**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ» імені Ігоря Сікорського**

**ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ**

**Кафедра системного проектування**

**ЗВІТ**

**про виконання самостійної роботи**

**з дисципліни**

**«Безпека інформаційних систем»**

**на тему: 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.**

**Київ - 2021**

**ЗМІСТ**

1. ВИТІК КОНФІДЕНЦІЙНИХ ДАНИХ 5

1.1 Поняття витоку конфіденційних даних 5

1.2 Класифікація видів витоку інформації 5

1.2.1 Навмисні витоки інформації 5

1.2.1.1. Види навмисних витоків 6

1.2.2 Випадкові витоки інформації 7

1.2.2.1 Канали випадкових втрат інформації 7

1.3 Канали витоку 9

1.4 Фінансові втрати від витоків 9

1.4.1 Продаж даних хакерами 9

2. ПОПЕРЕЖДЕННЯ ВИТОКІВ ІНФОРМАЦІЇ 11

2.1 Поняття DLP 11

2.2 Класифікація DLP-систем 12

2.2.1 Шлюзові DLP 12

2.2.2 Хостові DLP 13

2.2.3 Універсалізація DLP 13

2.3 Методи аналізу потоків даних для DLP 14

2.3.1 Морфологічний аналіз 15

2.3.2 Статистичний аналіз 15

2.3.3 Регулярні вирази (шаблони) 16

2.3.4 Цифрові відбитки 17

2.3.5 Цифрові мітки 17

2.4 Основні функції DLP-систем 18

2.5 Рівні захисту конфіденційної інформації 19

2.5.1 Перший рівень 19

2.5.2 Другий рівень 20

2.5.3 Третій рівень 20

3. АНАЛІЗ НАЙРОЗПОВСЮДЖЕНІШОЇ МІЖНАРОДНОЇ DLP-СИСТЕМИ 21

3.1 Symantec DLP 21

3.1.1 Архітектура Symantec DLP 12.5 21

3.1.2 Опис модулів Symantec DLP 12.5 24

3.1.2.1 Enforce Platform 24

3.1.2.2. Network 26

3.1.2.3. Storage 27

3.1.2.4 Endpoint 29

3.1.2.5. Mobile 30

3.1.2.6. Symantec Management Platform 31

3.1.3 Принципова схема роботи Symantec DLP 12.5 31

3.1.4 Функціональні можливості DLP 12.5 32

3.1.5 Переваги 34

3.1.6 Недоліки 35

Висновки 36

Літературні джерела 37

ВСТУП

Двадцять перше століття стало століттям інформаційних технологій, оскільки вони отримали великий розвиток за останні 20 років. Начебто тільки нещодавно з’явилися мобільні телефони, а зараз кожен має смартфон, персональний комп’ютер або ноутбук та інші девайси.

Але один з найголовніших проривів інформаційних технологій – мережа Інтернет, яка нині доступна кожному для пошуку інформації, покупок, отримання різного характеру послуг та інше. І кожен сервіс, що ми використовуємо зберігає наші персональні дані при реєстрації, такі як ім’я, прізвище, по-батькові, номер телефону, паролі, дані банківських карток, місце проживання тощо.

Кожна компанія, що надає такі послуги та збирає конфіденційні дані користувачів, має дбати про безпеку цих даних, аби не було їх витоку, адже в руках зловмисників, отримана з витоків конфіденційна інформація, може стати засобом нанесення шкоди людині, її коштам тощо.

Саме тому методи забезпечення безпеки конфіденційних даних від витоків змінюються та покращуються зі збільшенням об’ємів конфіденційних даних, що зберігаються на носіях, серверах сервісів. Для сприяння цьому у європейських країнах та США запроваджені штрафи за виток конфіденційних даних користувачів, якщо, звісно, буде доведено, що витік даних був проведений саме з серверів цієї компанії.

Отже, у даній самостійній роботі будуть розглянуті методи забезпечення безпеки конфіденційних даних.

Мета роботи: дослідити витоки конфіденційних даних, засоби їх запобігання.

1. ВИТІК КОНФІДЕНЦІЙНИХ ДАНИХ
   1. Поняття витоку конфіденційних даних

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

Будь-які дані, що знаходяться у комп’ютері, мають свою цінність. Тому викрадення особистих даних власника комп’ютера здатне нанести йому шкоду. Маючи доступ до логінів та паролів, а також до банківських карт та рахунків, зловмисники крадуть гроші громадян, промислові секрети та таємниці підприємств.

Інформація витікає в результаті безконтрольного розповсюдження секретів за межі кабінету, будівлі, підприємства. Втрата цінних відомостей може статися у разі неправильного використання норм і правил політики безпеки. Недотримання правил захисту та зберігання даних тягне за собою їх витік та розповсюдження у загальнодоступних місцях, таких як мережа Інтернет.

