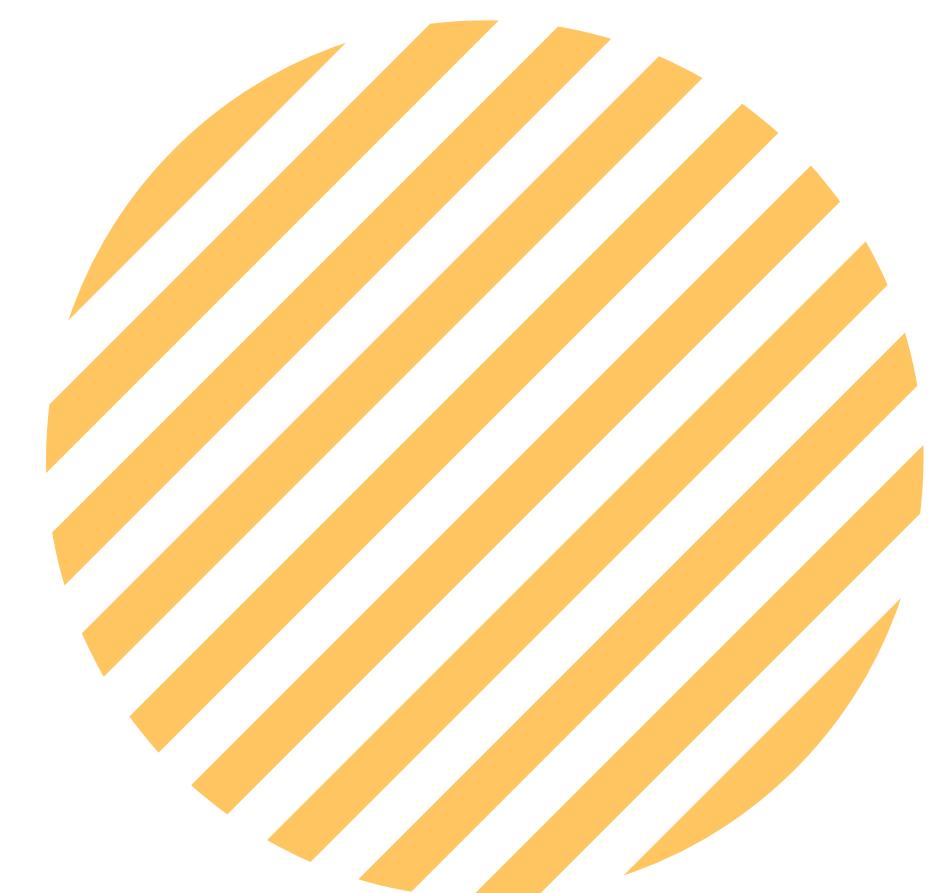


Аналіз методів і засобів запобігання витоку конфіденційних даних на пристроях зберігання даних

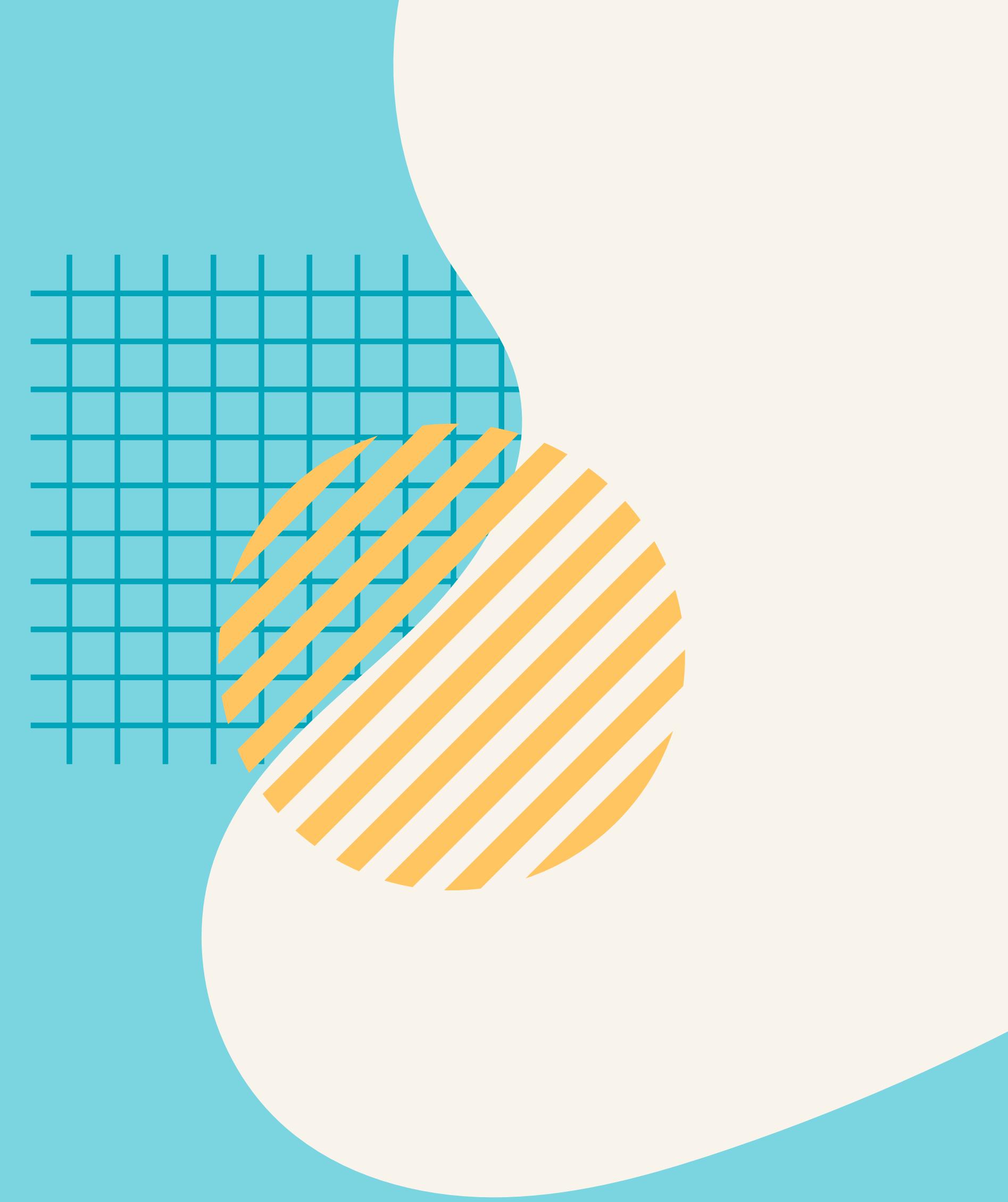
Студентки 4 курсу
Групи ДА-81 Желєзнової В.С.

