МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

_____ С.В. Казмірчук

«_____»_____ 2021 р.

На правах рукопису

УДК 004.056:004.738.5(079.2)

ДИПЛОМНА РОБОТА
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система запобігання витоку інформації на підприємстві

Виконавець: М.С. Кондратенко

Керівник: к.т.н., доцент М.Б. Гумен

Нормоконтролер: к.т.н., доцент М.Б. Гумен

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних та комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ С.В. Казмірчук
«___» _____ 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи
здобувача вищої освіти Кондратенка Матвія Сергійовича

1. Тема: *Система запобігання витоку інформації на підприємстві*
затверджена наказом ректора від 26.05.2021
2. Термін виконання з 10.05.2021 по 20.06.2021
3. Вихідні дані: розглянути існуючі загрози витоків інформації на підприємствах; Проаналізувати методи запобігання загрозам витоків інформації.
4. Зміст пояснювальної записки: аналіз рекомендацій щодо створення і модернізації системи протидії витоків інформації, проектування і налаштування системи протидіії витоків інформації підприємства.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	10.05.2021	*Виконано*
2.	Аналіз літературних джерел	11.05.2021-14.05.2021	*Виконано*
3.	Обґрунтування вибору рішення	15.05.2021-17.05.2021	*Виконано*
4.	Збір інформації	18.05.2021-22.05.2021	*Виконано*
5.	Дослідження сучасних технологій протидії витокам інформації	23.05.2021-24.05.2021	*Виконано*
6.	Дослідження механізмів реалізації витоків інформації	25.05.2021-28.05.2021	*Виконано*
7.	Розробка процедур протидії витокам інформації	29.05.2021-01.06.2021	*Виконано*
8.	Проектування архітектури модулю захисту та проведення експериментальних досліджень	01.06.2021-02.06.2021	*Виконано*
9.	Перевірка на антиплагіат	03.06.2021	*Виконано*
10.	Оформлення і друк пояснювальної записки	04.06.2021	*Виконано*
11.	Оформлення презентації	07.06.2021	*Виконано*
12.	Отримання рецензій від рецензента	09.06.2021	*Виконано*

Здобувач вищої освіти _____ М.С. Кондратенко
(підпис, дата)

Керівник дипломної роботи _____ М.Б. Гумен
(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальним обсягом робота складає 56 сторінок, має 17 рисунків, 7 таблиць. Список використаних джерел містить 21 найменування і займає 2 сторінки.

Метою дипломної роботи є забезпечення підприємства системою запобігання витоків інформації.

В роботі розглянуті існуючі загрози витоків, заходи щодо аналізу систем запобігання витоку інформації на підприємстві. Проведено аналіз оцінки ризиків існуючої системи безпеки підприємства, спроектовано локальну мережу підприємства і розгорнуто комплексну систему запобігання витоків інформації.

Ключові слова: система захисту інформації, оцінка ризику, корпоративна мережа, витік інформації.

ЗМІСТ

ВСТУП

Актуальність. За останні роки цінність даних тільки збільшується. Кого би ви не запитали, усі підтвердять важливість власних даних. Фактично, все більше число організацій усвідомлюють, що дані стають все більш актуальними з кожним днем. Так, різні компанії успішно зберігали та обробляли дані впродовж багатьох років, якщо не десятиліть, без спеціального управління ними та належного захисту. Але для того, щоб зрозуміти, що управління даними є необхідністю в наші часи, не потрібно бути експертом в області даних. Є багато можливостей, які пов'язані з даними, і є багато шляхів вилучити дорогоцінну інформацію.

Ефективність будь-якого бізнесу в більшості випадків залежить від збереження конфіденційності, цілісності і доступності інформації і витоки інформації являють собою чи не найбільшу загрозу в області інформаційної безпеки. Зумовлено це тим, що більшість технічних та програмних заходів не здатні захистити інформацію від внутрішніх порушників.

За статистикою, в одних лише сполучених штатах за 2020 рік було зафіксовано більше тисячі випадків витоків інформації. Серед жертв були компанії “Facebook”, “Ebay”, “Adobe”, “Instagram”.

За даними сайту “Ponemon”, середні втрати однією компанією від одного витоку в 2018-2019 роках становила 3,92 мільйонів доларів.