* 1. Класифікація видів витоку інформації
     1. Навмисні витоки інформації

Умисні витоки інформації відбуваються навмисно: користувач, який мав доступ до цінних відомостей знав про можливі негативні наслідки своїх дій і розумів, що вони мають протиправний характер. Крім того, порушник отримував попередження про відповідальність, але все одно передавав дані або створював умови для їх витоку, бажаючи отримати матеріальну винагороду або іншу вигоду для себе. Внаслідок таких дій співробітника або підрядника виникли обставини, що сприяють втраті контролю за інформацією, порушення конфіденційності даних. При цьому наявність або відсутність негативних наслідків для компанії чи окремих осіб не має значення.

Зростання кількості навмисних витоків обумовлено виникненням нових можливостей, пов’язаних з обробкою, зберіганням, передачею інформації у цифровому вигляді. З кожним днем розширюється спектр послуг, що надаються на онлайн-майданчиках та із застосуванням даних електронного формату, збільшується обсяг інтелектуальної власності.

* + - 1. Види навмисних витоків
* **Інсайдери та надлишкові права**

До цього виду належать випадки, основною причиною яких стали дії працівників, які мають доступ до секретів легально, через свої службові обов’язки. Всі варіанти інсайду умовно можна розділити на дві групи: в одному випадку співробітник, не маючи доступу до інформації, отримує її незаконно, а в іншому він має офіційних доступ до закритих даних і навмисне виносить їх за межі компанії.

* **Крадіжка інформації (ззовні)**

Проникнення в комп'ютер за допомогою шкідливих програм та викрадення інформації з метою використання в корисливих інтересах. На хакерські атаки припадає 15% всього обсягу витоків інформації. Вторгнення у пристрій ззовні та непомітна установка шкідливих програм дозволяють хакерам повністю контролювати систему та отримувати доступ до закритих відомостей, аж до паролів для банківських рахунків та карт. І тому можуть застосовуватися різні програми на кшталт «троянських коней». Головний атрибут цього виду витоку – активні дії зовнішніх осіб з метою доступу до інформації.

* **Зламування програмного забезпечення**

Програми, що використовуються в робочому процесі або на особистому комп'ютері співробітника, часто мають незакриті вразливості, які можна експлуатувати і отримувати тим самим різні небезпечні можливості на кшталт виконання довільного коду або підвищення привілеїв.

* **Шкідливі програми (бедкори, трояни)**

Вони націлені на заподіяння шкоди власнику пристрою, дозволяють непомітно проникати в систему і потім перекручувати або повністю видаляти інформацію, замінювати її схожими даними.

* **Крадіжки носіїв**

Досить поширений варіант витоків, який трапляється внаслідок навмисного розкрадання пристроїв з інформацією - ноутбуків, смартфонів, планшетів та інших знімних носіїв даних у вигляді флешок, жорстких дисків.

* + 1. Випадкові витоки інформації

Випадкові витоки інформації — інциденти ненавмисної передачі інформації, що захищається, особі, яка не повинна мати до них доступу. Таке може відбуватися, наприклад, внаслідок неналежного (недбалого) поводження з носіями даних, які виявляються втраченими або вкраденими, через відправлення внутрішньої корпоративної інформації собі на зовнішню пошту та інших порушень політик безпеки щодо конфіденційних даних.

1.2.2.1 Канали випадкових втрат інформації

* **Мобільні телефони та смартфони**

Портативні пристрої зв'язку часто губляться і забуваються, а через компактність і високу ціну вони дуже привабливі для злодія. Втрата може бути обумовлена випаданням гаджета з погано застебнутого чохла, кишені або сумочки (особливо при фізичній активності). Іноді людина забуває забрати із собою телефон, який поклав на стіл або тумбочку у чужому приміщенні. Крадуть найчастіше (знову ж таки) пристрої в погано застебнутих чохлах і сумках або апарати, залишені без нагляду.

* **Планшети та ноутбуки**

Завдяки розмірам забути або втратити портативний комп'ютер складніше (хоча і таких випадків достатньо), проте висока вартість робить ноутбук ласим видобутком злодія. Часто крадіжки трапляються без власника, у тому числі - зі зломом (машини, кімнати, кабінету).

* **Електронна пошта та месенджери**

Втома, неуважне введення адреси з клавіатури можуть стати причиною надсилання даних помилковому адресату, і це стане причиною випадкового витоку.

* **Файлообмінники**

Співробітники багатьох компаній потребують доступу до файлів за межами організації, і для зручності деякі з них викладають дані у файлообмінні мережі та хмарні сховища. Якщо неправильно налаштувати права доступу до файлу, люди, які мають посилання, зможуть відкрити і завантажити його. У деяких файлообмінниках можна знайти адресу шляхом перебору.

* 1. Канали витоку

Рис.1. Графік відсоткового співвідношення частоти витоків відповідно до каналів витоку

* 1. Фінансові втрати від витоків

Фінансові втрати від витоку даних завдають істотних збитків бізнесу компанії, а іноді можуть його зруйнувати. Якщо злочинці що неспроможні отримати у компанії викуп, вони виставляють дані продаж.

* + 1. Продаж даних хакерами

Десятки підпільних сайтів конкурують у купівлі та перепродажі облікових даних для авторизації у найрізноманітніших сервісах, і оператори «ботів логів» можуть забезпечити собі безбідне життя, лише продаючи чужі паролі. Такий висновок зробив журналіст Браян Кребс, який спеціалізується на розкритті та висвітленні кіберзлочинів.