Керівник доц., к.т.н. Капшук О.О.



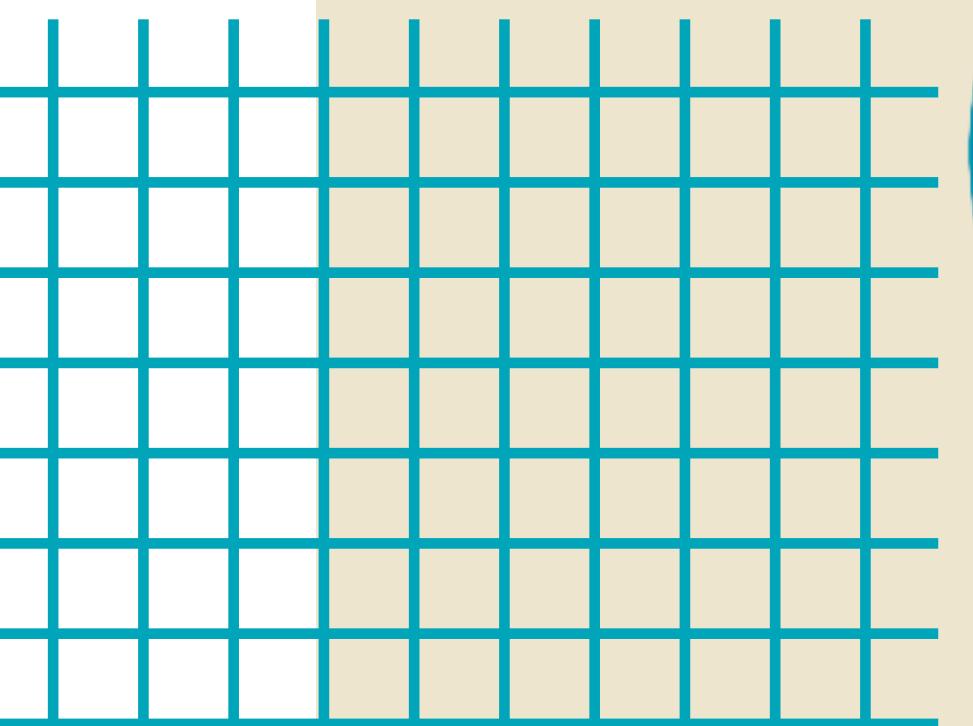
Зміст

1. Витік конфіденційних даних
2. Класифікація видів витоку інформації
3. Канали витоку
4. Поняття DLP
5. Класифікація DLP-систем
6. Методи аналізу потоків даних для DLP
7. Основні функції DLP-систем
8. Symantec DLP
9. Архітектура Symantec DLP 12.5
10. Схема роботи Symantec DLP
11. Функціональні можливості Symantec DLC
12. Переваги
13. Недоліки



Витік конфіденційних даних

Витік даних – неправомірна передача конфіденційних даних (матеріалів, важливих для різних компаній чи держави, персональних даних громадян), яка може бути навмисною чи випадковою.



Класифікація видів витоку інформації

Умисні витоки інформації відбуваються навмисно: користувач, який мав доступ до цінних відомостей знат про можливі негативні наслідки своїх дій і розумів, що вони мають протиправний характер.