Але що заважає організаціям зробити важливий крок протидії витокам інформації? Щоб зрозуміти, як організації працюють з даними сьогодні, варто поглянути на історичний розвиток: дані в електронному вигляді не з'явилися раптово. Актуальність даних поступово збільшувалася протягом останніх декількох десятиліть. Як наслідок, часто не було єдиного моменту або події, яка б спонукала організацію вирішити, «нам необхідно управляти і координувати даними». Часто IT-відділ ставав інкубатором, де люди реалізовували технічні можливості. Однак у багатьох інших випадках нетехнічні люди у відділах

управлінням інформацією відчували велику потребу у захисті даних і вирішували щось з цим робити. Згодом цей розвиток привів до ряду типових підходів.

Останнім часом активно розроблялися технології запобігання витоків інформації, які отримали термін DLP (DataLeakPrevention), які і розглядаються в роботі. Системи захисту від витоків інформації призначені для відстежування і блокування передачі даних за межі корпоративної мережі, але окрім цього дані системи можуть відстежувати дії співробітників даного підприємства в мережі.

Нині немає чіткого розуміння цього терміну. Дійсно, DLP-системою можна назвати навіть антивірус, оскільки він дозволяє уникнути установки троянів, які посилають інформацію з локального пристрою своїм творцям або замовникам, і програму для блокування USB-портів, оскільки вона бореться з витоками через USB-накопи-чувачі. Проте антивірус і система блокування портів не захищають організацію від витоків – вони лише закривають один з каналів або усувають одну з причин. Теоретично за допомогою подіб лаптевих» рішень можна запобігти витокам, проте для крупних організацій такий підхід категорично неприйнятний. Тому під DLP-системою зазвичай розуміють комплексне рішення корпоративного масштабу, яке бореться з витоками для різних каналів і причин. Це визначення є неп підходить іпотетична си ема, яка фізично блокує всі порти і перекриває доступ до Internet. Сучасним організаціям потрібні Internet і доступ до мобільних накопичувачів. Перекривати ці канали не можна – а значить, доступ до них слід контролювати. Іншими словами, DLP-система зобов'язана аналізувати трафік, який проходить по каналах і «голосно кричати» адміністратору, якщо цей трафік виявився секретним. Остання те є функціонал DLP-систем від більшості других рішень з інформаційної безпеки. У рамках окремого узятого каналу DLP-система працює як «чорний ящик», куди на вхід подається інформація, що йде по каналу, а на виході формується вердикт, чи є вхідна інформація секре ип не залежить в д специфіки каналу, яка, втім, може бути використана в алгоритмі винесення вердикту. Таким чином, основна цінність DLP-системи полягає в алгоритмі, на основі якого працює «чорний ящик». Архітектура і навіть список підтримуваних каналів є вторинними харак-

теристиками дан оте, з погляду кінцевого замовника, дані чинники також дуже важливі, оскільки без них додаток практично марний. На даний момент у галузі не існує стандартного алгоритму аналізу трафіку, більш того – не існує навіть стандартної технології. Кожна, представлена на ринку компанія, сповідає власний спосіб фільтрації даних, говорити про два концептуально різних підходи, що мають як переваги, так і недоліки.

Метою дипломної роботи є проектування, розгортання і модернізація системи запобігання витоків інформації підприємства.

Досягнення мети досліджень потребує розв'язання таких задач:

-Аналіз існуючих каналів витоків інформації і факторів цих витоків.

-Аналіз існуючих систем контролю і управління доступом до конфіденційної інформації на підприємстві.

-Проведення порівняльного аналізу DLP-систем.

-Розроблення системи запобігання витоку інформації на підприємстві.

Об'єкт дослідження: порівняльний аналіз комплексних систем запобігання витоків інформації і реалізація такої на підприємстві.

Предмет дослідження: система запобігання витоку інформації на підприємстві.

Практична цінність полягає у розробці системи запобігання витоку інформації, що забезпечує ефективність інформаційної безпеки на підприємстві.

РОЗДІЛ 1. ІНФОРМАЦІЙНА БЕЗПЕКА І ВИТОКИ ІНФОРМАЦІЇ

1.1 Основні фактори і канали витоку інформації

В наші дні майже всі підприємства використовують багаторівневі системи обробки інформації, кожен рівень якої може бути середовищем витоку важливої для фірми інформації.

Фактори витоків можна поділити на такі групи:

-Персонал

Жодна фірма зі штабом співробітників не може бути захищеною від цього фактору витоку, адже кожен робітник потенційно являється загрозою для безпеки інформації. Під час роботи з даними людина зберігає робочі файли на різні носії, пересилають її собі на альтернативні пошти, спілкуються про робочі моменти з друзями, які можуть поширити цю інформацію далі.

