанії, таких як мережевий трафік і документи на різних пристроях зберігання інформації. У деяких системах також є можливість вилучення тексту зображень і розпізнавання перехоплених голосових повідомлень. Усі аналізовані тексти порівнюються із заздалегідь встановленими правилами і позначаються відповідним чином у разі виявлення збігів.

З метою забезпечити зручність роботи аналітиків служби безпеки, у DLP-системі може бути передбачено окремий модуль, що дає змогу налаштовувати політику безпеки компанії, відстежувати порушення, проводити детальне розслідування інцидентів і генерувати відповідні звіти. Цікаво, що, порівнюючи всі рівні, можливості аналізу інцидентів, проведення повноцінного розслідування та формування звітів виявляються найбільш важливими в сучасній DLP-системі.

Отже, потреба в забезпеченні захисту інформації від внутрішніх загроз була очевидною на кожному етапі розвитку засобів забезпечення інформаційної безпеки.

1.2. Аналіз загроз втраті даних.

Інформаційна безпека є невід'ємною частиною будь-якої організації. Успіх компанії безпосередньо залежить від її ставлення до безпеки, оскільки втрата даних є неприпустимим проступком, який не прощають ні інвестори, ні клієнти. Якщо в організації є власні розробки, необхідно також забезпечити їхній захист від внутрішніх і зовнішніх атак. Для виявлення та подальшого усунення потенційних витоків інформації, на початкових етапах розвитку компанії необхідно провести ретельний аналіз вразливостей. Це допоможе як забезпечити надійність збережених даних, так і показати організацію з кращого боку.

Загроза інформаційній безпеці являє собою комбінацію умов і чинників, які можуть створювати потенційні або реальні ризики порушення інформаційної безпеки. Ці ризики включають порушення фізичної цілісності, порушення логічної структури, несанкціоновану зміну, отримання та розкриття інформації. У контексті інформаційних систем, усі загрози можна розділити на дві основні групи.

Інформаційні загрози поділяють на три види (рисунок 1.2).

Основними каналами, за допомогою яких порушник здійснює розкрадання інформації та досуп до ресурсів ІС, є (рисунок 1.3):

Рис.1.1. Загрози по відношенню до інформаційної системи.

Рис.1.2. Інформаційні загрози

Рис.1.3. Канали витоку інформації

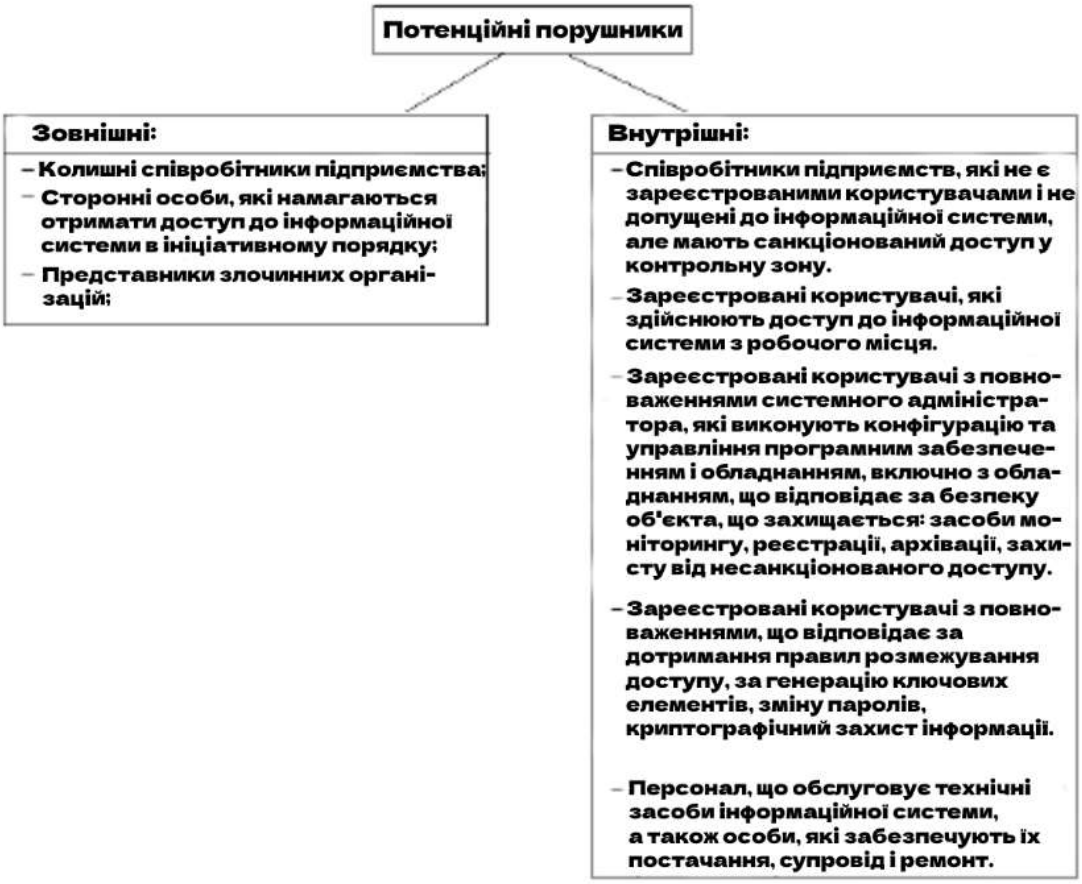

Рис. 1.4. Потенційні порушники.

Аналізування та складання списку загроз і потенційних каналів витоку інформації дає змогу детально розглянути всі можливі способи несанкціонованого доступу до конфіденційних даних і визначити вимоги до системи захисту. Дотримання цих вимог забезпечить необхідний рівень безпеки інформації.

В організаціях для забезпечення захисту даних часто застосовується єдина автоматизована система інформаційної безпеки, яка відіграє ключову роль у запобіганні витокам інформації. Тому вкрай важливо враховувати всі можливі канали технічних витоків, які можуть бути використані зловмисниками для крадіжки даних з використанням фізичних характеристик системи. Ці канали можуть включати вразливості у фізичній інфраструктурі, такі як несанкціонований

доступ до серверів або комп'ютерів, пристроїв зберігання даних, перехоплення мережевого трафіку та інші методи експлуатації фізичних вразливостей.

На рисунку 1.5. представлено схему основних технічних каналів витоку інформації. Ці канали можуть об'єднуватися, створюючи мультиканал, який містить характеристики кількох основних каналів одночасно. структура має визначений ланцюг командування, тоді як децентралізовані структури дають майже кожному працівнику високий рівень особистої відповідальності.

Рис. 1.5 Технічні канали витоку інформації

Типи каналів технічного витоку включають:

Акустичні – несанкціоноване зчитування звуку на об’єкті інформаційної активності, наприклад, прослуховування телефонних розмов в реальному часі.

Акустоелектричні – зчитування за допомогою звукових хвиль, після чого інформація передається по електромережі і на стороні зловмисника перетворюється в читабельний вигляд.

Оптичний канал – варіант крадіжки даних, при якій зловмисник фотографує або проводить довгострокове візуальне спостереження за об'єктом.

Віброакустичний – зчитування вібрацій, створюваних акустикою при впливі на стіни, вікна та інші архітектурні конструкції.

Електромагнітний – зчитування індуктивних сигналів які надходять від полів інформаційної системи.

Побічне електромагнітне випромінювання, яке зловмисник знімає і за допомогою спеціального обладнання перетворює в зрозумілий вид. 4. типи організаційних структур включають функціональні, дивізіональні, плоскі і матричні структури.

На підставі поданої інформації, є можливість провести аналіз вразливих місць у структурі організації та докласти зусиль щодо їх усунення. У разі, якщо повне усунення цих слабких місць неможливе, метою буде мінімізація можливого витоку інформації через такі вразливі канали. Для цього може бути вжито додаткових заходів безпеки, впроваджено відповідні контрольні механізми і регулярно проводитися моніторинг та аудит, щоб виявляти і реагувати на потенційні порушення безпеки інформації. Це дасть змогу створити надійнішу систему захисту даних і забезпечити збереження конфіденційної інформації організації.

1.3. Аналіз рішень для вибору DLP-системи організації.

Аналіз можливих рішень для вибору DLP-системи в організації є ключовим етапом, що дає змогу оцінити різні варіанти та визначити найбільш підходящу систему для забезпечення інформаційної безпеки. Під час проведення цього аналізу рекомендується врахувати наступні аспекти.

Функціональність системи. Важливо вивчити різноманітні інструменти та модулі, пропоновані різними системами, для виявлення, моніторингу та запобігання витокам інформації. Особливу увагу слід приділити визначенню найбільш значущих функцій для організації та вибору системи, яка найбільш повно відповідає вимогам.
Керівники вищої ланки повинні розглянути низку факторів, перш ніж вирішити, який тип організації найкращий для їхнього бізнесу, включаючи бізнес-цілі, галузь і культуру компанії.

Інтеграція. Під час вибору DLP-системи необхідно врахувати її інтеграцію та сумісність з наявними системами інформаційної безпеки та іншими компонентами IT-інфраструктури організації. Важливо провести перевірку сумісності з уже наявними системами і переконатися в можливості обміну даними між ними. Така інтеграція дасть змогу створити єдине й ефективне рішення в галузі безпеки.

Масштабованість і гнучкість. При виборі слід враховувати її здатність до масштабування та адаптації зростаючих потреб організації. Важливо, щоб система була гнучкою і давала змогу налаштовувати політики безпеки відповідно до вимог і змін, що відбуваються в організації.

Зручність використання. Для вибору DLP-системи також слід звернути увагу на те, щоб користувацький інтерфейс і функціонал системи були інтуїтивно зрозумілими та зручними у використанні. Також важливо врахувати можливості автоматизації та централізованого управління системою, щоб полегшити її адміністрування та моніторинг.

Безпека. Дуже важливо враховувати рівень безпеки DLP-системи, вона повинна мати надійні механізми захисту, шифрування і контролю доступу до конфіденційних даних.

Репутація та надійність. Під час розгляду варіантів DLP-системи важливо приділяти увагу репутації та надійності постачальника. Рекомендується провести дослідження відгуків і рейтингів про системи, а також оцінити доступність і якість

підтримки, яку надає постачальник.

Вартість. На додаток до ціни ліцензії на DLP-систему, необхідно врахувати витрати на впровадження, навчання персоналу, підтримку та оновлення системи. Важливо провести оцінку загальної вартості володіння TCO (Total Cost of Ownership) і визначити, які варіанти є найбільш економічно вигідними.

Більшість систем отримують конкурентну перевагу завдяки своєму модулю аналізу. Виробники так акцентують увагу на цьому модулі, що часто називають свої продукти, наприклад, "DLP-рішення на основі міток". Тому користувачі обирають рішення виходячи не стільки з продуктивності, масштабованості або інших традиційних критеріїв корпоративного ринку інформаційної безпеки, а скоріше на основі типу аналізу документів, який використовується.

Очевидно, що використання тільки одного методу аналізу документів тягне за собою залежність рішення від цього методу, оскільки кожен метод має свої переваги та недоліки. Більшість виробників включають у свої системи кілька методів, при цьому один із них зазвичай виділяється як основний.

Контерний Аналіз - Цей метод ґрунтується на аналізі властивостей файлу або іншого сховища, такого як архів або криптодиск, у якому міститься інформація. Ці методи часто називаються "рішення на мітках", що ясно відображає їхню сутність. Кожне сховище має мітку, яка однозначно визначає тип вмісту, що знаходиться всередині. Ці методи практично не вимагають значних обчислювальних ресурсів для аналізу переміщуваної інформації, оскільки мітка повністю описує права користувача на переміщення контенту будь-яким шляхом.

Цей підхід має явні переваги: швидкий аналіз і повна відсутність помилкових спрацьовувань (коли система помилково визначає відкритий документ як конфіденційний). Такі методи іноді називаються "детерміністичними" в деяких джерелах.

Очевидні й недоліки цього підходу: система забезпечує захист тільки позначеної інформації, і якщо мітка не присутня, контент не буде захищено.

Потрібно розробити процедуру для привласнення міток новим і вхідним документам, а також систему, яка протидіятиме переміщенню інформації з поміченого контейнера в непомічений через операції з буфером, файлові операції, копіювання даних із тимчасових файлів тощо.

Якщо автор документа самостійно ставить мітки, то зі злого умислу він може опустити позначку для інформації, яку планує вкрасти. Навіть за відсутності злого наміру, з плином часу можуть виникнути недбалість або неуважність. Якщо потрібно, щоб мітки ставив певний співробітник, наприклад, інформаційний безпековець або системний адміністратор, то він не завжди зможе однозначно відрізнити конфіденційний контент від відкритого, оскільки не володіє всією необхідною інформацією про процеси в компанії.