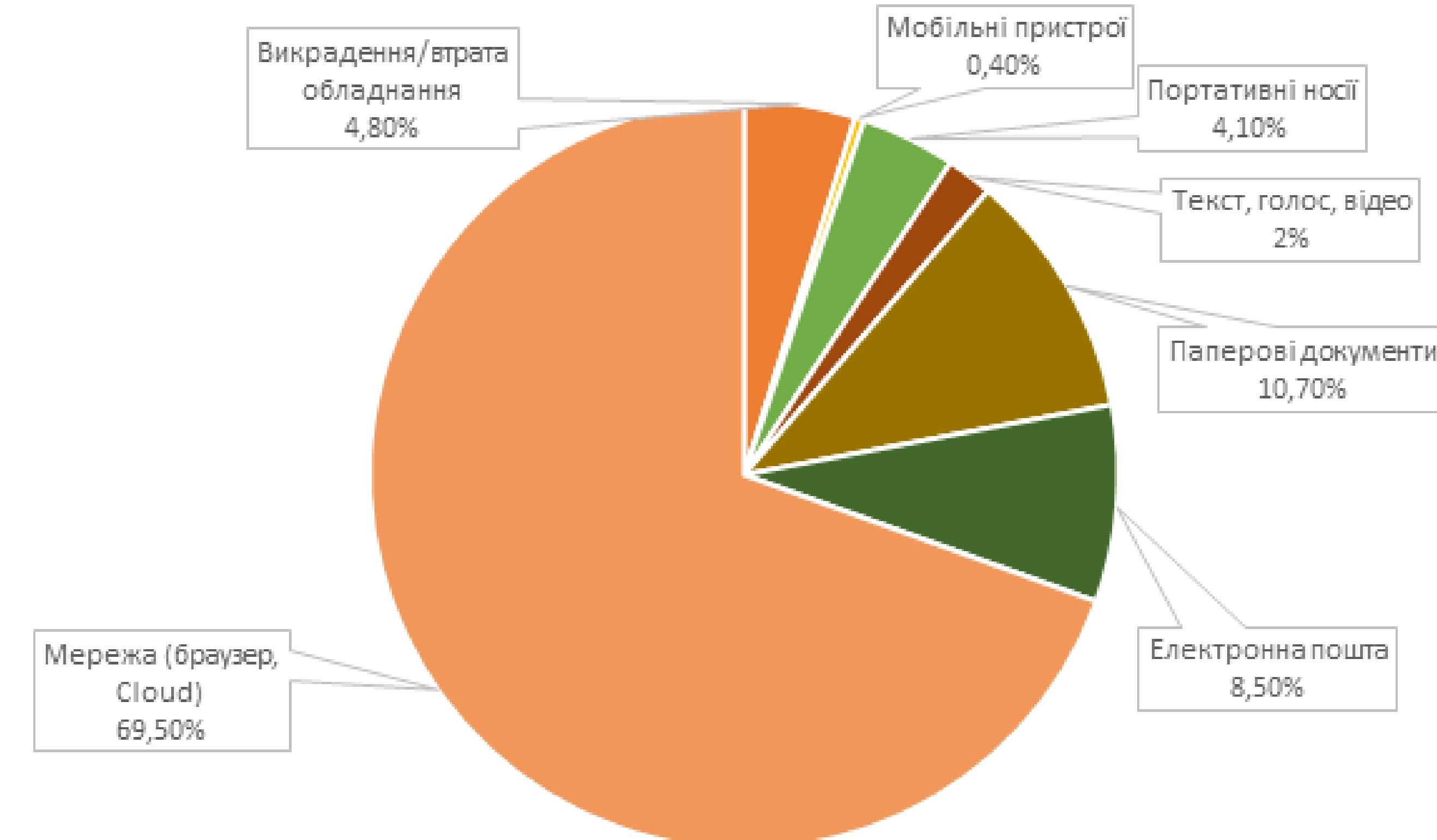
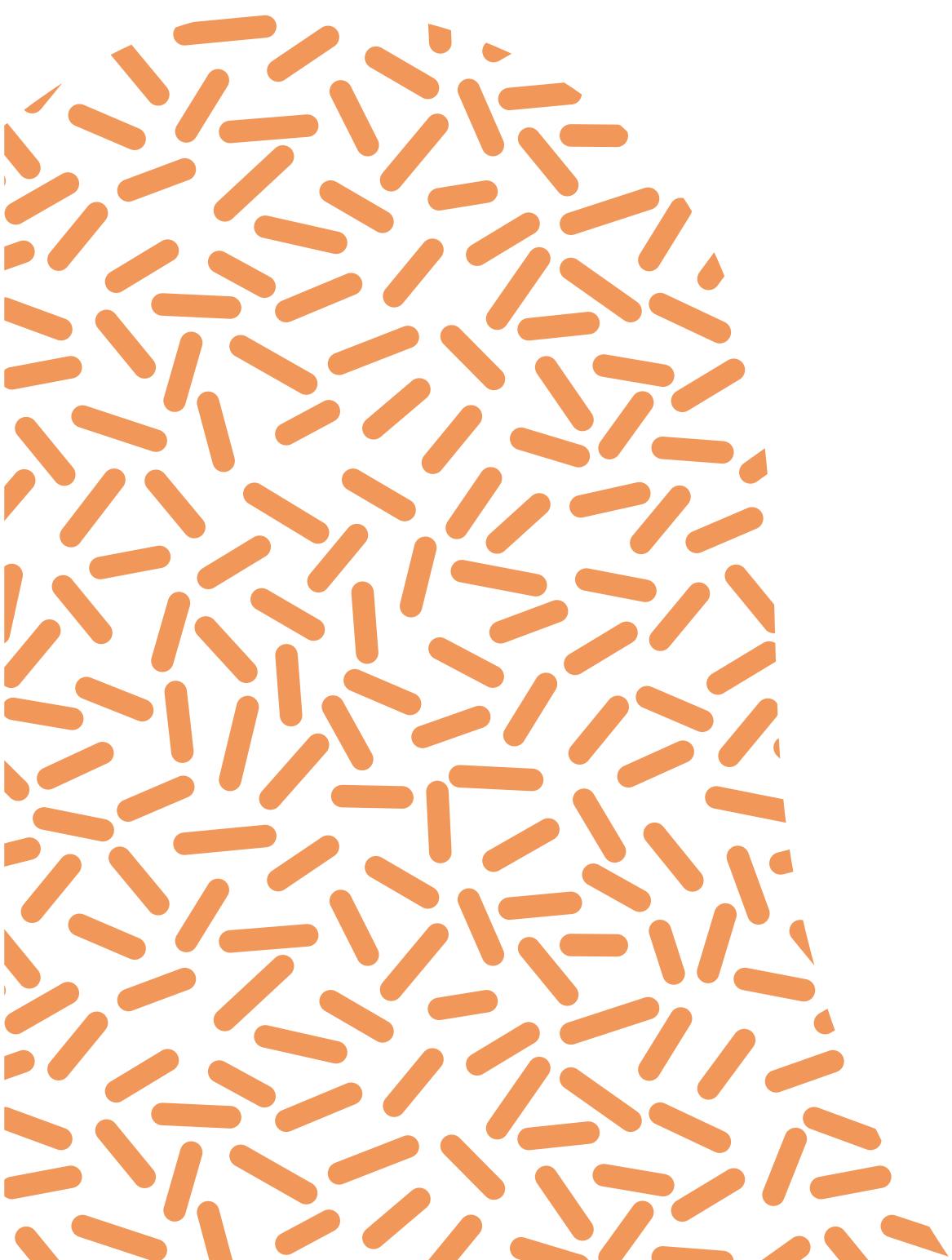
- Інсайдери та надлишкові права
- Крадіжка інформації ззовні
- Зламування ПО
- Шкідливі програми (бедкори, трояни)
- Крадіжки носіїв

Випадкові витоки інформації – інциденти ненавмисної передачі інформації, що захищається, особі, яка не повинна мати до них доступу.