Згідно зі статистикою, хакер, який продає дані через Seller's Paradise, лише за кілька місяців може заробити понад $288 тис. За даними Кребса, успішний продавець на Seller's Paradise може за сім місяців продати близько 35 тис. пар облікових даних.

Продавець отримує гроші лише коли хтось купує запропонований ним товар. При цьому близько половини вартості товару Seller's Paradise забирає собі як комісійні. Середня вартість облікових даних користувачів банківських сайтів та сайтів електронної комерції на Carder's Paradise – $15. Така вартість логінів та паролів користувачів airbnb.com, comcast.com, creditkarma.com, logmein.com та uber.com. Облікові дані абонентів AT&T Wireless у парі з доступом до вмісту їхніх поштових скриньок коштують удвічі дорожче – $30.

Найдорожчими на Carder's Paradise є облікові дані клієнтів магазину frys.com ($190). Облікові дані американських військових із кредитної спілки NavyFederal.com коштують $60, а облікові дані для авторизації в агрегаторах Thomson Reuters – $50.

1. ПОПЕРЕЖДЕННЯ ВИТОКІВ ІНФОРМАЦІЇ

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 (ІБ) є захист конфіденційних даних від несанкціонованих дій користувачів.

Це пов'язано з тим, що більшість традиційних засобів захисту таких як антивіруси, міжмережні екрани (Firewall) і системи запобігання вторгнень (IPS) не здатні забезпечити ефективний захист від внутрішніх порушників (інсайдерів), метою яких може бути передача інформації за межі компанії для подальшого використання - Продажі, передачі третім особам, опублікування у відкритому доступі тощо. Вирішити проблему випадкових та умисних витоків конфіденційних даних, покликані системи запобігання витоку даних (DLP — Data Leak Prevention).

* 1. Поняття DLP

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

Подібного роду системи створюють захищений «цифровий периметр» навколо організації, аналізуючи всю вихідну, а часом і вхідну 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.

DLP-системи здійснюють аналіз потоків даних, що перетинають периметр інформаційної системи, що захищається. При виявленні в цьому потоці конфіденційної інформації спрацьовує активний компонент системи і передача повідомлення (пакета, потоку, сесії) блокується. Виявлення конфіденційної інформації в потоках даних здійснюється шляхом аналізу змісту та виявлення спеціальних ознак: грифу документа, спеціально введених міток, значень хеш-функції з певної множини тощо.

Сучасні DLP-системи мають величезну кількість параметрів і характеристик, які обов'язково необхідно враховувати під час виборів рішення організації захисту конфіденційної інформації від витоків.

* 1. 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.

* + 1. 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.