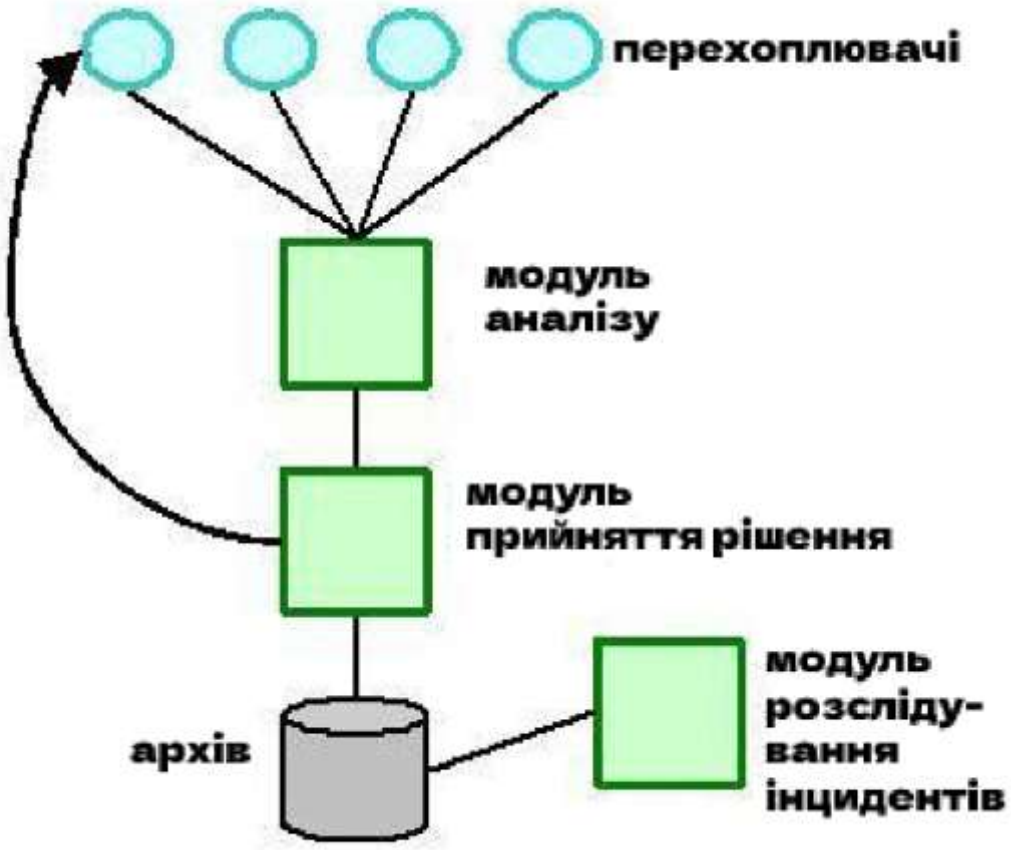

Рис. 1.6 Схема DLP-Системи.

1.4. Контейнерні структури в інформаційній безпеці

Захист документних сховищ є ключовим застосуванням рішень на основі міток. Коли компанія має сховище документів, яке оновлюється рідко, але відомі категорія та рівень конфіденційності кожного документа, організація його захисту стає простішою з використанням міток. Встановлення міток на документи, що надходять у сховище, можна організувати за допомогою певної процедури. Наприклад, перед надсиланням документа до сховища співробітник, відповідальний за управління сховищем, може звернутися до автора і фахівця, щоб визначити рівень конфіденційності документа. Особливо ефективним способом є використання форматних міток, де кожен вхідний документ зберігається в захищеному форматі та надається співробітнику для читання за запитом, вказуючи його як авторизованого читача. Сучасні рішення надають можливість встановлювати обмежений час доступу до документів, і після закінчення цього часу документ автоматично стає недоступним для читання. Така схема активно застосовується, наприклад, у видачі документації для державних закупівель у США. У цьому випадку система управління закупівлями створює документ, який можуть прочитати тільки учасники конкурсу, перелічені в ньому, і при цьому вони не можуть змінити або скопіювати його вміст. Ключ для доступу дійсний тільки до закінчення терміну подання документів на конкурс, після чого документ стає недоступним для читання.

Також з використанням міток компанії можуть організувати обмін документами в захищених сегментах мережі, де обробляється інтелектуальна власність і державна таємниця.

Зрозуміло, що успіх впровадження системи DLP пов'язаний з тісним зв'язком між процесом впровадження і загальною стратегією бізнесу компанії. Важливо зазначити, що DLP-система не може бути простим та ізольованим рішенням; вона повинна забезпечувати комплексний захист інформації протягом усього її життєвого циклу. Тому компаніям-замовникам не варто очікувати миттєвого,

ефективного та дешевого розв'язання проблеми, оскільки такого рішення немає в природі.

Участь акціонерів компанії є ще одним важливим аспектом впровадження DLP, і вона має починатися від самого початку проекту. В іншому випадку можуть виникнути розбіжності між функціоналом, що реалізується в DLP, і вимогами бізнесу організації. Це може призвести до неефективності DLP-системи або перешкоджати нормальному функціонуванню бізнес-процесів.

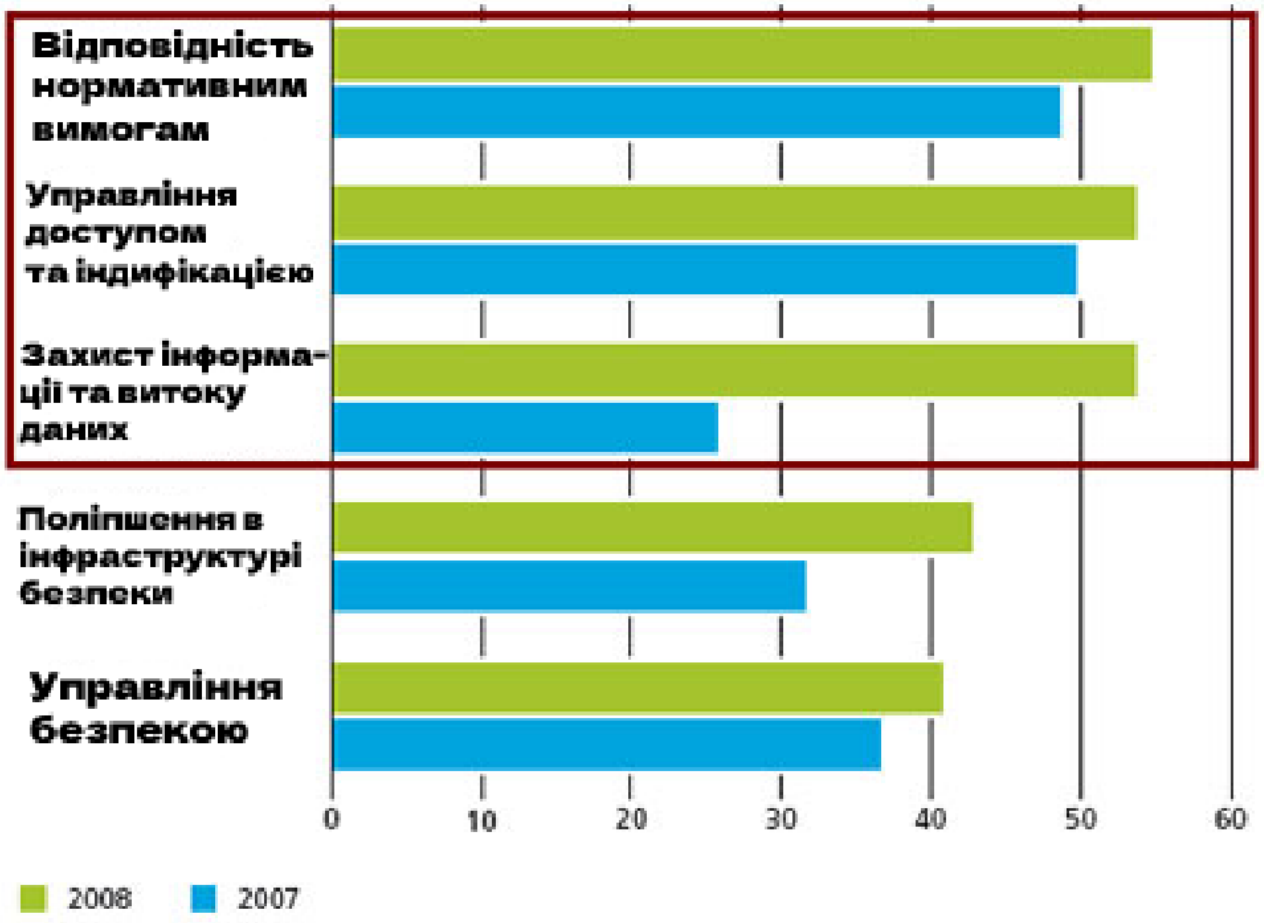

Рис. 1.7. Найбільш значимі ініціативи з безпеки

Згідно зі звітом іншої консалтингової компанії Deloitte, керівники бізнесу усвідомлюють цінність, яку являють собою DLP-системи. Дослідження вказує на три ключові ініціативи в галузі безпеки, які безпосередньо пов'язані із загальною

внутрішньою безпекою і особливо з DLP-системами. Ці результати підтверджують, що завдання стоять важливі та потребують вирішення.

2. МЕТОДИ ТА ЗАСОБИ ЩОДО ЗАХИСТУ ВІД ПОРУШЕНЬ ДАНИХ І КОНТРОЛЮ ПЕРСОНАЛУ НА БАЗІ SYMANTEC DLP

2.1. Модульна архітектура рішення Symantec DLP.

Symantec DLP надає комплексний захист інформації на всіх компонентах IT-інфраструктури організації:

- Моніторинг і блокування передавання інформації як усередині організації, так і за її межами.
- Виявлення конфіденційної інформації, доступної публічно, у файлових сховищах, веб-серверах, системах поштового обміну та документообігу.
- Захист конфіденційної інформації на робочих станціях і ноутбуках, включно з пристроями, що перебувають за межами корпоративної мережі- Контроль над мобільними додатками, хмарними і веб-сервісами, а також над одержуваною і відправленою електронною поштою на смартфонах і планшетних комп'ютерах.

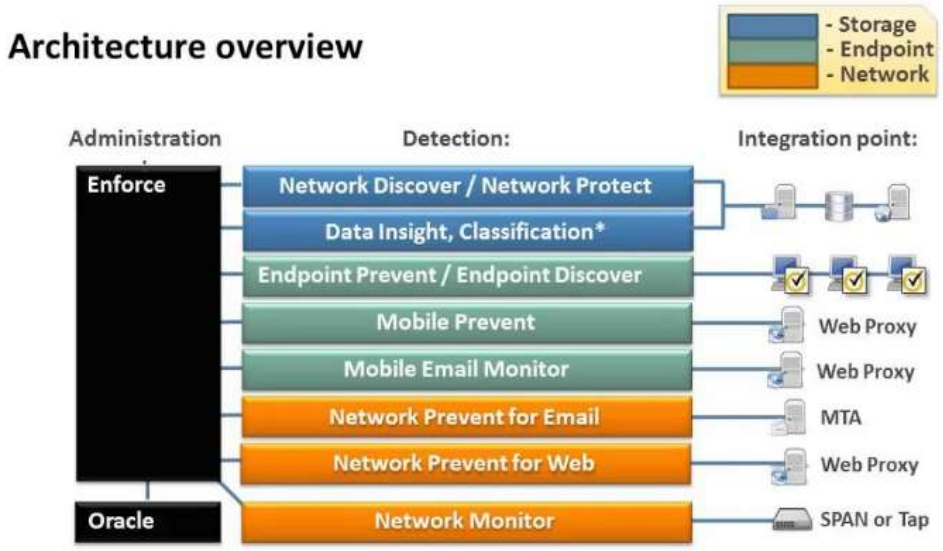

Рис. 2.1. Огляд роботи Symantec Data Loss Prevention

Таблиця 2.1.