- Мобільні телефони та смартфони
- Планшети та ноутбуки
- Електронна пошта та месенджери
- Файлообмінники

Канали витоку



- Викрадення/втрата обладнання
- Текст, голос, відео
- Мережа (браузер, Cloud)

- Мобільні пристрой
- Паперові документи

- Портативні носії
- Електронна пошта

Поняття DLP

Запобігання витоку (англ. Data Leak Prevention, DLP) – технології запобігання витоку конфіденційної інформації з інформаційної системи зовні, а також технічні пристрой (програмні або програмно-апаратні) для запобігання витокам.

Подібного роду системи створюють захищений «цифровий периметр» навколо організації, аналізуючи всю вихідну, а часом і входну інформацію. Контрольована інформація виступає не тільки інтернет-трафік, але й ряд інших інформаційних потоків: документи, які виносяться за межі захисту контуру безпеки на зовнішніх носіях, що роздруковуються на принтері, що відправляються на мобільні носії через Bluetooth, WiFi тощо.

Класифікація DLP-систем

Усі DLP-системи можна розділити за низкою ознак кілька основних класів.

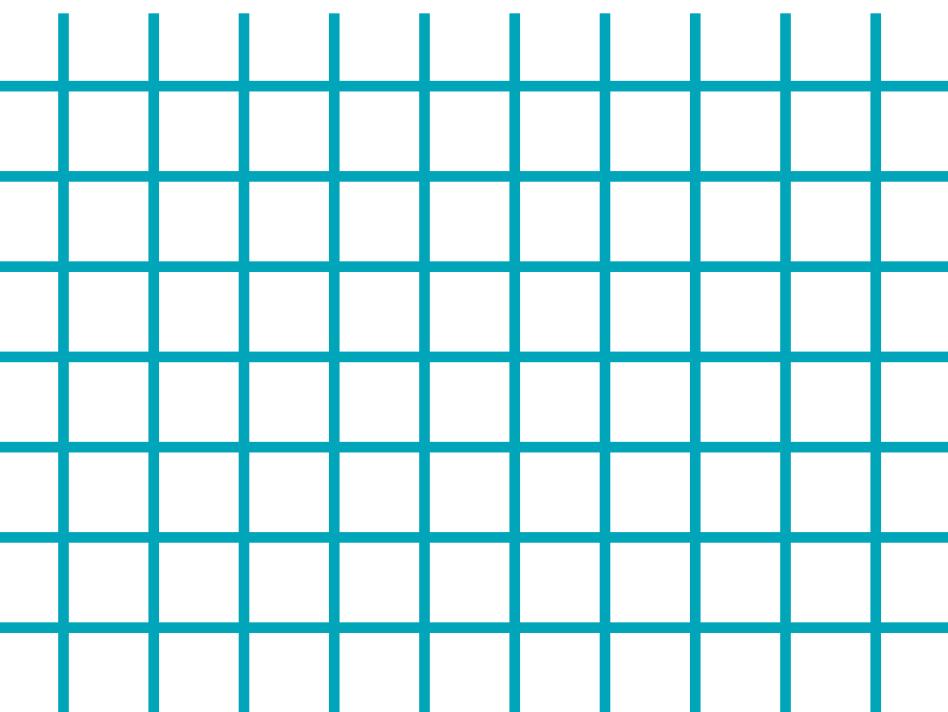
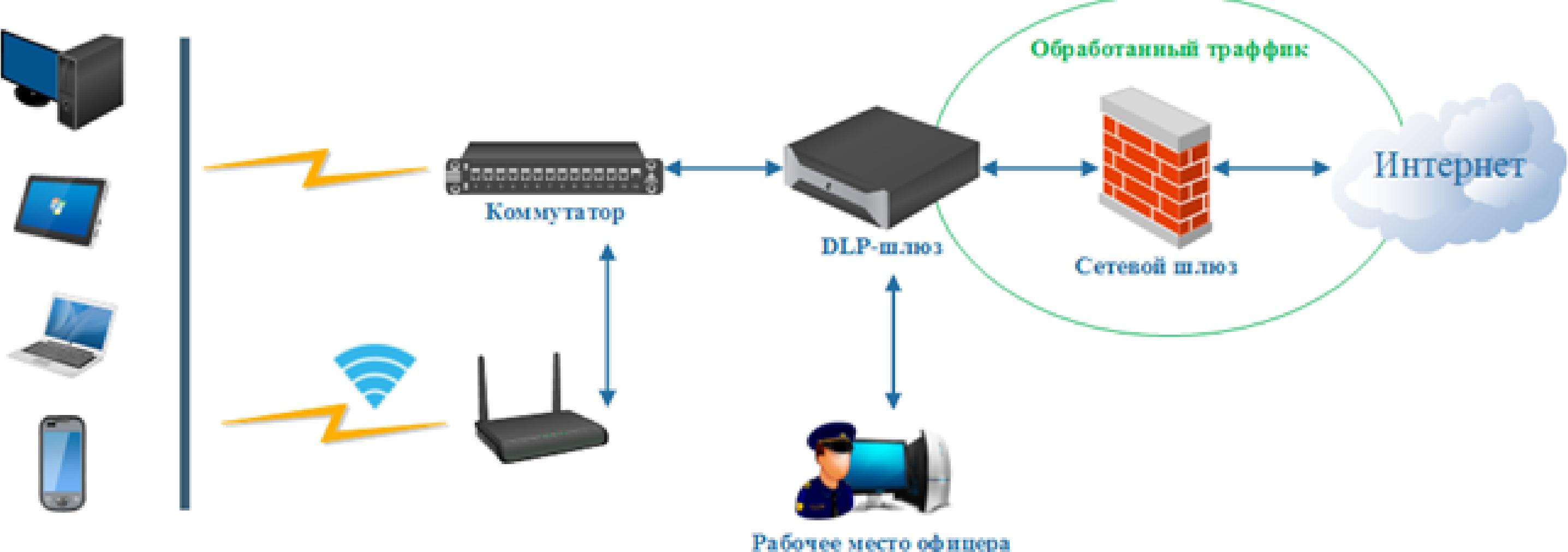
За здатністю блокування інформації, упізнаної як конфіденційна, виділяють системи з активним та пасивним контролем дій користувача.