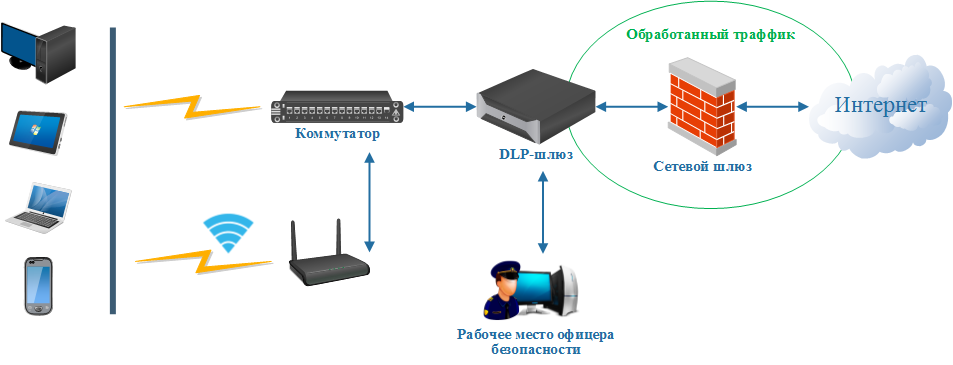


Рис. 2. Функціональна схема шлюзового DLP-рішення

* + 1. Хостові DLP

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

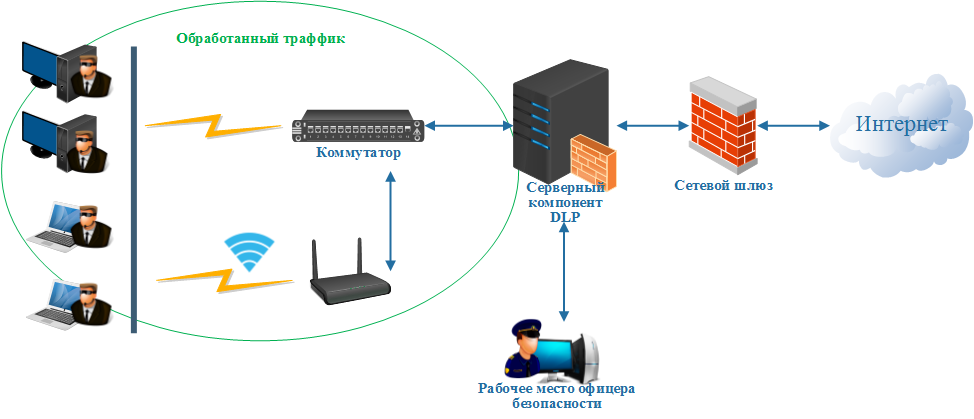


Рис. 3. Функціональна схема хостового DLP-рішення

* + 1. Універсалізація DLP

Останнім часом спостерігається стійка тенденція універсалізації DLP-систем. На ринку вже не залишилося або майже не залишилося рішень, які можна було б назвати суто хостовими або шлюзовими. Навіть ті розробники, які тривалий час розвивали виключно якийсь один напрямок, додають до своїх рішень модулі другого типу.

Причин переходу до універсалізації DLP-рішень дві:

1. Різні сфери застосування у систем різних типів. Як було сказано вище, хостові DLP-рішення дозволяють контролювати всілякі локальні, а мережеві - інтернет-канали витоку конфіденційної інформації. Ґрунтуючись на тому, що в переважній більшості випадків організація потребує повного захисту, їй потрібно і те, й інше.
2. Другою причиною універсалізації є деякі технологічні особливості та обмеження, які не дозволяють суто шлюзовим DLP-системам повністю контролювати всі необхідні інтернет-канали.

Оскільки повністю заборонити використання потенційно небезпечних каналів передачі даних неможливо, то можна поставити їх під контроль. Суть контролю полягає в моніторингу всієї інформації, що передається, виявленні серед неї конфіденційної та виконання тих чи інших операцій, заданих політикою безпеки організації. Очевидно, що основним, найважливішим і трудомістким завданням є аналіз даних. Саме його якості залежить ефективність роботи всієї DLP-системи.

* 1. 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.

Умовно всі способи виявлення витоків можна поділити на дві групи. До першої відносяться ті технології, які засновані на аналізі безпосередньо самих текстів повідомлень, що передаються, або документів (морфологічний і статистичний аналізи, шаблони). За аналогією з антивірусним захистом їх можна назвати проактивними. Другу групу складають реактивні способи (цифрові відбитки та мітки). Вони визначають витоку за властивостями документів чи наявності у яких спеціальних міток.

* + 1. 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. З одного боку, морфологічний аналіз може використовуватися для контролю будь-яких каналів зв'язку, починаючи з файлів, що копіюються на знімні накопичувачі, і закінчуючи повідомленнями в ICQ, Skype, соціальних мережах, а з іншого – за його допомогою можуть аналізувати будь-які тексти та відстежувати будь-яку інформацію. При цьому конфіденційні документи не потребують будь-якої попередньої обробки. А захист починає діяти відразу після включення правил обробки та поширюється на всі задані канали зв'язку.

Основним недоліком морфологічного аналізу є низька ефективність визначення конфіденційної інформації. Причому залежить вона як від використовуваних у системі захисту алгоритмів, так і від якості семантичного ядра, що застосовується для опису даних, що захищаються.

* + 1. 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. Так, наприклад, якщо в процесі навчання системі було запропоновано недостатню кількість договорів, вона не зможе визначати факт їх передачі. Тобто якість роботи статистичного аналізу залежить від коректності його настроювання. При цьому необхідно враховувати імовірнісний характер цієї технології.

* + 1. 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. Щодо інцидентів випадкових витоків вона прагне 100%. Випадки з навмисними пересилками складніші. Знаючи про можливості DLP-системи, зловмисник може протидіяти їй, зокрема, розділяючи символи різними символами. Тому методи захисту конфіденційної інформації, що використовуються, повинні триматися в секреті.

До недоліків шаблонів належить насамперед обмежена сфера їх застосування. Вони можуть бути використані лише для стандартизованої інформації, наприклад, для захисту персональних даних. Ще одним мінусом аналізованого методу є відносно висока частота помилкових спрацьовувань. Наприклад, номер паспорта складається із шести цифр. Але, якщо задати такий шаблон, то він спрацьовуватиме щоразу, коли зустрінеться 6 цифр поспіль. А це може бути номер договору, який надсилається клієнту, сума тощо.

* + 1. 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. Такі рішення дозволяють створювати диференційовані правила, де описані різні дії для різних відсотків збігу.

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.

* + 1. 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. Захистити за її допомогою можна лише текстові документи, причому вже існуючі. На новостворені документи це не поширюється. Частково цей недолік нівелюється засобами автоматичного створення міток, наприклад, на основі набору ключових слів. Однак цей аспект зводить технологію цифрових міток до технології морфологічного аналізу, тобто, по суті, дублювання технологій.

Іншим недоліком технології цифрових міток є легкість її обходу. Достатньо вручну набрати текст документа в листі (не скопіювати через буфер обміну, а саме набрати), і цей спосіб буде безсилим. Тому він добрий лише у поєднанні з іншими методами захисту.

* 1. Основні функції DLP-систем

Основні функції DLP-систем візуалізовані на малюнку нижче (рис. 4)

* 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.