Склад і призначення модулів Symantec DLP

Група модулів	**Функціональний склад**	**Призначення**
Enforce platform	Сервер Symantec DLP Enforce	Центральна платформа управління Symantec DLP
	Oracle Database for Symantec DLP	База даних для зберігання звітності, інцидентів, конфігурації та налаштувань системи
Endpoint	Symantec DLP Endpoint Discover	Виявлення конфіденційних даних на локальних дисках робочих станцій і ноутбуків
	Symantec DLP Endpoint Prevent	Контроль і запобігання витокам даних з робочих станцій і ноутбуків
Storage	Symantec DLP Network Discover	Виявлення конфіденційних даних розміщених на корпоративних сховищах інформації (файлові сервери, веб-сервери)
	Symantec DLP Data Insight	Відстеження використання інформації, розміщеної на сховищах, контроль прав доступу, визначення власників даних тощо.
	Symantec DLP Self-Service Remediation portal	Залучення власників до виправлення помилок розміщення КІ або зміни прав доступу на ресурси
	Symantec DLP Network Protect	Автоматичне виправлення розміщення КІ на файлових серверах і порталах Sharepoint (карантин)
	Symantec DLP Classification Server	Класифікація електронної пошти під час поміщення в архіви та журнали Symantec Enterprise Vault
Network	Symantec DLP Network Monitor	Контроль переміщення конфіденційних даних мережевими каналами зв'язку (пасивний)
	Symantec DLP Network Prevent for Web	Контроль переміщення конфіденційних даних мережевими каналами зв'язку (активний з можливістю блокування та аналізу шифрованого трафіку)
	Symantec DLP Network Prevent for Mail	
Mobile	Symantec DLP Mobile Prevent	Контроль конфіденційної інформації, що надсилається з мобільних пристроїв (пошта, додатки, веб-сервіси)
	Symantec DLP Mobile Email Monitor	Контроль завантажуваної на мобільні пристрої через пошту конфіденційної інформації
Symantec Management Platform	Symantec DLP IT Analytics	Додатковий модуль (безкоштовний) для розширеної звітності
	Symantec DLP Integration Component	Інструментарій автоматичного розгортання агентів і контролю їхньої роботи (безкоштовний)

Symantec DLP - це розподілена комплексна модульна система.

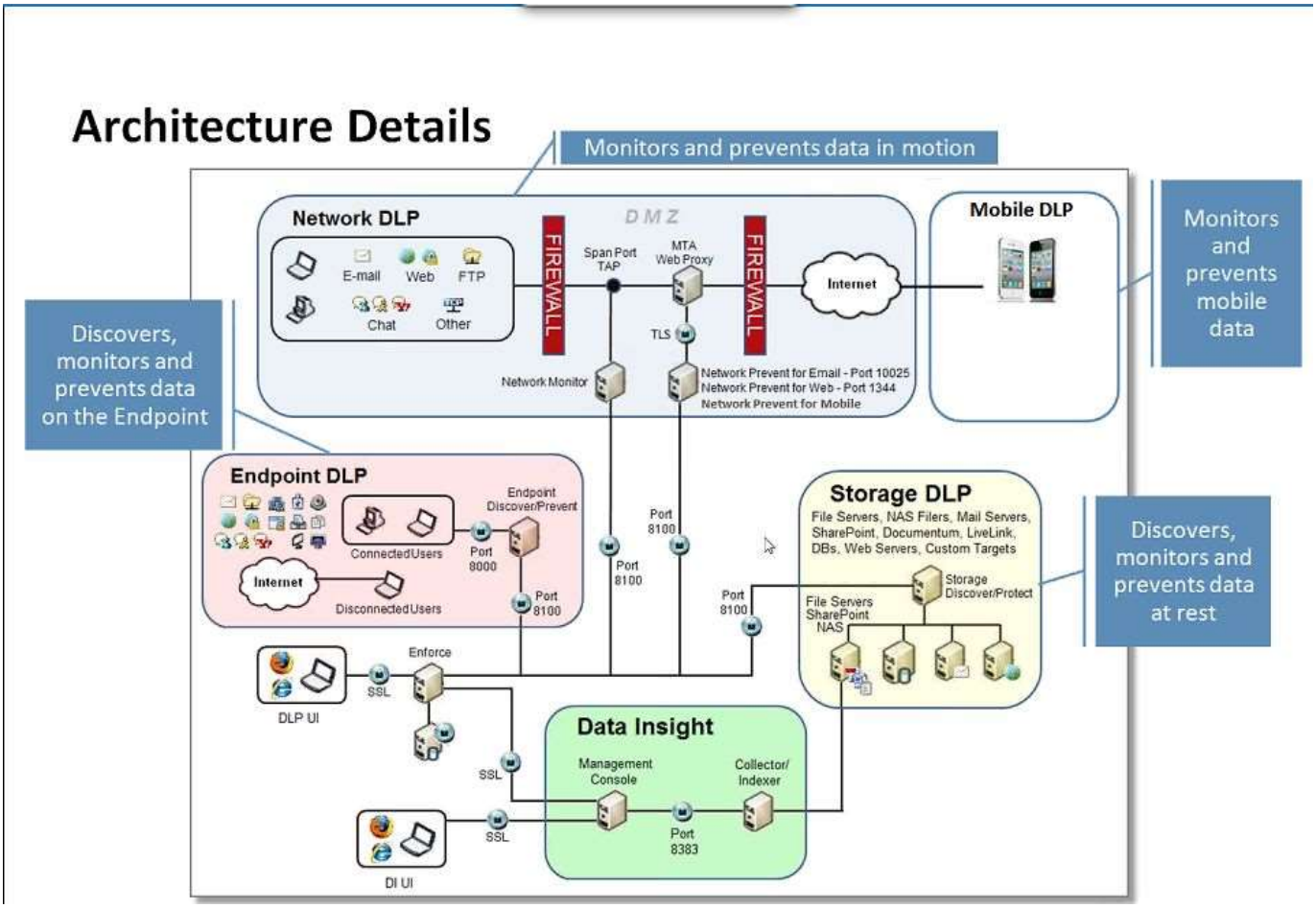

Рис. 2.2. Принципова схема роботи Symantec DLP

На рис. 2.2 представлено принципову схему розгортання і роботи Symantec.DLP. На відміну від більшості інших рішень, Symantec DLP пропонується у вигляді готового програмного забезпечення, готового до встановлення.

Модулі Symantec DLP можуть бути встановлені в різних комбінаціях на сумісному апаратному забезпеченні, що відповідає системним вимогам, включно з віртуальними серверами мати рішення.

2.2. Функціональні можливості Symantec DLP

Основною метою Symantec DLP є виявлення та запобігання передавання або обмеження доступу до конфіденційної інформації (КІ), що перебуває в:

- У файлах різних форматів на всіх ресурсах корпоративної мережі, включно зі стаціонарними та мобільними комп'ютерами, серверами, сховищами даних і загальними мережевими файловими ресурсами;
- У повідомленнях електронної пошти;
- Веб-трафіку;
- Під час запису на знімні носії інформації або компакт-диски CD/DVD;
- Під час надсилання документів на друк;
- Під час копіювання в буфер обміну;
- Під час запису на локальні диски;
- При копіюванні в загальні мережеві папки;
- Під час звернення додатків до конфіденційних даних;
- У документах, що надсилаються через інтернет-пейджери.

Для вирішення цього завдання Symantec DLP має в своєму розпорядженні кілька технологій виявлення КІ, що застосовуються спільно або окремо (залежно від характеру даних, що захищаються):

- Described Content Matching (DCM);
- Exact Data Matching (EDM);
- Indexed Document Matching (IDM);
- Vector Machine Learning (VML).

Друга функція Symantec DLP полягає у швидкому реагуванні на події, пов'язані з обміном, передачею або виявленням конфіденційної інформації на заборонених ресурсах згідно з визначеними правилами та політиками. Це включає попередження, переміщення в ізоляцію, блокування, зміну прав доступу, переміщення з небезпечного середовища на безпечні ресурси, шифрування та інші заходи.

Коли політика, пов'язана з потенційними або фактичними порушеннями інформаційної безпеки (витоком конфіденційної інформації), спрацьовує, Symantec

DLP активує механізм повідомлення і контролю для проведення розслідування інцидентів.

Отже, основним завданням Symantec DLP є запобігання несанкціонованому розкриттю конфіденційної інформації шляхом застосування різноманітних технологій і засобів технічного контролю, навчання персоналу правилам обробки конфіденційних даних і ретельного розслідування кожного інциденту, що стався.

Тепер перейдемо до розгляду функціональних можливостей кожного модуля, включеного до складу Symantec DLP.

Enforce Platform є основною інтеграційною та керуючою платформою Symantec DLP. Управління модулями DLP здійснюється через веб-інтерфейс, що дає змогу виконати такі операції:

- Отримання цифрових відбитків із неструктурованих даних;
- Отримання цифрових відбитків зі структурованих даних здійснюється шляхом завантаження файлу вивантаження у форматі CSV через веб-інтерфейс;
- Створення профілю захисту даних за допомогою Vector Machine Learning;
- Створення та редагування ідентифікаторів, які містять комбінацію регулярних виразів і перевірок;
- Створення політик засноване на використанні цифрових відбитків, ключових слів, профілів VML, регулярних виразів, ідентифікаторів, атрибутів файлів, ідентифікаторів знімних носіїв, розташування робочої станції, протоколів, списків користувачів, доменів, адрес електронної пошти та IP-адрес;
- Формування правил для реагування на спрацьовування політики;
- Створення цілей мережевого сканування;

- Додавання, зміна призначення, управління та видалення серверів виявлення;
- Створення груп політик;
- Перегляд і контроль системних повідомлень про події;
- Перегляд статистики мережевого трафіку;
- Збір логів модулів системи;
- Відстеження стану, видалення, зміна конфігурації та створення повідомлень про стан агентів, які встановлюються на робочихстанціях;
- Управління функціоналом контролю додатків;
- Створення, зміна та видалення ідентифікаторів знімних пристроїв;
- Керування основними параметрами системи, налаштуваннями мережевих протоколів, групами користувачів на основі груп Active Directory, зберігання облікових записів і управління інтеграцією з модулями Data Insight і Management Console. Створення та зміна атрибутів інцидентів, управління вивантаженням даних інцидентів в архів і управління користувачами та їхніми ролями.

Для контролю і моніторингу даних, що передаються через мережеві канали зв'язку, є група модулів Network, що включає Symantec DLP Network Monitor, Network Prevent for Web і Network Prevent for Mail.

Network Monitor - модуль, розроблений для аналізу скопійованого мережевого трафіку, який спрямовується на аналіз із використанням додаткового мережевого обладнання, такого як комутатори або пристрої TAP.

За допомогою модуля Network Monitor можна аналізувати протоколи, такі як SMTP, HTTP, NNTP, AOL, MSN, YAHOO, на основі сигнатур. Інші мережеві протоколи аналізуються на основі використовуваних ними мережевих портів.

Network Prevent for E-Mail це модуль, який призначений для аналізу та блокування електронної пошти, яка передається за протоколами SMTP або ESMTP, з технічної точки зору, він є (E)SMTP Proxy. Модуль забезпечує різні варіанти інтеграції з поштовою інфраструктурою, включно з можливістю впровадження в наявну інфраструктуру або паралельну обробку.

Network Prevent for Web - останній модуль у цій групі, він надає можливість аналізувати і блокувати трафік, що передається через Proxy-сервери. Модуль підтримує аналіз протоколів HTTP, HTTPS (у разі використання Proxy-серверів із можливістю дешифрування SSL-трафіку) і FTP через HTTP. Він надає можливість аналізувати і блокувати трафік, що передається через Proxy-сервери. Модуль підтримує аналіз протоколів HTTP, HTTPS (у разі використання Proxy-серверів із можливістю дешифрування SSL-трафіку) і FTP через HTTP.

Далі розглянемо функціональні можливості групи модулів Storage, яка включає в себе Symantec DLP Network Discover, Network Protect, Data Insight, Self-Service Remediation Portal і Classification server. Ця група модулів розроблена для забезпечення контролю за даними, що зберігаються на мережевих ресурсах компанії, у файлових сховищах і в системах електронного документообігу.

Network Discover - модуль, розроблений для виявлення даних на мережевих сховищах. Він здатний виявляти дані на файлових серверах, у файлових системах серверів, базах даних SQL, поштових серверах та інших джерелах.

Підтримується сканування таких джерел даних:

- Мережеві файлові системи (CIFS, NFS, DFS);
- Локальні файлові системи на серверах під керуванням ОС Microsoft Windows, Linux, Solaris, AIX;
- Веб-сервери;
- Microsoft Exchange;
- Microsoft Sharepoint 2007/2010/2013/2016/2019;

- База даних Lotus Notes, база даних SQL;
- Documentum;
- Livelink;
- Користувацькі додатки, дані з яких можуть бути витягнуті та передані Network Discover.

Сканування джерел здійснюється за розкладом з правами заданого користувача.