Активні вміють блокувати передану інформацію, пасивні такої здатності не мають. Активні системи краще борються з випадковими витоками даних, але при цьому здатні допустити випадкову зупинку бізнес-процесів організації, пасивні ж безпечні для бізнес-процесів, але підходять тільки для боротьби з систематичними витоками.

Ще одна класифікація DLP-систем проводиться за їхньою мережевою архітектурою.

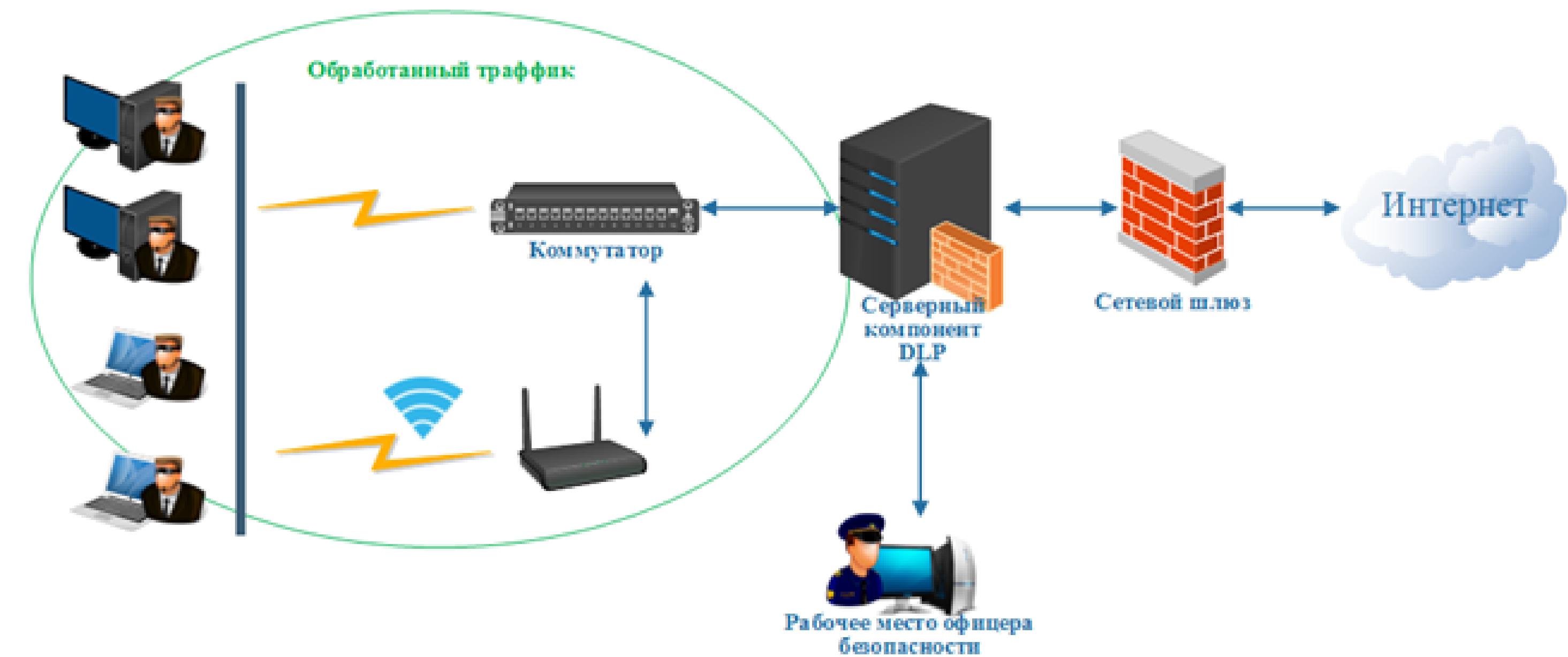
Шлюзові DLP

У шлюзових використовується єдиний сервер, який направляється весь вихідний мережевий трафік корпоративної інформаційної системи. Цей шлюз займається його обробкою з метою виявлення можливих витоків конфіденційних даних.