Рис. 4. Основні функції DLP-систем

* 1. Рівні захисту конфіденційної інформації
     1. Перший рівень

Data-in-Motion – дані, що передаються мережевими каналами:

* Web (HTTP/HTTPS протоколи);
* Служби миттєвого обміну повідомленнями (ICQ, QIP, Skype, MSN тощо);
* Корпоративна та особиста пошта (POP, SMTP, IMAP тощо);
* Бездротові системи (WiFi, Bluetooth, 3G тощо);
* Ftp – з'єднання.
  + 1. Другий рівень

Data-at-Rest – дані, що статично зберігаються на:

* Сервери;
* Робочих станціях;
* Ноутбуки;
* Системах зберігання даних (СЗД).
  + 1. Третій рівень

Data-in-Use – дані, які використовуються на робочих станціях.

1. АНАЛІЗ НАЙРОЗПОВСЮДЖЕНІШОЇ МІЖНАРОДНОЇ DLP-СИСТЕМИ
   1. 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. Рішення Symantec Data Loss Prevention (DLP) орієнтоване на впровадження в компаніях практично будь-яких масштабів, починаючи від невеликих (з кількістю користувачів від 100 і більше) і до великих компаній (з кількістю користувачів, що перевищує позначку 10 і навіть 100 тисяч). Найбільше впровадження Symantec DLP було зроблено у компанії, в якій працює понад 300 тисяч співробітників, на жаль, назва компанії не розголошується. Найбільшим відкритим використанням було використання в консалтинговій компанії Deloitte, в якій працює близько 180 тисяч співробітників. Рішення Symantec DLP забезпечує захист інформації на всіх ресурсах IT-інфраструктури підприємства:

* Відстеження та блокування переміщення інформації як усередині організації, так і за її межі;
* Виявлення конфіденційної інформації у відкритому доступі на файлових сховищах, веб-серверах, базах даних, системах поштового обміну та документообігу;
* захист конфіденційної інформації на робочих станціях та ноутбуках, у тому числі тих, що знаходяться поза корпоративною мережею;
* Контроль мобільних додатків, хмарних та веб сервісів, а також електронної пошти, що отримується та надсилається на смартфонах і планшетних комп'ютерах.
  + 1. Архітектура Symantec DLP 12.5

Symantec DLP 12.5 - це розподілена модульна комплексна система, склад якої наведено в таблиці 1.

|  |  |  |
| --- | --- | --- |
| Група модулів | Функціональний склад | Призначення |
| Enforce Platform | Symantec DLP  Enforce server | Центральна платформа керування 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 та ноутбуків |
| Symantec DLP  Endpoint Prevent | Контроль та запобігання витоків даних з робочих станцій та ноутбуків |
| Storage | Symantec DLP  Network Discover | Виявлення конфіденційних даних, розміщених на корпоративних сховищах інформації |
| Symantec DLP  Data Insight | Відслідковування використання інформації, що розміщена на сховищах, контроль прав доступу, визначення власників даних |
| Symantec DLP Self-Service  Remediation portal | Залучення власників до виправлення помилок розміщення КІ чи зміні прав доступу на ресурси |
| Symantec DLP  Classification Server | Класифікація електронної пошти при поміщенні в архіви та журнали Symantec Enterprise Vault |
| Symantec DLP  Network Protect | Автоматичне виправлення розміщення КІ на файлових серверах та порталах Sharepoint (карантин) |
| Network | Symantec DLP  Network Monitor | Контроль переміщення КІ по мережевим каналам зв’язку (пасивний) |
| Symantec DLP  Network Prevent for Mail | Контроль переміщення конфіденційних даних по мережевим каналам зв’язку (активний з можливістю блокування та аналізу шифрованого трафіку) |
| Symantec DLP  Network Prevent for Web |
| Mobile | Symantec DLP  Mobile Prevent | Контроль КІ (пошта, додатки, веб-сервіси), що відправляється з мобільних пристроїв |
| Symantec DLP  Mobile Email Monitor | Контроль КІ, що завантажуються на мобільні пристрої через пошту |
| Symantec Management Platform | Symantec DLP IT  Analytics | Додатковий модуль для розширеної звітності |
| Symantec DLP  Integration  Component | Інструментарій автоматичного розгортання агентів та контроля їх роботи |

Табл. 1. Архітектура Symantec DLP 12.5

* + 1. Опис модулів Symantec DLP 12.5

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

3.1.2.1 Enforce Platform

Це основна інтегруюча та керуюча платформа Symantec DLP. Управління набором модулів DLP здійснюється через Web-інтерфейс і дозволяє виконувати такі операції:

* Зняття цифрових відбитків із неструктурованих даних. Зняття може виконуватися з таких джерел: загальна мережева папка, доступна за протоколом SMB, CIFS; локальна папка на сервері Enforce; у вигляді архіву, що завантажується через web-інтерфейс, що містить потрібні документи;
* Зняття цифрових відбитків із структурованих даних. Зняття проводиться через файл-розвантаження формату CSV, що завантажується через web-інтерфейс;
* Створення профілю захисту даних за допомогою технології Vector Machine Learning. Створення відбувається під час обробки досить великого масиву документів «позитивного» та «негативного» характеру. Документи завантажуються через веб-інтерфейс;
* Створення та редагування ідентифікаторів, що представляють поєднання регулярних виразів та перевірок;
* Створення політик на основі 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;
* Створення правил реагування на спрацьовування політики; створення цілей мережевого сканування;
* Додавання, перепризначення, керування та видалення серверів детектування; створення груп політик;
* Перегляд та керування повідомленнями про системні події;
* Перегляд статистики трафіку;
* Збирання логів модулів системи;
* Перегляд стану, видалення, зміна конфігурації та повідомлення про стан агентів, що встановлюються на робочих станціях;
* Управління функціоналом контролю за додатками;
* Створення, зміна та видалення ідентифікаторів знімних пристроїв;
* Управління основними налаштуваннями системи, налаштуваннями мережевих протоколів, груп користувачів на основі груп Active Directory, зберіганням облікових записів та управління інтеграцією з модулями Data Insight та Management Console, створення та зміна атрибутів інцидентів, управління вивантаження даних інцидентів в архів та управління користувачами та ролями;
* Перегляд інцидентів, створення звітів.

СУБД Oracle є централізованим сховищем інцидентів, журналів подій, налаштувань системи, політики безпеки та тіньових копій перехоплених даних

3.1.2.2. Network

Для відстеження та контролю даних, що передаються мережевими каналами зв'язку, призначена група модулів Network, до складу якої входять модулі Symantec DLP Network Monitor, Network Prevent for Web та Network Prevent for Mail.

**Network Monitor** – модуль, призначений для аналізу дзеркального мережевого трафіку, який передається на аналіз за допомогою додаткового мережного обладнання: комутаторів або TAP пристроїв.

Модуль **Network Monitor** дозволяє на основі сигнатур аналізувати протоколи: SMTP, HTTP, NNTP, AOL, MSN, Yahoo. Інші мережеві протоколи аналізуються, виходячи з використовуваних ними мережевих портах.

**Network Prevent for E-Mail** це модуль, який призначений для аналізу та блокування електронної пошти, що передається за протоколами SMTP або ESMTP. З технічного погляду є (E)SMTP Proxy. Надає кілька варіантів інтеграції в поштову інфраструктуру – як розрив, так і паралельна обробка.

Останній модуль цієї групи – **Network prevent for Web**. Він дозволяє здійснювати аналіз та блокування трафіку, що передається на нього Proxy-серверами. Можливий аналіз протоколів HTTP, HTTPS (при використанні proxy-серверів, що мають функціонал розшифровки SSL-трафіку), FTP over HTTP. Інтеграція з Proxy-серверами можлива за протоколом ICAP або за допомогою додаткового програмного забезпечення, що встановлюється на сервери Microsoft ISA 2004/2006 та TMG.

3.1.2.3. Storage

Тепер розглянемо функціональність групи модулів Storage, до складу якої входять Symantec DLP Network Discover, Network Protect, Data Insight, Self-Service Remediation Portal, Classification Server. Ця група модулів призначена для контролю даних, що знаходяться на мережевих ресурсах компанії, файлових сховищах та системах електронного документообігу.

Першим розглянемо модуль **Network Discover**. Його призначення – виявлення даних на мережевих джерелах зберігання. Виявлення можливе на файлових серверах, файлових системах серверів, базах даних SQL, поштових серверах та інших. Підтримується сканування таких джерел даних:

* Мережеві файлові системи (CIFS, NFS, DFS);
* Локальні файлові системи на серверах під керуванням Microsoft Windows, Linux, Solaris, AIX;
* Веб-сервер;
* Microsoft Exchange;
* Microsoft Sharepoint 2007/2010/2013;
* БД Lotus Notes;
* БД SQL;
* Livelink;
* Documentum;
* Додаткові програми, дані з яких можуть бути вилучені та передані Network Discover.

Сканування джерел здійснюється за розкладом із правами заданого користувача.

**Network Protect**. Цей модуль є розширенням модуля **Network Discover** і дозволяє переміщувати або копіювати дані, які порушують політики безпеки. У разі переміщення файлів передбачена можливість залишати на їх місці файл-заглушку, що має ту саму назву, що і файл, що переноситься, але із заданим текстом всередині.

**Data Insight** - модуль, призначений для збору інформації про дії (створення файлу, запис, читання тощо), що здійснюються з файлами на рівні файлової системи. Дані можуть збиратися з файлових серверів на платформі Windows, серверів Microsoft Sharepoint, а також NAS серверів компанія NetApp і EMC. Крім цього, можна сформувати звітність щодо доступу до файлів, а також зайняте місце на серверах. Також модуль Data Insight дозволяє контролювати за допомогою політик безпеки доступ до файлу, доступ до файлу користувачів, які не перебувають у білих списках.

Можливості Data Insight дозволяють визначити нестандартну поведінку користувачів щодо доступу до даних. Data Insight складається з наступних компонентів, які можуть встановлюватися як на одному, так і на різних серверах, залежно від інфраструктури замовника:

* Management – ​​настроювання, керування, зберігання даних та надання звітності;
* Indexer – індексування та обробка даних, що передаються з collector;
* Collector – збір даних із серверів-джерел.