Network Protect. Цей модуль є розширенням модуля Network Discover і дає змогу переміщати або копіювати ті дані, які порушують політики безпеки. У разі переміщення файлів передбачено можливість залишати на їхньому місці файл-заглушку, що має ту саму назву, що й файл, який можна перенести, але із заданим текстом усередині.

Data Insight - модуль, призначений для відстеження різних дій, пов'язаних із файлами в системі. Модуль може бути використаний для збору інформації про те, хто створив файл, записав, читав тощо. Дані можуть бути зібрані з багатьох серверів і платформ, включно з Windows, Microsoft SharePoint, NetApp і EMC. Користувачі також можуть використовувати звіти, щоб отримати інформацію про доступ до файлів і місце, займане файлами на серверах. Крім того, модуль Data Insight дає змогу користувачам керувати доступом до файлів за допомогою політик безпеки, і блокувати доступ користувачів, яких немає в списку дозволених.

Можливості Data Insight дають змогу визначити нестандартну поведінку користувачів щодо доступу до даних. Компоненти Data Insight можуть бути встановлені на одному або декількох серверах відповідно до інфраструктури клієнта:

- Management - налаштування, управління, зберігання даних і надання звітності;

- Indexer - індексування та обробка даних, що передаються сумісно з collector;
- Collector - збір даних із серверів-джерел.

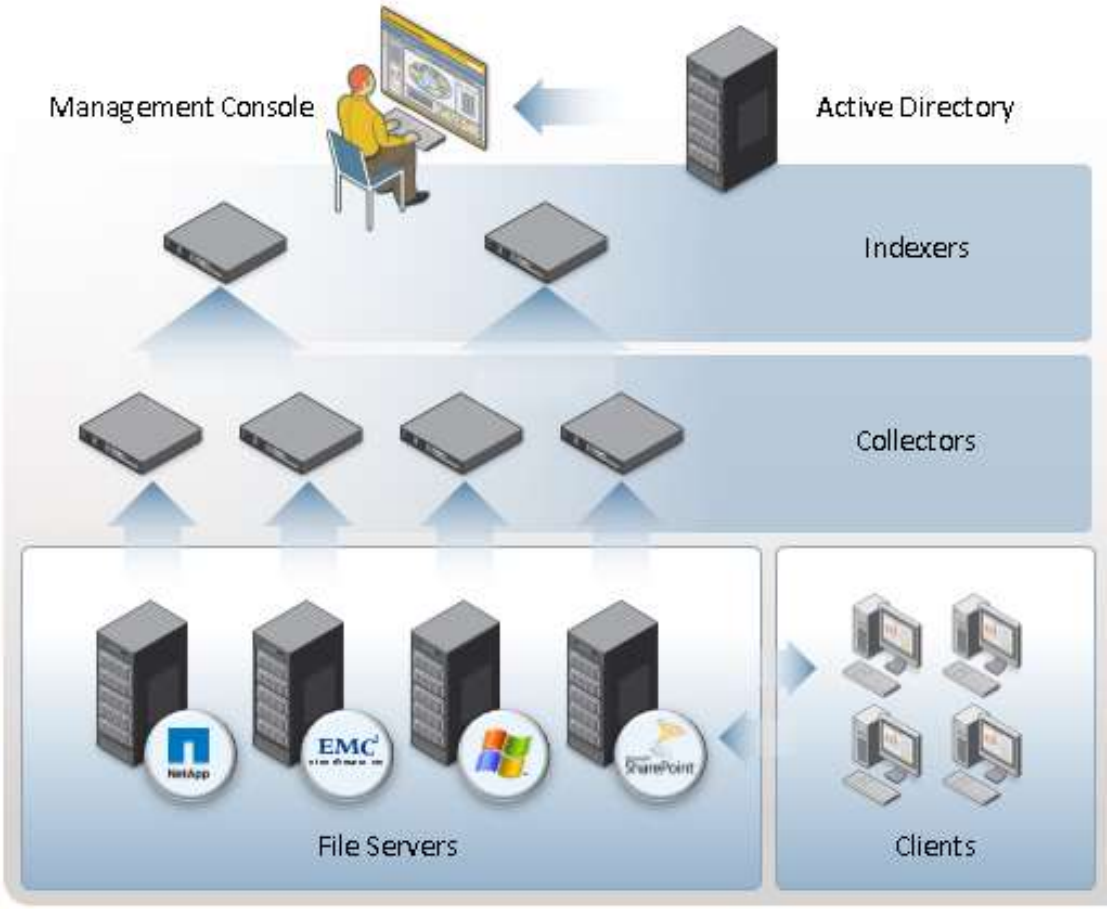

Рис. 2.3. Схема роботи та розгортання Data Insight зі складу Symantec DLP

Модуль Self-Service Remediation Portal для Data Insight надає можливість адміністраторам сховищ файлів і відділам безпеки залучати власників бізнес-даних для виправлення помилок у розміщенні критичної інформації, а також для зміни прав доступу до важливих даних, використовуючи веб-портал.

Classification Server - останій модуль, який входить до у групу Storage, функціонал цього модулю полягає в класифікації електронних листів, які зберігаються в архівах і журналах електронної пошти Symantec Enterprise Vault.

Для захисту кінцевих точок інфраструктури компанії використовуються модулі Symantec DLP Endpoint Discover і Endpoint Prevent.

Endpoint Discover - модуль, який відповідає за пошук і аналіз файлів, що знаходяться на робочих станціях. Для цього використовується Endpoint-агент, встановлений на комп'ютері.

Локальний аналіз файлів здійснюється на робочій станції, за винятком порівняння цифрових відбитків, для якого дані передаються на Endpoint-сервер. Після аналізу дані про інцидент передаються з агента на сервери Endpoint і потім на модуль Enforce шифрованим каналом. Сертифікат шифрування може бути як вбудованим, так і створеним додатково.

Для контролю дій користувачів на робочих станціях використовується модуль Endpoint Prevent. Контроль здійснюється за допомогою Endpoint-агента, який встановлюється на робочі станції та сервери.

Endpoint - агент аналізує дані, що передаються наступним чином:

- Запис на USB носій;
- Запис на локальний диск;
- Запис на SD і CF карти пам'яті;
- Копіюванняв буфер обміну;
- Запис на CD/DVD носії;
- Запис на загальні мережеві папки;
- Надсилання через POST-запити на веб-сторінки. Аналізу підлягає як HTTP протокол (для всіх браузерів), так і HTTPS (для браузерів Microsoft Internet Explorer і Mozilla Firefox);
- Відправлення даних електронною поштою через поштові клієнти Microsoft Outlook і Lotus Notes;
- Відправлення даних через інтернет-пейджери, такі як MSN, Yahoo тощо;

- Звернення програм до файлів і передача даних по мережі (Application Control).

Якщо на робочій станції порушуються політики, то Endpoint-агент може викликати діалогове вікно для користувача із запитом пояснень про причини виконання цієї дії.

Для забезпечення захисту даних, які передаються за допомогою мобільних пристроїв призначені модулі Symantec DLP Mobile Prevent і Mobile Email Monitor.

Symantec DLP Mobile Prevent - модуль, який забезпечує контроль інформації, що надсилається через мобільні пристрої iPad і iPhone в інтернет за протоколами HTTP/S і FTP. Він також дає змогу відстежувати мобільну пошту і додатки, як-от FaceBook, DropBox, Twitter, Gmail, GoodReader, тощо**.**

Для контролю пошти, яка передається на мобільні пристрої, використовується модуль Symantec DLP Mobile Email Monitor.

Додатковий контроль і управління Symantec DLP 12.5 здійснюється за допомогою Symantec Management Platform. До її складу входять Symantec DLP Integration Component і Symantec DLP IT Analytics.

Symantec DLP Integration Component - це компонент, розроблений для автоматизації процесу встановлення, обліку, оновлення та видалення агентів Symantec DLP. Цей компонент може бути додатково розширений і використовуватися як повноцінне рішення для управління патчами, інвентаризації тощо.

Symantec DLP IT Analytics забезпечує можливість отримання докладної звітності та створення індивідуальних звітів для багатьох продуктів Symantec, зокрема і для Symantec DLP 12.5.

У разі виявлення неправомірних дій користувача Symantec DLP 12.5 дозволяє:

- Заблокувати передачу даних;

- Зареєструвати порушення з блокуванням передачі або без;
- Створити тіньову копію даних;
- Повідомити користувача про вчинення неправомірної дії;
- Запросити пояснення у користувача щодо скоєних порушень;
- Повідомити працівника служби безпеки про порушення;

2.3. Аналіз процесу розробки та впровадження стратегії запобігання втраті даних.

У багатьох випадках успішність бізнесу безпосередньо пов'язана зі збереженням конфіденційності, цілісності та доступності інформації. У сучасних умовах однією з основних загроз інформаційній безпеці (ІБ) є несанкціонований доступ користувачів до конфіденційних даних та їхнє неправомірне використання.

Причина цього полягає в тому, що більшість традиційних засобів захисту, як-от антивіруси, міжмережеві екрани (Firewall) та системи запобігання вторгненням (IPS), не забезпечують надійний захист від внутрішніх порушників (інсайдерів). Інсайдери можуть мати на меті передачу конфіденційної інформації за межі компанії для подальшого використання, такого як продаж, передача третім особам або публікація у відкритому доступі. Такі засоби захисту не здатні ефективно запобігти таким діям. Системи запобігання витокам даних (DLP - Data Loss Prevention) призначені для розв'язання проблеми випадкових і навмисних витоків даних.

Подібні системи формують захищений "цифровий периметер" навколо організації, проводячи аналіз всієї вихідної та в деяких випадках, вхідної інформації. Вони контролюють не тільки інтернет-трафік, а й інші потоки інформації, як-от документи, що залишають захищену зону безпеки на зовнішніх носіях, друковані документи, що передаються на мобільні пристрої через Bluetooth, WiFi тощо.

DLP-системи проводять аналіз потоків даних, які перетинають периметр інформаційної системи, що захищається. Коли виявляється конфіденційна інформація в цих потоках, активна компонента системи спрацьовує і передача повідомлення (пакета, потоку, сесії) блокується. Виявлення конфіденційної інформації в потоках даних здійснюється шляхом аналізу вмісту та виявлення спеціальних ознак, таких як гриф документа, спеціальні мітки або значення хеш-функції з певного набору.

Під час вибору DLP-системи для захисту конфіденційної інформації від витоків необхідно враховувати безліч параметрів і характеристик. Одним із найважливіших параметрів є вибір мережевої архітектури. Відповідно до цього параметра продукти цього класу можна розділити на дві основні групи: шлюзові (рис. 2.3.) і хостові (рис. 2.4.).

У шлюзовій групі використовується єдиний сервер, на який спрямовується весь вихідний мережевий трафік корпоративної інформаційної системи. Цей шлюз здійснює обробку трафіку з метою виявлення можливих витоків конфіденційних даних.

Рис. 2.3. Функціональна схема шлюзового DLP-рішення

Другий варіант заснований на застосуванні спеціальних програмних агентів,

які встановлюються на кінцевих точках мережі, таких як робочі станції, сервери застосунків та інші.