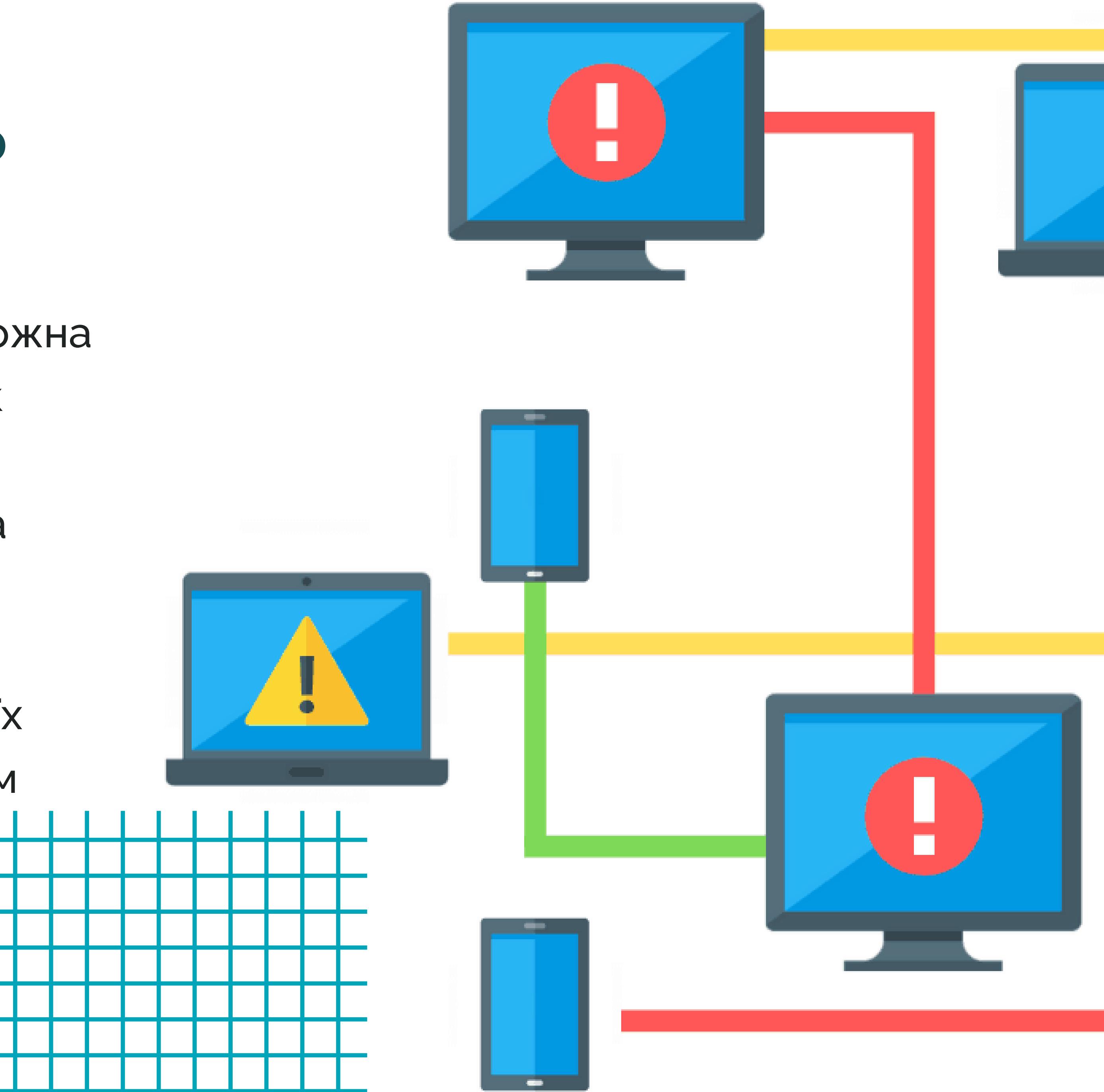
Хостові DLP

Хостові DLP засновані на використанні спеціальних програм – агентів, які встановлюються на кінцевих вузлах мережі – робочих станціях, серверах додатків та ін.



Методи аналізу потоків даних для DLP

Задачу аналізу потоку даних з метою виявлення конфіденційної інформації можна назвати нетривіальною. Оскільки пошук потрібних даних ускладнений безліччю чинників, які потребують обліку. Тому на сьогоднішній день розроблено кілька технологій для детектування спроб передачі конфіденційних даних. Кожна їх відрізняється від інших своїм принципом роботи.



Морфологічний аналіз



Морфологічний аналіз є одним із найпоширеніших контентних способів виявлення витоків конфіденційної інформації. Суть цього методу полягає в пошуку в тексті певних слів і/або словосполучень.

Головною перевагою методу, що розглядається, є його універсальність.

Основним недоліком морфологічного аналізу є низька ефективність визначення конфіденційної інформації.

Статистичний аналіз

Принцип роботи статистичних методів полягає у ймовірнісному аналізі тексту, що дозволяє припустити його конфіденційність чи відкритість. Для їхньої роботи зазвичай потрібне попереднє навчання алгоритму. У ході його обчислюється ймовірність знаходження тих чи інших слів, і навіть словосполучень у конфіденційних документах.

Перевагою статистичного аналізу є його універсальність. При цьому варто зазначити, що ця технологія працює у штатному режимі лише у рамках підтримки постійного навчання алгоритму.



Регулярні вирази (шаблони)



Суть методу така: адміністратор безпеки визначає рядковий шаблон конфіденційних даних: кількість символів та їх тип (літера чи цифра). Після цього система починає шукати в аналізованих текстах поєднання, що задовольняють йому, та застосовувати до знайдених файлів або повідомлень, вказаних у правилах дії.

Головною перевагою шаблонів є висока ефективність виявлення передачі конфіденційної інформації.

До недоліків шаблонів належить насамперед обмежена сфера їх застосування.

Цифрові відбитки

Під цифровим відбитком у разі розуміється цілий набір характерних елементів документа, яким можна з високої достовірністю визначити у майбутньому.

Сучасні DLP-рішення здатні детектувати як цілі файли, а й їх фрагменти. При цьому навіть можна розрахувати ступінь відповідності.

Важливою особливістю цифрових відбитків є те, що вони можуть бути використані не тільки для текстових, але і для табличних документів, а також для зображень.

Це відкриває широке поле для застосування даної технології.



Цифрові мітки



Принцип даного методу наступний: на вибрані документи накладаються спеціальні мітки, які видно лише клієнтським модулям DLP-рішення. Залежно від наявності системи дозволяє чи забороняє ті чи інші дії з файлами. Це дозволяє не тільки запобігти витоку конфіденційних документів, але й обмежити роботу з ними користувачів, що є безперечною перевагою даної технології.

До недоліків цієї технології належить, насамперед, обмеженість сфери її застосування та легкість її обходу.