**Data Insight Self-Service Remediation portal** – це модуль, за допомогою якого адміністратори файлових сховищ та співробітники відділів безпеки можуть залучити власників бізнес-даних для виправлення помилок розміщення критичної інформації та зміни прав доступу на важливі дані за допомогою веб-порталу.

Останній модуль, який входить до групи **Storage**, це Classification Server. Його призначення - класифікація листів, які розміщуються в архівах та журналах пошти Symantec Enterprise Vault.

3.1.2.4 Endpoint

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

Завдання модуля **Endpoint Discover** включають пошук та аналіз файлів, що зберігаються на робочих станціях. Пошук здійснюється встановленим на робочій станції Endpoint-агентом.

Аналіз файлів відбувається локально, крім аналізу по цифровим відбиткам, навіщо дані передаються на Endpoint-сервер. Дані про інцидент передаються з агента на сервери Endpoint і далі модуль Enforce по шифрованому каналу. Сертифікат шифрування може бути використаний як вбудований, так і створений додатково.

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

Endpoint-агент аналізує дані, що передаються такими способами:

* Запис на носій USB;
* запис на локальний диск;
* Запис на SD та CF карти пам'яті;
* Копіювання у буфер обміну;
* Запис на CD/DVD носії;
* Запис на спільні папки мережі;
* Надсилання через запити POST на веб-сторінки. Аналізу підлягає як HTTP протокол (для всіх браузерів), і HTTPS (для браузерів Microsoft Internet Explorer і Mozilla Firefox);
* Надсилання даних електронною поштою через поштові клієнти Microsoft Outlook і Lotus Notes;
* Надсилання даних через інтернет-пейджери, такі як MSN, Yahoo, та ін
* Звернення програм до файлів та передача даних через мережу (Application Control).

У разі порушення політик на робочій станції, за допомогою агента може видаватися діалогове вікно для користувача з вимогою пояснити необхідність дії, що здійснюється.

3.1.2.5. Mobile

Для забезпечення захисту даних, що передаються за допомогою мобільних пристроїв, призначені модулі **Symantec DLP Mobile Prevent** та **Mobile Email Monitor.**

**Symantec DLP Mobile Prevent** призначений для контролю інформації, що відправляється в мережу інтернет через мобільні пристрої iPad та iPhone по мережевих каналах HTTP/S, FTP. Він дозволяє контролювати мобільну пошту та мобільні програми такі як: FaceBook, DropBox, Twitter, Gmail, GoodReader.

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

3.1.2.6. Symantec Management Platform

Додатковий контроль та керування Symantec DLP 12.5 здійснюється за допомогою Symantec Management Platform. До її складу входять Symantec DLP Integration Component та Symantec DLP IT Analytics. Розглянемо функції цих модулів.

Symantec DLP Integration Component – ​​це компонент, який призначений для автоматизації розгортання, обліку, оновлення та видалення агентів Symantec DLP. Він може бути розширений до повноцінного патч-менеджмент рішення та рішення щодо інвентаризації тощо.

Symantec DLP IT Analytics дає змогу отримати розширену звітність. Також він призначений для створення кастомізованої звітності з багатьох продуктів Symantec, включаючи Symantec DLP 12.5. У разі виявлення неправомірних дій користувача Symantec DLP 12.5 дозволяє:

* заблокувати передачу даних;
* Зареєструвати порушення з блокуванням передачі чи без;
* Створити тіньову копію даних;
* Повідомити користувача про вчинення неправомірної дії;
* Запитати пояснення у користувача щодо порушень;
* Повідомити працівника служби безпеки про порушення;
* Запустити будь-яку програму або команду для реакції на інцидент.
  + 1. Принципова схема роботи Symantec DLP 12.5

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.