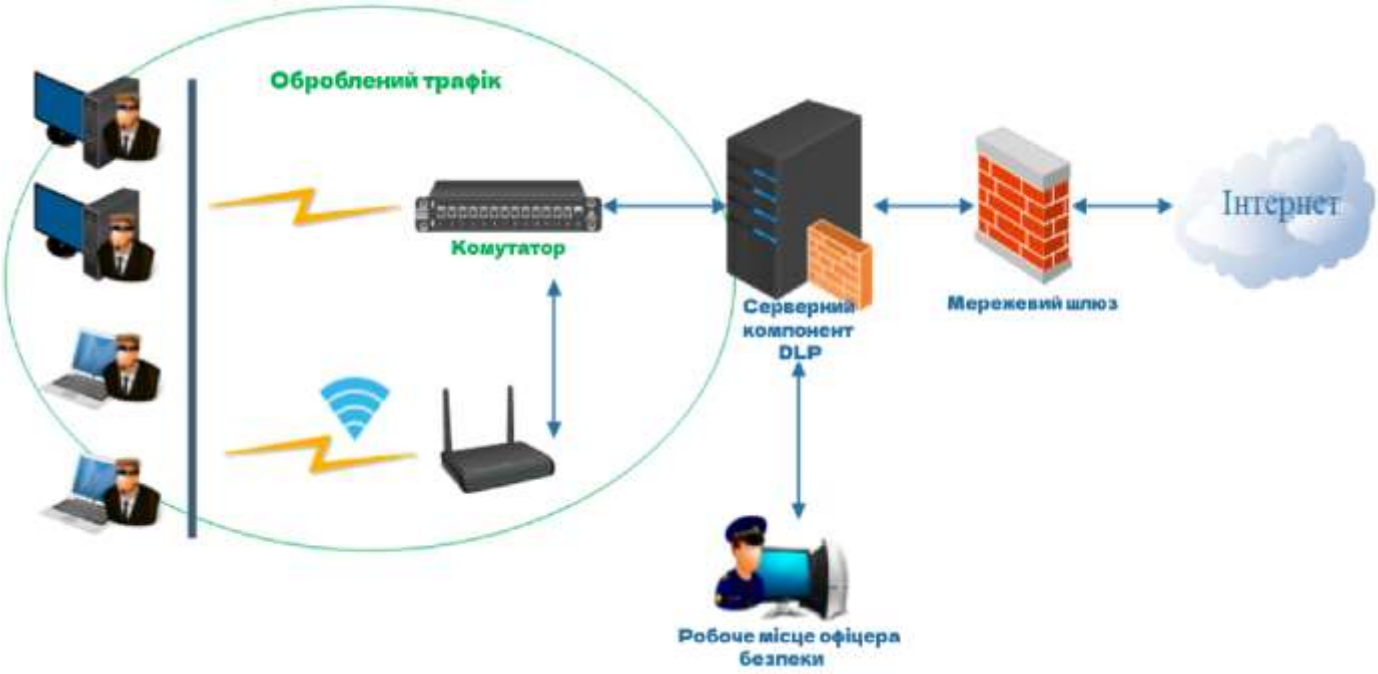

Рис. 2.4 Функціональна схема хостового DLP рішення

Останнім часом спостерігається стійка тенденція до об'єднання та універсалізації DLP-систем. На ринку майже не залишилося або зовсім не залишилося рішень, які можна було б чітко класифікувати як винятково хостові або шлюзові. Навіть розробники, які раніше фокусувалися лише на одному з цих напрямків, додають модулі другого типу до своїх рішень.

Причини переходу до універсалізації DLP-рішень дві. Перша з них - різні сфери застосування у систем різних типів. Як було сказано вище, хостові DLP-рішення дають змогу контролювати всілякі локальні, а мережеві - інтернет-канали витоку конфіденційної інформації. Грунтуючись на необхідності забезпечення повного захисту в переважній більшості випадків, організація стикається з потребою в обох підходах. Універсалізація DLP-систем зумовлена також

технологічними особливостями та обмеженнями, які можуть перешкодити шлюзовим системам забезпечити повний контроль над усіма інтернет-каналами, необхідними для захисту.

Враховуючи неможливість повної заборони використання потенційно небезпечних каналів передачі даних, можна встановити над ними контроль. Основна мета контролю полягає в моніторингу всієї інформації, що передається, виявленні конфіденційних даних серед неї та виконанні відповідних операцій відповідно до політики безпеки організації. Очевидно, що основним і найбільш значущим завданням є аналіз даних, оскільки від його якості залежить ефективність роботи всієї системи DLP.

2.4. Методи аналізу потоків даних для DLP

Аналіз потоку даних з метою виявлення конфіденційної інформації є складним завданням, яке можна сміливо назвати нетривіальним. Пошук необхідних даних ускладнений безліччю факторів, які потребують урахування. У зв'язку з цим на сьогоднішній день існує кілька технологій для виявлення спроб передачі конфіденційних даних. Кожна з цих технологій відрізняється своїм принципом роботи від інших.

Морфологічний аналіз. Цей метод широко поширений і активно використовується для виявлення витоків конфіденційної інформації. Він заснований на контентному аналізі переданого тексту з метою виявлення певних слів або фраз**.**

У децентралізованій організації співробітники повинні проявляти більше ініціативи та творчо вирішувати проблеми. Це також може допомогти встановити очікування щодо того, як працівники можуть відстежувати свій власний розвиток у компанії та підкреслювати певний набір навичок, а також для потенційних

працівників, щоб оцінити, чи така компанія буде добре відповідати їхнім власним інтересам і стилям роботи.

Основною перевагою цього методу є його універсальність. Його можна застосувати для контролю будь-яких видів зв'язку, починаючи від файлів, що копіюються на знімні накопичувачі, і закінчуючи повідомленнями в ICQ, Skype і соціальних мережах. Крім того, він здатний аналізувати будь-які тексти і відстежувати різну інформацію. Цей метод не вимагає попереднього опрацювання конфіденційних документів і активується відразу після застосування відповідних правил опрацювання, поширюючи свій захист на всі задані канали зв'язку.

Недоліком морфологічного аналізу є його відносно низька ефективність при визначенні конфіденційної інформації. Ця ефективність залежить як від алгоритмів, що використовуються в системі захисту, так і від якості семантичного ядра, що використовується для опису даних, які захищаються.

Незалежно від того, як працює корпоративне середовище, для обміну даними і отримання відповідних сервісів клієнтам організації необхідно створити клієнт-серверну архітеужність обробки.

Статистичний аналіз грунтуються на принципі ймовірного аналізу тексту, який дає змогу оцінити ступінь конфіденційності або відкритості інформації. Ці методи зазвичай вимагають попереднього навчання алгоритму, під час якого обчислюють імовірність наявності певних слів або словосполучень у конфіденційних документах.

Перевага статистичного аналізу полягає в його універсальності. Важливо зазначити, що ця технологія ефективно працює тільки за умови постійного навчання алгоритму. Наприклад, якщо система отримала недостатню кількість зразків договорів у процесі навчання, вона може не розпізнати факт їхнього передання. Тобто якість роботи статистичного аналізу залежить від правильного налаштування алгоритму. Крім того, слід враховувати, що ця технологія ґрунтується на ймовірнісному підході.

Шаблони або регулярні вирази. Процедура цього методу полягає у визначенні адміністратором безпеки шаблону конфіденційних даних, де вказується кількість символів і їхній тип (буква або цифра). Потім система здійснює пошук у текстах сполучень, що відповідають цьому шаблону, і застосовує задані правила дій до знайдених файлів або повідомлень.

Шаблони мають важливу перевагу - високу ефективність у виявленні передачі конфіденційної інформації. Коли йдеться про випадкові витоки, їхня здатність до виявлення наближається до 100%. Однак у випадках навмисних пересилань складнощі виникають. Зловмисник, маючи інформацію про можливості використовуваної DLP-системи, може протидіяти їй, наприклад, замінюючи символи різними альтернативними символами. Тому методи захисту конфіденційної інформації, які застосовуються, мають залишатися в секреті.

Цифрові відбитки. Цифровий відбиток у цьому контексті являє собою унікальний набір характеристик документа, за якими його можна з високим ступенем точності ідентифікувати в майбутньому. Сучасні рішення DLP можуть виявляти не тільки цілі файли, а й їхні фрагменти. Крім того, можна розрахувати ступінь відповідності, що дає змогу створювати різні правила, які описують різні дії залежно від відсотка збігу. Таким чином, ці рішення забезпечують можливість створення гнучких правил, заснованих на різних рівнях відповідності.

Цифрові відбитки мають важливу особливість - вони можуть бути застосовані не тільки до текстових документів, а й до табличних документів і зображень. Така різноманітність застосувань розширює сферу застосовності цієї технології.

Цифрові мітки. Цей метод ґрунтується на застосуванні спеціальних міток, які накладаються на обрані документи і видно тільки клієнтським модулям використовуваного DLP-рішення. Залежно від наявності цих міток, система дозволяє або забороняє певні дії з файлами. Це дає змогу не тільки запобігти витоку конфіденційних документів, а й обмежити доступ користувачів до них, що є значущою перевагою цієї технології.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВІД ПОРУШЕНЬ ДАНИХ І КОНТРОЛЮ ПЕРСОНАЛУ НА БАЗІ SYMANTEC DLP

3.1. Розробка рекомендацій щодо встановлення та налашування DLP-системи Symantec

В огляді розглядається Symantec Data Loss Prevention 12.5, комплексне DLP-рішення від корпорації Symantec, одного з визнаних лідерів світового ринку.

Для організацій з більш ніж 1000 користувачами рекомендується встановлювати кожен модуль Symantec DLP на окремий сервер для контролю. З версії 12.5 офіційно підтримується розгортання декількох модулів або навіть практично всіх на одному сервері.

Для Symantec DLP 12.5 передбачено кілька різних варіантів встановлення:

- Однорівневий;
- Дворівневий;
- Трирівневий.

У разі однорівневої установки база даних, Enforce-сервер і модулі виявлення розміщуються на одному сервері. Такий варіант установки рекомендується для компаній або філій з кількістю користувачів, що не перевищує 1000.

У разі дворівневої установки база даних і Enforce-сервер розміщуються на одному сервері, а модулі виявлення встановлюються на окремі сервери. Такий варіант установки може бути рекомендований, якщо в компанії відсутній окремий відділ підтримки баз даних, який міг би забезпечувати їх своєчасне обслуговування.

Для ситуацій, коли в компанії є відділ, що спеціалізується на обслуговуванні баз даних, компанія Symantec рекомендує використовувати трирівневий варіант установки.

У цьому варіанті всі компоненти Symantec DLP 12.5 встановлюються на окремі сервери.

Розгортання Symantec DLP відбувається за наступною схемою:

- Встановлення БД Oracle;
- Встановлення Enforce-сервера;
- Встановлення серверів виявлення;
- Встановлення Data Insight;
- Опціональне встановлення додаткових модулів, наприклад, Symantec IT Analytics;
- Встановлення агентів на кінцеві точки мережі.

У цьому варіанті встановлення для розгортання Symantec DLP 12.5 необхідне виділення в інфраструктурі щонайменше двох серверів.

Декілька типових схем розгортання окремих модулів. Варто зазначити, що ці варіанти дуже приблизні, і кінцева схема розгортання залежить від інфраструктури замовника. Давайте почнемо з модуля Symantec Network Monitor.

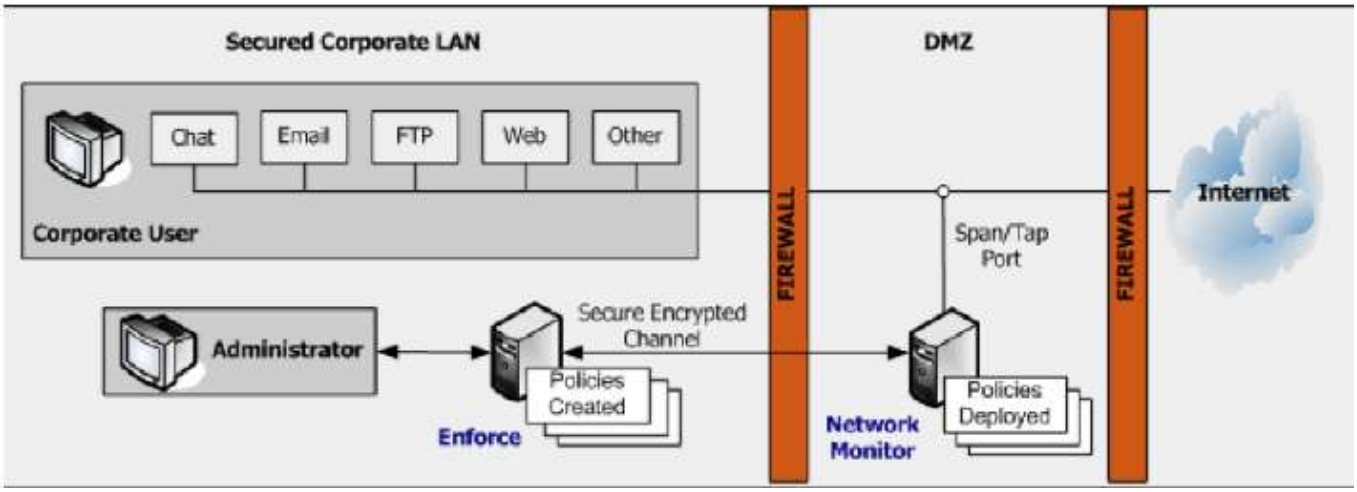

Рис. 3.1. Типова схема розгортання сервера з Symantec DLP Network Monitor 12.5

Зображення показує, що сервер Network Monitor отримує політики від сервера управління і шляхом опрацювання трафіку, отриманого з Span(Tap)-порту мережевого комутатора, здійснює пошук порушень цих політик.

Типовий варіант сервера Network Prevent for Email для захисту вихідної електронної пошти. Ця схема дає змогу відстежувати й аналізувати поштові повідомлення та вкладення, а також застосовувати до них різні дії, відповідно до заданих політик. Модуль Network Prevent for Web можна інтегрувати в інфраструктуру так, як показано на малюнку 3.3.