Основні функції DLP-систем

- Контроль передачі інформації через Інтернет з використанням E-Mail, HTTP, HTTPS, FTP, Skype, ICQ та інших додатків та протоколів;
- Контроль збереження інформації на зовнішні носії - CD, DVD, flash, мобільні телефони тощо;
- Захист інформації від витоку шляхом контролю виведення даних на друк;
- Блокування спроб пересилання/збереження конфіденційних даних, інформування адміністраторів ІБ про інциденти, створення тіньових копій, використання карантинної папки;
- Пошук конфіденційної інформації на робочих станціях та файлових серверах за ключовими словами, мітками документів, атрибутами файлів та цифровими відбитками;
- Запобігання витоку інформації шляхом контролю життєвого циклу та руху конфіденційних відомостей.





Symantec DLP

Компанія Symantec є визнаним світовим лідером на ринку систем DLP. Протягом багатьох років рішення Symantec займає лідируючу позицію за версією аналітичної агенції Gartner у дослідженні Content-Aware Data Loss Prevention.

Найбільше впровадження Symantec DLP було зроблено у компанії, в якій працює понад 300 тисяч співробітників, на жаль, назва компанії не розголошується.

Рішення Symantec DLP забезпечує захист інформації на всіх ресурсах IT-інфраструктури підприємства.

Архітектура Symantec DLP 12.5

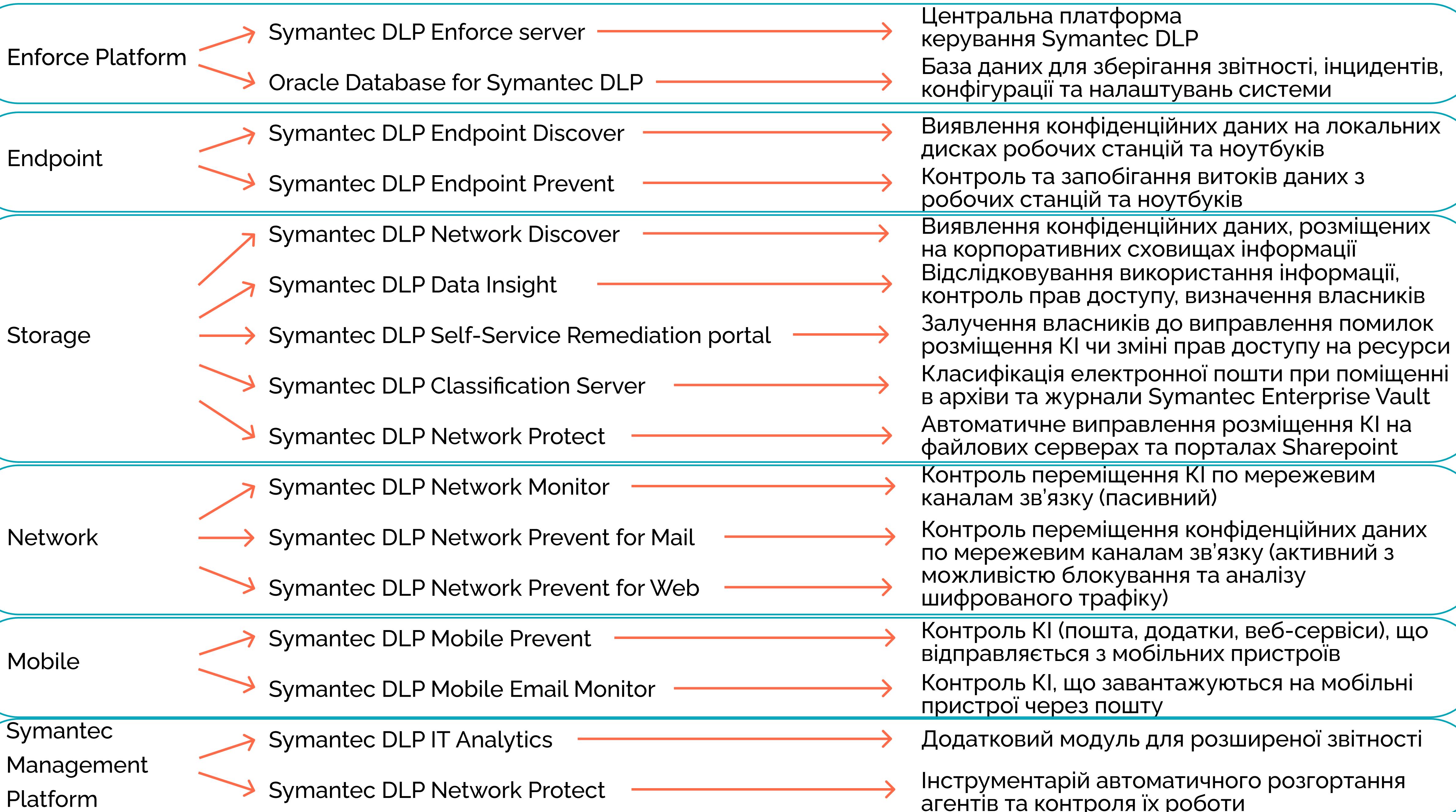
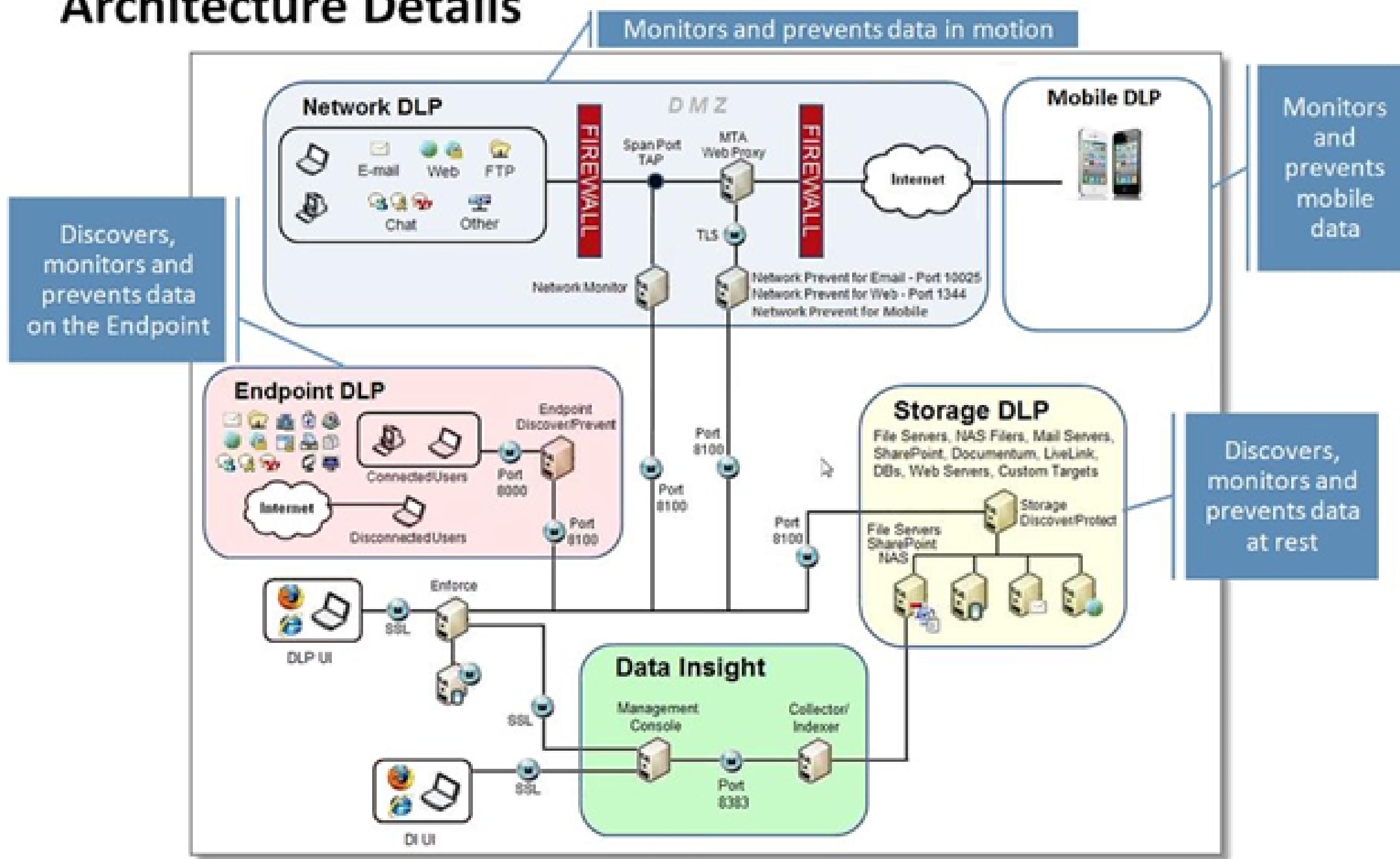