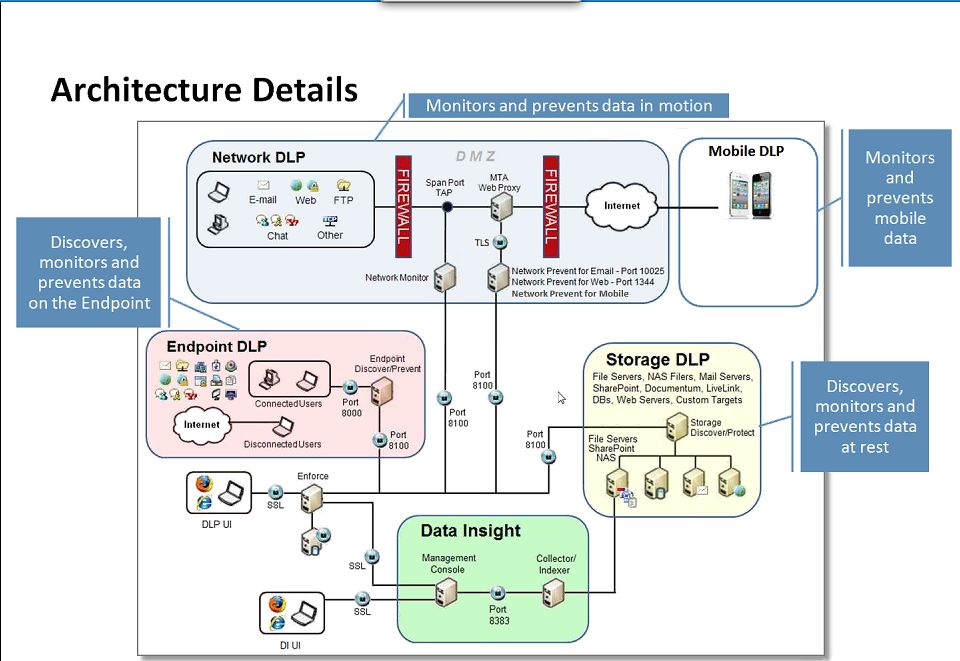


Рис. 5. Принципова схема роботи Symantec DLP 12.5

* + 1. Функціональні можливості DLP 12.5

Первинним 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;
* Під час запису на локальні диски;
* При копіюванні з/в спільні папки мережі;
* При зверненні 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).

Друге завдання Symantec DLP – це оперативне реагування на події, пов'язані з обміном, передачею або виявленням КВ 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.

Для створення політик можна використовувати готові шаблони, які можна використовувати без змін (наприклад, для контролю персональних даних) або змінювати відповідно до поточних вимог.

У разі спрацьовування політики – потенційного або реального інциденту ІБ (витоку КІ), Symantec DLP включає механізм сповіщення та контролю розслідування інцидентів.

Symantec DLP містить засоби підготовки аналітичної звітності та візуального представлення інформації щодо ризиків ІБ, динаміки, тенденцій та кількісних характеристик.

Таким чином, основною метою Symantec DLP є запобігання витоку конфіденційної інформації за рахунок використання різних технологій та засобів технічного контролю, навчання співробітників правилам обробки конфіденційної інформації та розслідування кожного інциденту.

* + 1. 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 пристроїв під керуванням Android та iOS.
  + 1. 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.

Висновки

Використання DLP-систем давно стало вже не просто модою, а необхідністю, адже витік конфіденційних даних може призвести до величезних збитків для компанії, а головне зробити не одномоментний, а тривалий вплив на бізнес компанії. При цьому шкода може мати як прямий, а й непрямий характер. Тому що, крім основного збитку, особливо у разі розголошення відомостей про інцидент, компанія «втрачає обличчя». Збитки від втрати репутації оцінити в грошах дуже складно, адже кінцевою метою створення системи забезпечення безпеки інформаційних технологій є запобігання або мінімізація шкоди (прямої чи непрямої, матеріальної, моральної чи іншої), що завдається суб'єктам інформаційних відносин за допомогою небажаного впливу на інформацію, її носії та процеси обробки.

У даній самостійній роботі було розглянуто витоки конфіденційних даних, їх класифікація, канали витоку. Також було розглянуто DLP-системи, їх класифікацію та проаналізовано найрозповсюдженішу DLP-систему Symantec DLP.

Літературні джерела

1. <https://www.anti-malware.ru/threats/intentional-information-leaks>
2. <https://www.anti-malware.ru/threats/leaks>
3. <https://www.anti-malware.ru/threats/accidental-leaks>
4. <https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85#.D0.A4.D0.B8.D0.BD.D0.B0.D0.BD.D1.81.D0.BE.D0.B2.D1.8B.D0.B5_.D0.BF.D0.BE.D1.82.D0.B5.D1.80.D0.B8_.D0.BE.D1.82_.D1.83.D1.82.D0.B5.D1.87.D0.B5.D0.BA>
5. <https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A0%D0%B0%D1%81%D1%86%D0%B5%D0%BD%D0%BA%D0%B8_%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D0%BA%D0%B8%D1%85_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85_%D0%BD%D0%B0_%D1%80%D1%8B%D0%BD%D0%BA%D0%B5_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2#2017:_.D0.9E.D1.81.D0.BD.D0.BE.D0.B2.D0.B0_.D0.B1.D0.B5.D0.B7.D0.B1.D0.B5.D0.B4.D0.BD.D0.BE.D0.B9_.D0.B6.D0.B8.D0.B7.D0.BD.D0.B8_.D1.85.D0.B0.D0.BA.D0.B5.D1.80.D0.BE.D0.B2_-_.D0.BF.D1.80.D0.BE.D0.B4.D0.B0.D0.B6.D0.B0_.D0.BF.D0.B0.D1.80.D0.BE.D0.BB.D0.B5.D0.B9>
6. <http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/dlp-systems>
7. <https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B4%D0%BE%D1%82%D0%B2%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%B8%D0%B5_%D1%83%D1%82%D0%B5%D1%87%D0%B5%D0%BA_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8>
8. <https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/>
9. <https://www.anti-malware.ru/reviews/Symantec_Data_Loss_Prevention_12_5#part4>
10. <https://www.anti-malware.ru/products/symantec-dlp>