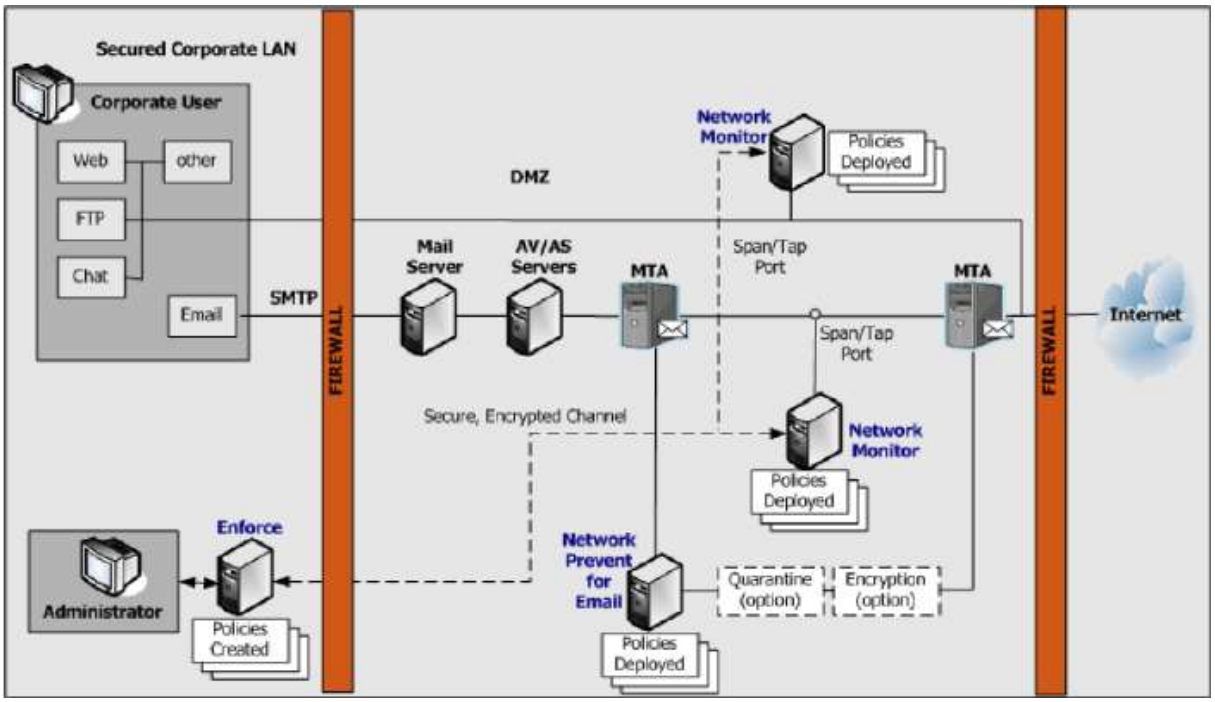

Рис. 3.2. Типова схема підключення модуля Symantec DLP Network Prevent for Web в інфраструктурі 12.5

Network Prevent Web працює спільно з проксі-сервером за протоколом ICAP**.**

Типова схема роботи модуля Mobile Email Monitor. Модуль Mobile Email Monitor дозволяє здійснювати нагляд за корпоративною електронною поштою, коли вона використовується з мобільних пристроїв. Під час запиту даних із мобільних пристроїв, інформація проходить через проксі-сервер, після чого надсилається на сервер Mobile Email Monitor для перевірки наявності конфіденційних даних.

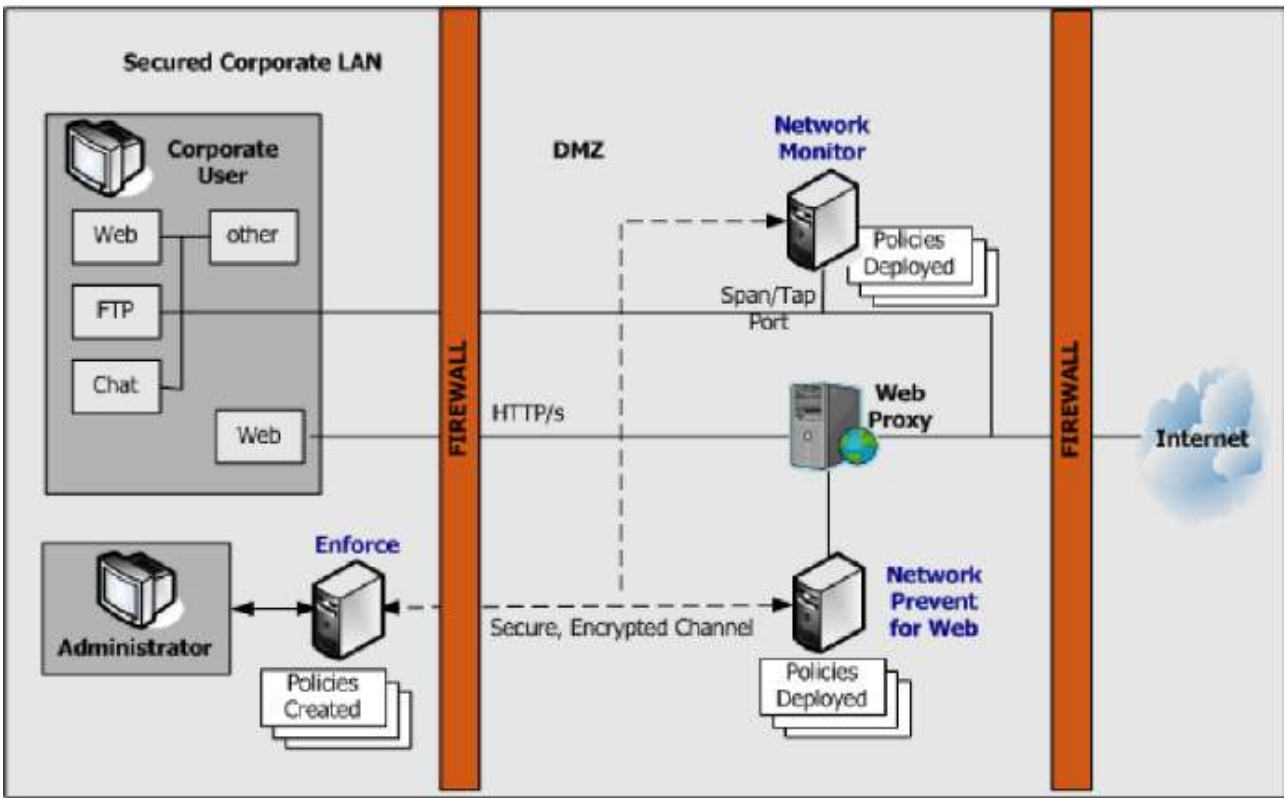

Рис. 3.3. Типова схема підключення модуля Symantec DLP Network Prevent for Web в інфраструктурі 12.5

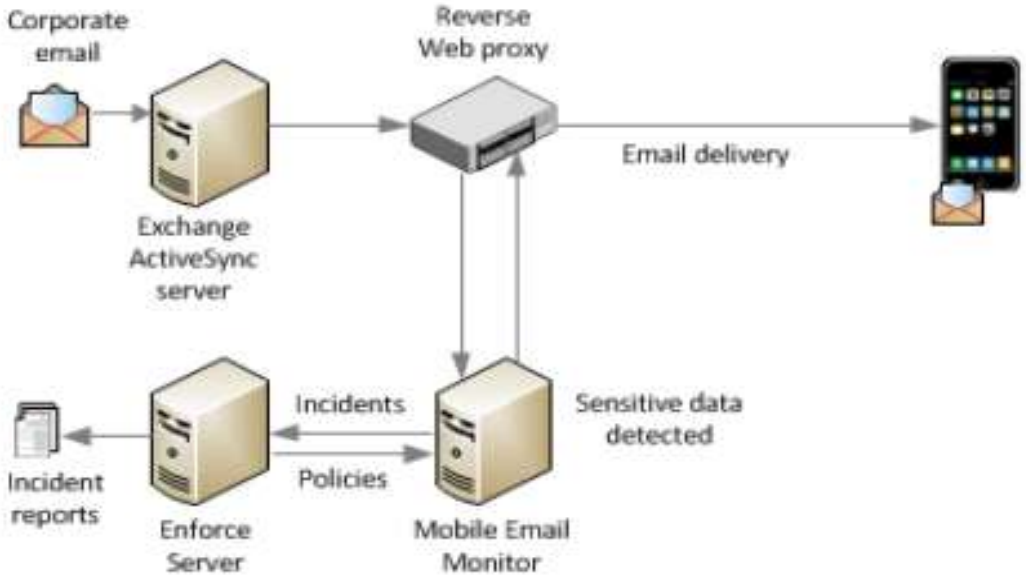

Рис. 3.4 Типова схема роботи модуля Symantec DLP Mobile Email Monitor 12.5

Типова схема підключення модуля Mobile Prevent for Web.

Для реалізації схеми потрібно, щоб мобільні пристрої підключалися до корпоративної інфраструктури через VPN-канал. У цьому випадку модуль Mobile Prevent for Web здатний контролювати трафік HTTP/HTTPS, FTP, ActiveSync і мобільних додатків. Однак, якщо пристрій підключається до корпоративної мережі без використання VPN, Mobile Prevent for Web не може здійснювати контроль передачі даних, за винятком ActiveSync. Проте, така схема роботи знімає навантаження з мобільного пристрою і дає змогу продовжити час роботи його батареї.

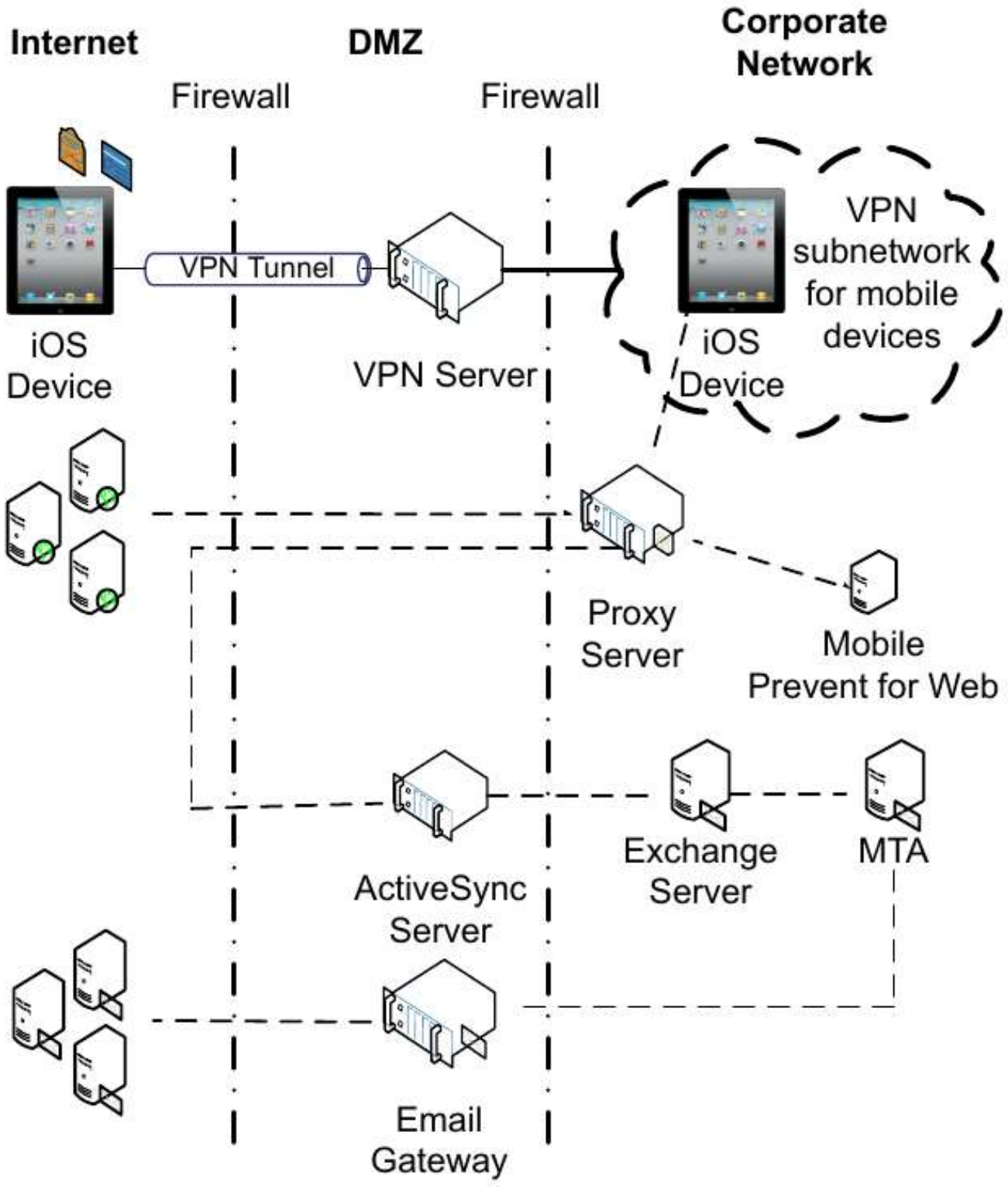

Рис. 3.5. Типова схема підключення Symantec DLP Mobile Prevent for Web 12.5

Інтеграція модулів Endpoint Discover і Endpoint Prevent у корпоративну інфраструктуру здійснюється схожим чином, як показано на малюнку 3.6.