Схема роботи Symantec DLP

Architecture Details



На відміну від багатьох інших рішень, що постачаються як програмно-апаратні комплекси, Symantec DLP 12.5 постачається як набір програмного забезпечення, готового для встановлення. Модулі Symantec DLP 12.5 можна встановлювати практично в будь-якому складі будь-якого апаратного забезпечення, яке відповідає системним вимогам, у тому числі на віртуальні сервери.

Функціональні можливості Symantec DLC

Первінним завданням Symantec DLP є виявлення та блокування передачі (або приміщення на карантин) конфіденційної інформації (КІ), що міститься:

- У файлах різних форматів на всіх ресурсах корпоративної мережі, включаючи стаціонарні та мобільні комп'ютери, сервери, сховища даних та загальні мережеві файлові ресурси;
- У повідомленнях електронної пошти; Веб-трафіку;
- Під час запису на знімні носії інформації або компакт-диски CD/DVD;
- При надсиланні документів на друк; При копіюванні буфер обміну;
- При зверненні додатків до конфіденційних даних;

Друге завдання Symantec DLP – це оперативне реагування на події, пов'язані з обміном, передачею або виявленням КІ на неприпустимих ресурсах відповідно до заданих правил/політик:

- попередження, переміщення в карантин,
- блокування, зміна прав/списку доступу,
- переміщення з недовіреного середовища на «правильні» ресурси, шифрування та ін.

Переваги

- Велика кількість методів аналізу: контентний, цифрові відбитки, автоматичне навчання, аналіз контексту, гібридний аналіз.
- Багаторівневий захист інфраструктури: функціональний агент, високопродуктивні мережеві компоненти, захист багатьох сховищ.
- Можливість масштабування системи для забезпечення функціонування у складних високонавантажених інфраструктурах.
- Підтримка великої кількості мережевих протоколів для перехоплення та аналізу даних. - Широкі можливості інтеграції як з лінійкою продуктів Symantec, так і сторонніми рішеннями.
- Endpoint-агент із можливістю блокування даних по всіх заявлених каналах із здійсненням контентного аналізу.
- Модуль Data Insight (аналіз прав доступу на сховищах, аналіз доступу на сховищах, старіння даних і т.д.).
- Широкі можливості контролю HTTP/HTTPs трафіку, включаючи веб-пошту, соціальні мережі та інші довільні веб-сервіси (система записує повідомлення як HTTP(S)-трафік із певного сайту).
- Контроль мобільних пристройів під керуванням Android та iOS.



Недоліки

- Відсутність можливості контролю IM-протоколів таких як OSCAR, Mail.Ru Agent, Jabber, Microsoft Lync (компенсується контролем буфера обміну та контролем обігу додатків до конфіденційних файлів).
- Відсутність обробки на агентах індексів табличних даних.