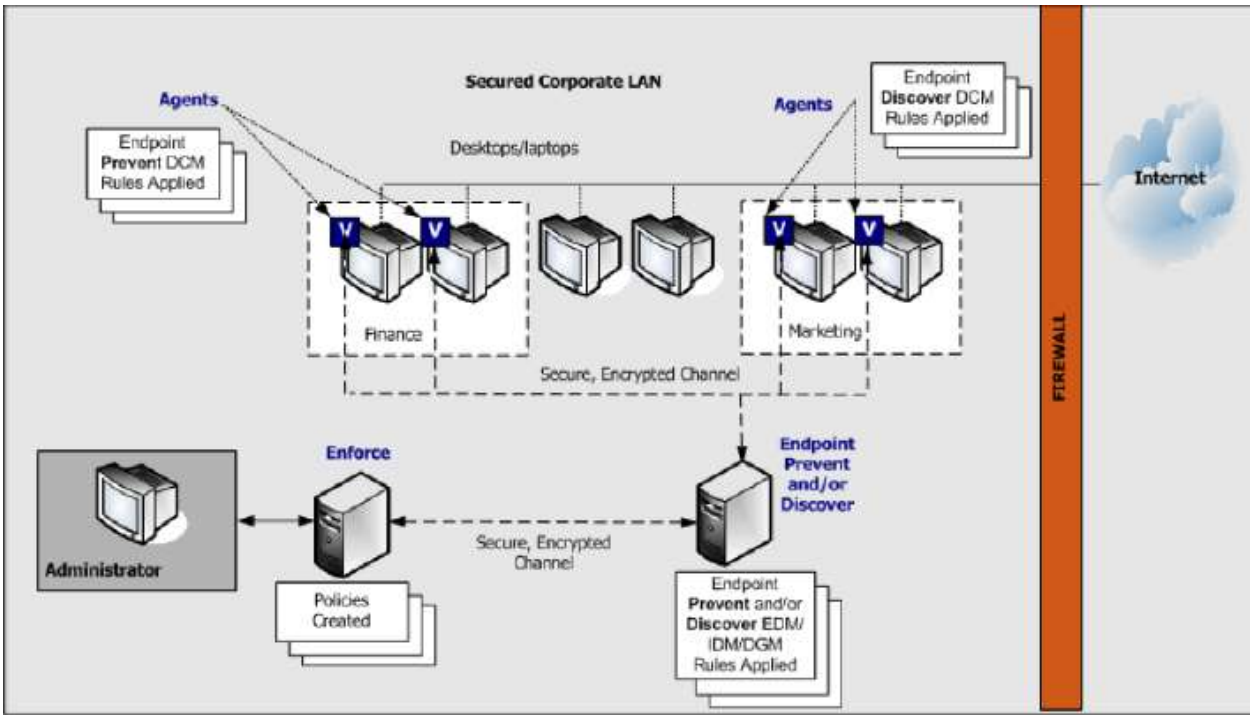

Рис. 3.6. Типова схема підключення модулів Symantec DLP Endpoint Discover і Endpoint Prevent 12.5

Архітектура роботи модулів Data Insight і Self-Service Remediation Portal виглядає приблизно так:

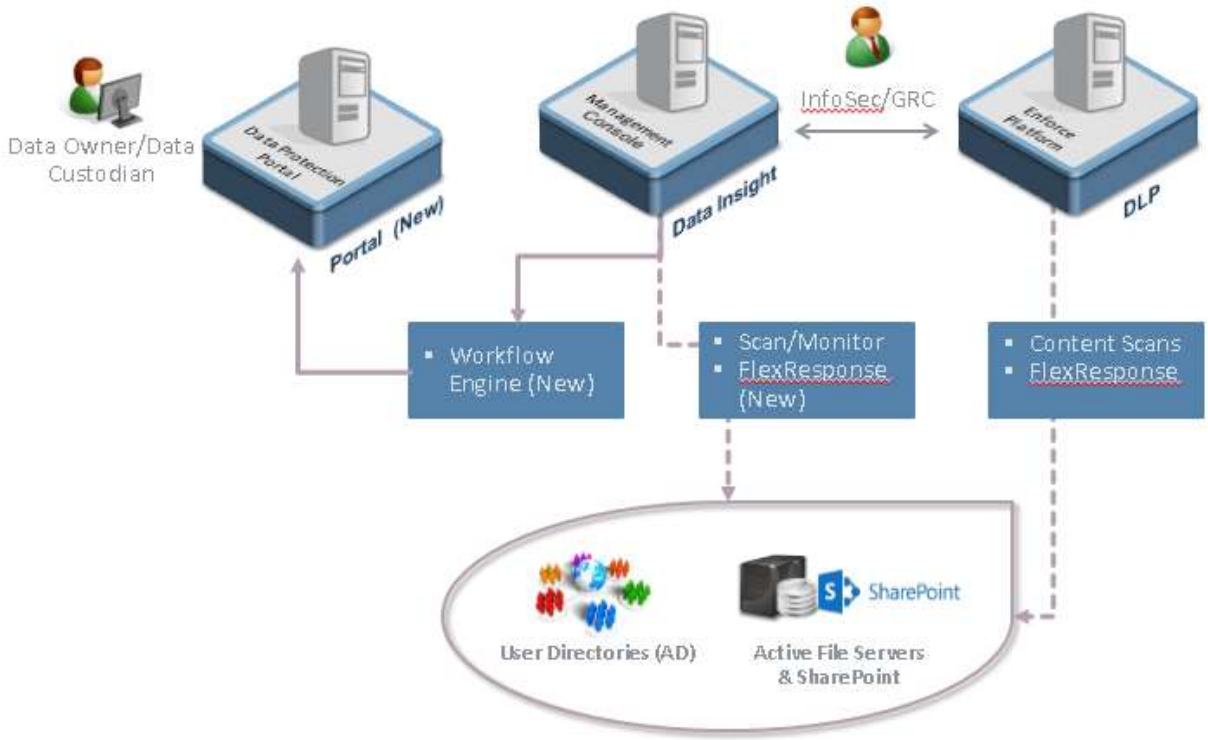

Рис. 3.7. Архітектура роботи модулів Symantec Data Insight і Self-Service Remediation Portal 12.5

Повністю описати всі етапи встановлення Symantec DLP 12.5 в рамках даної роботи не представляється можливим. Ми розглянули деякі ключові моменти. На цьому закінчимо короткий опис принципів розгортання Symantec DLP 12.5.

Також зважаючи на великий обсяг можливостей, не представляється можливим у повному обсязі розповісти про всі аспекти роботи з Symantec DLP. Як приклад розглянемо основні робочі завдання.

Після завершення всіх початкових етапів розгортання Symantec DLP 12.5, можна приступити до використання та налаштуванню системи.

Внутрішній доступ до даних у Symantec DLP можливий тільки через веб-інтерфейс. Для забезпечення підвищеного рівня безпеки в роботі з Symantec DLP 12.5 використовується система ролей з деталізованим розподілом прав доступу. Доступ до даних регулюється на основі різних атрибутів системи, інцидентів,

користувачів тощо. Якщо необхідно, можна створювати додаткові атрибути і використовувати їх для контролю доступу.

Завдяки інтеграції з Active Directory, користувачі можуть зручно отримати доступ до консолі системи DLP, використовуючи свої звичні облікові дані. У поєднанні з рольовою моделлю доступу, інтеграція з AD дозволяє навіть керівникам підрозділів отримати доступ до системи для контролю своїх підлеглих.

Рис. 3.8. Головне вікно веб-консолі Symantec DLP 12.5

На самому початку потрібно встановити з'єднання між Enforce-сервером і розгорнутими серверами виявлення. Потім слід налаштувати політики системи. Для цього достатньо використовувати консоль управління, де можна навести як приклад модуль Symantec DLP Mobile Email Monitor.

Рекомендується проводити підключення та налаштування сервера Mobile Email Monitor за таким алгоритмом:

- Додавання та налаштування нового сервера Mobile Email Monitor;
- Налаштування проксі-сервера;
- Налаштування сервісів ICAP на проксі-сервері для перенаправлення трафіку на сервер Mobile Email Monitor;

- Налаштування режиму відповіді (respmod) на проксі-сервері;
- Додавання на проксі-сервер цифрового сертифіката;
- Налаштування облікових записів пошти;
- Створення та застосування політики безпеки для Mobile Email Monitor;
  - Тест реагування системи на інциденти згідно зі створеною політикою.

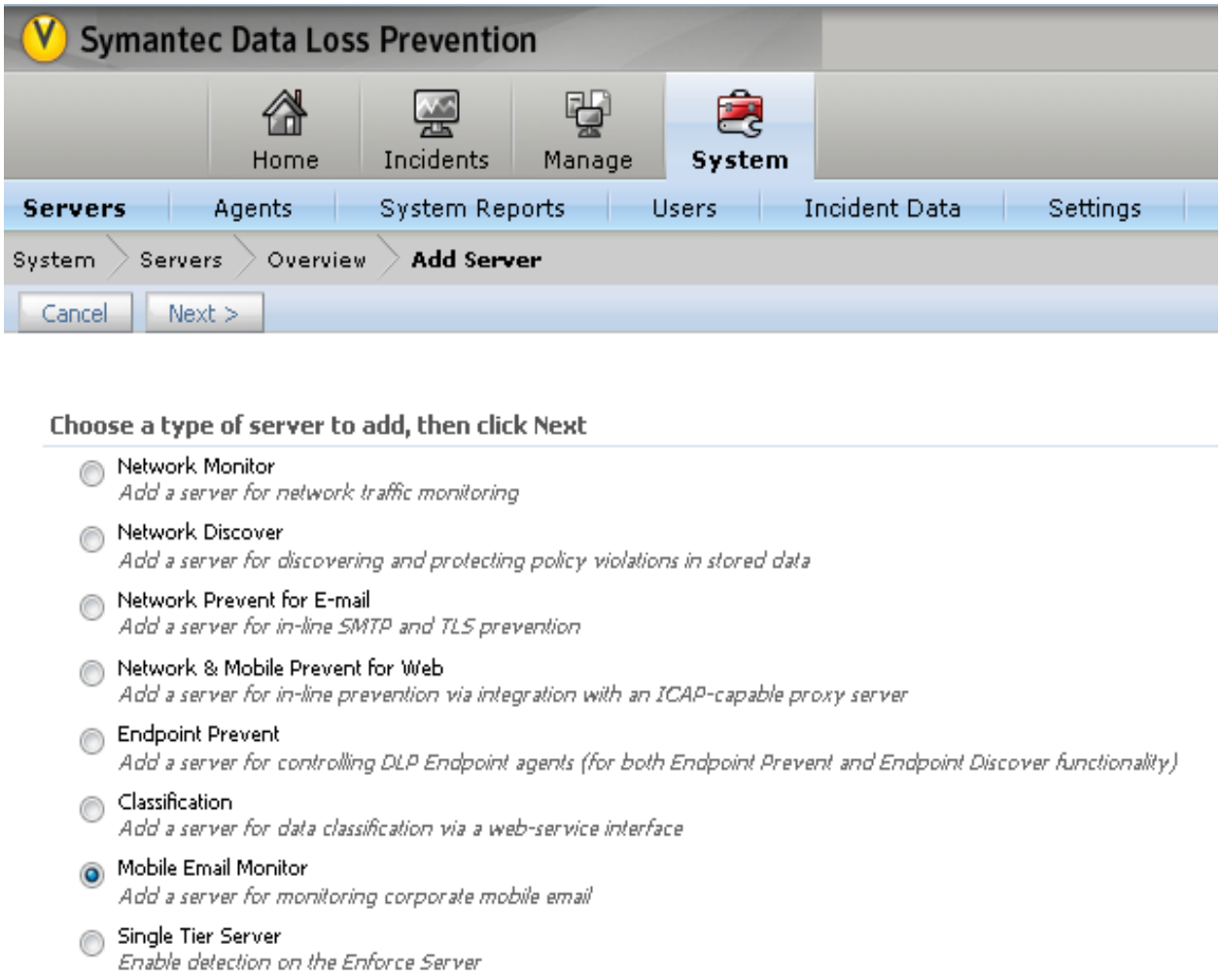

Рис. 3.9. Підключення сервера Mobile Email Monitor до Enforce-сервера за допомогою консолі управління Symantec DLP 12.5

На рис 3.10. показано розширені налаштування сервера Mobile Email

Monitor.

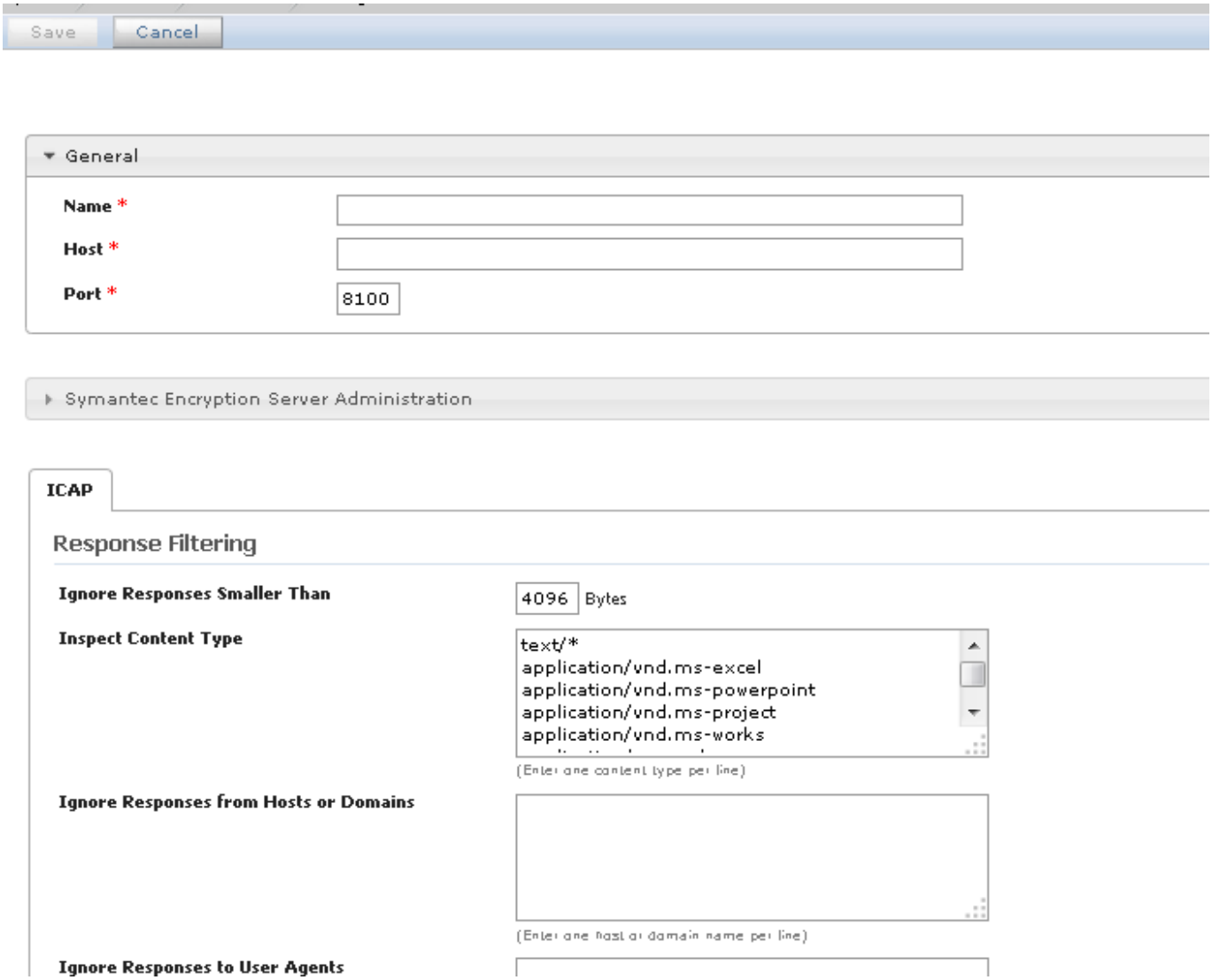

Рис. 3.10. Розширені налаштування сервера Symantec DLP Mobile Email Monitor 12.5

Давайте зосередимося на створенні тестової політики, яку використовуватимуть для перевірки функціональності сервера.

У Symantec DLP 12.5 політики представлені у вигляді набору правил, які дозволяють виявляти вміст, контекст і приймати відповідні реакції. Політики можуть бути створені користувачем або базуватися на попередньо встановлених шаблонах. У поточній версії Symantec DLP надається 65 різних шаблонів політик.

Таблиця 3.1.

Склад політик Symantec DLP 12.5 Symantec DLP 12.5

Компонент	**Необхідність**	**Пояснення**
Ім'я політики	Обов'язково	Ім'я політики має бути унікальним
Група політики	Обов'язково	Політика має бути призначена групі політик
Правила політики та винятки	Обов'язково	Політика повинна містити правила, які визначають хоча б одну умову збігу
Профілі даних і винятки	Може знадобитися	Профілі даних необхідно задавати в політиці, якщо методи виявлення в політиці їх вимагають. (EDM, IDM, VML)
Група користувачів і винятки	Може знадобитися	Зазначення групи користувачів необхідне в тому разі, якщо групові методи в політиці цього вимагають
Опис політики	Опціонально	Використовується для полегшення адміністрування
Правила реагування та винятки	Опціонально	Використовуються в тому разі, якщо потрібно реагування системи на інцидент у разі спрацьовування політики
Винятки	Опціонально	Використовуються для зазначення об'єктів. Вони можуть включати інформацію певної категорії, профілі даних (включно з цифровими відбитками тощо), протоколи, веб-домени, поштові домени та інші.

У таблиці подано компоненти політики, де вказано, які з них є обов'язковими, а які - необов'язковими.

3.2. Розробка загальних рекомендацій щодо використання Symantec DLP в огранізаціях

Коли йдеться про використання Symantec DLP в організаціях, важливо адаптувати загальні рекомендації під конкретні потреби та характеристики кожної організації. Це дасть змогу максимально ефективно використовувати систему для захисту інформації та запобігання.

Визначення цілей і вимог: Першим кроком є визначення цілей і вимог організації від використання Symantec DLP. Це може включати захист конфіденційної інформації, дотримання регуляторних вимог, запобігання витокам даних та інші аспекти інформаційної безпеки. Чітке визначення цілей допоможе зосередитися на конкретних аспектах, які необхідно забезпечити під час використання Symantec DLP.

Проведення аналізу ризиків: Важливим кроком є проведення аналізу ризиків інформаційної безпеки. Це дасть змогу ідентифікувати потенційні джерела витоку інформації та оцінити можливі наслідки. Аналіз ризиків допоможе визначити пріоритети і приділити особливу увагу тим областям, де найбільш вірогідні витоки даних.

Налаштування політик безпеки: Symantec DLP надає гнучкі інструменти для налаштування політик безпеки. Важливо визначити, які типи даних і активів необхідно захищати, і створити відповідні політики. Це може включати визначення конфіденційних даних, встановлення правил доступу та використання, а також моніторинг і виявлення витоків. Кожна організація має свої унікальні потреби, і налаштування політик має бути адаптоване під них.

Чутливість даних: Оцініть рівень чутливості даних, з якими працює ваша організація. Це допоможе визначити, які типи даних потребують особливої уваги та додаткових заходів безпеки.

Розмір і структура організації: Врахуйте розмір вашої організації та її структуру, оскільки це може вплинути на розподіл повноважень і відповідальності в рамках системи Symantec DLP.

Навчання та інформування співробітників: Поширення знань та інформування співробітників про використання Symantec DLP є ключовим аспектом успішного впровадження. Проведення навчальних програм і створення інформаційних матеріалів допоможуть підвищити поінформованість співробітників про загрози інформаційній безпеці та про те, як ефективно використовувати систему DLP для запобігання витокам даних.

Технічні можливості: Проаналізуйте технічні можливості вашої організації, включно з наявністю необхідних апаратних і програмних ресурсів, щоб визначити, які функції Symantec DLP можуть бути використані найбільш ефективно.

Моніторинг та аналіз результатів: Після впровадження Symantec DLP важливо проводити моніторинг і аналіз результатів. Система надає можливість збирати дані про події та інциденти, пов'язані з інформаційною безпекою. Регулярний аналіз цих даних допоможе ідентифікувати потенційні вразливості, поліпшити політики безпеки та вживати додаткових заходів для запобігання витокам даних.

Постійне вдосконалення: Використання Symantec DLP має розглядатися як процес безперервного вдосконалення. Технології та загрози інформаційної безпеки постійно розвиваються, і необхідно підтримувати систему актуальною. Регулярне оновлення системи, аналіз нових трендів і технологій допоможуть організації адаптуватися до мінливого загрозливого середовища.

Адаптація загальних рекомендацій Symantec DLP під конкретні потреби та характеристики вашої організації забезпечить ефективний захист інформації та

запобіжить витоку даних відповідно до унікальних вимог вашої компанії.

ВИСНОВКИ

В результаті виконання бакалаврської роботи було розглянуто проблеми витоку інформації з інформаційних систем організацій, які можуть мати серйозні наслідки, включно зі шкодою репутації, фінансовими втратами та юридичними проблемами. Витоки інформації стають все більш актуальними і серйозними в сучасному інформаційному суспільстві.

DLP-систему Symantec було вивчено як ефективний інструмент забезпечення інформаційної безпеки компанії та підприємств. Її широкий спектр функціональних можливостей, масштабованість, інтеграція та високий рівень безпеки роблять її конкурентоспроможним рішенням на ринку.

Результати дослідження дали змогу визначити основні шляхи витоку інформації, класифікувати й оцінити загрози інформаційній безпеці, а також виявити роль DLP-системи Symantec у виявленні та запобіганні витоку даних. Symantec DLP володіє розвиненими можливостями виявлення і класифікації конфіденційної інформації, гнучкістю налаштування політик безпеки і високим рівнем безпеки, що дозволяє ефективно боротися з сучасними загрозами і запобігати витоку інформації.

У процесі аналізу наявних випадків витоків інформації та їхніх наслідків було виявлено основні слабкі місця та ризики, пов'язані з інформаційною безпекою. Це підкреслює необхідність вжиття відповідних заходів щодо захисту даних і застосування DLP-системи Symantec в організаціях.

Загалом, використання DLP-системи Symantec являє собою ефективний підхід до захисту від витоку інформації в інформаційних системах організацій. Правильна конфігурація та налаштування Symantec DLP, спільно з розробленими рекомендаціями, дадуть змогу організаціям знизити ризики інформаційної безпеки, захистити конфіденційні дані та забезпечити надійний захист від витоків інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ушатов В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки / В. Ушатов, О. Сєвєрінов // GLOBAL CYBER SECURITY FORUM. Матеріали першого міжнародного науково-практичного форуму – Х.: ХНУРЕ, 2019. – С. 104-105.

3. Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах / А.В. Платоненко. Матеріали Науково-технічної конференції «Світ телекомунікації та інформатизації». – ДУТ. – 2015 р

4. Міжнародний стандарт ISO/IEC 27001 «Інформаційні технології – Методи безпеки – Системи управління інформаційною безпекою – Вимоги».

5. Johansen G. Digital forensics and incident response: an intelligent way to respond to attacks. – 2017.

6. Chapple M., Stewart J. M., Gibson D. (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide. – John Wiley & Sons, 2018.

7. Можливості Symantec DLP - [Електронний ресурс] Режим доступу: https://www.antimalware.ru/products/symantec-dlp

8. Закон України “Про Інформацію”: Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650 [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

9. Сучасні загрози інформаційної безпеки для державних та приватних установ України / А.В. Платоненко // Сучасний захист інформації. – 2015. – № 4, С.86-90.

10. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу

11. Хорошко В.А., Методи і інструмети захисту інформації. / Хорошко В.А., Чекатков А.М. // К.: Юниор, 2003. – С. 504

КОПІЇ ДЕМОНСТРАЦІЙНИХ АРКУШІВ