Дії персоналу поділяють на навмисні і ненавмисні. В випадках навмисного витоку інформації зловмисник вчиняє злодіяння з метою вигоди, як продаж даних, шантаж тощо. Ненавмисні ж дії являються наслідком незнання співробітником нормативних документів фірми стосовно інформаційної безпеки.

Спричинити витік через співробітників відбувається частіше, якщо умови роботи не є на досить високому рівні, різного виду скорочення та реорганізації на підприємстві тощо.

-Переміщення

Іноді виникають умови, при яких всьому штабу треба змінити місцезнаходження, як наприклад переїзд головного офісу до нової будівлі. В такому випадку є підвищений ризик витоку інформації через недобросовісних робочих, які будуть допомагати з переїздом і через банальну необачність співробітників.

-Кооперація

Співпрацювання є важливою складовою розвитку будь-якої фірми, але цей процес є доволі ризиковим. Часто під час виконання проектів сумісно з іншою фірмою неможливо повною мірою захистити дані, адже доступ до них є в більшої кількості людей.

-Використання складних систем обробки інформації

Великі фірми часто використовують складні багаторівневі системи захисту і передачі даних, але, як парадоксально б це не звучало, це збільшує ризики витоків інформації при некомпетентному підході персоналу. Наприклад, один адміністратор бази даних змінить деякі правила розмежування доступу, а інший не врахувати цього і випадково дати права доступу до серверів з базами даних співробітнику, який не повинен їх мати.

-Помилки в роботі програмного забезпечення

На жаль, навіть найновіша і найдосконаліша програма може давати збої, програмні заходи захисту інформації в тому ж числі. На жаль, від програмних збоїв ніхто не захищений і вони виникають доволі часто. Під час неполадок важлива інформація може бути перехоплена третіми особами і тому важливо завжди тримати програмну складову систем захисту в працездатному стані.

Також, через програмні помилки інформація може бути видалена з машини, тому варто завжди мати резерві копії даних на інших захищених носіях.

-Помилки в роботі технічних заходів

Іноді техніка стає несправною з різних причин, що можу зумовити витік інформації. Наприклад, через сервісний центр, в який ви віднесете зламаний технічний засіб.

-Проблеми в роботі серверів

Найбільші фірми часто використовують хмарні обчислення, бо це полегшує доступ до інформації співробітникам, а також пришвидшує обробку будь-якої інформації. Але, на жаль, останнім часом збільшилася кількість хакерських атак на сервери. Також, проблеми в роботі серверів можуть виникати через погодні умови та інші непередбачувані події.

Загальна класифікація каналів витоку:

Відповідно до загальноприйнятої класифікації існуючі канали витоку інформації можуть бути непрямими або прямими. Коли мова йде про непрямі канали, це означає, що зловмисник має прямий доступ до технічного середовища конкретної системи захисту інформації.

Приклади непрямих витоків:

Втрата фізичного носія або його навмисна крадіжка.

Пошук конфіденційних даних шляхом пошуку в смітті, пошук викинутих документів тощо.

Зчитування помилкового електромагнітного випромінювання і перешкод.

Спроба крадіжки інформації з використанням оптичних засобів: фотографування об’єктів інформаційної системи, прослуховування приміщень.

При взаємодії з прямими каналами зловмисник отримує доступ до обладнання та інформації, яка використовується в інформаційній системі.

Яскравим прикладом прямого каналу витоку є робота інсайдерів. Самі співробітники компанії в більшості випадків стають засобом передачі інформації зловмиснику. Це може статися навмисно або випадково. У першому випадку співробітник навмисно влаштовується на роботу в організацію, щоб і далі вишукувати секрети, у другому – ненавмисне розкриття інформації відбувається в неформальній обстановці.

Пряме копіювання інформації також належить до каналу прямих витоків.

Для захисту даних в компаніях найчастіше задіюється одна основна автоматизована система захисту інформації, тому важливо враховувати всі канали технічних витоків, які являють собою крадіжку даних безпосередньо з використанням фізичних властивостей системи.

На рисунку 1.1 зображена схема основних технічних каналів витоку інформації. Канали можуть об’єднуватися для створення одного мультиканалу, який включає властивості одразу декількох основних каналів.

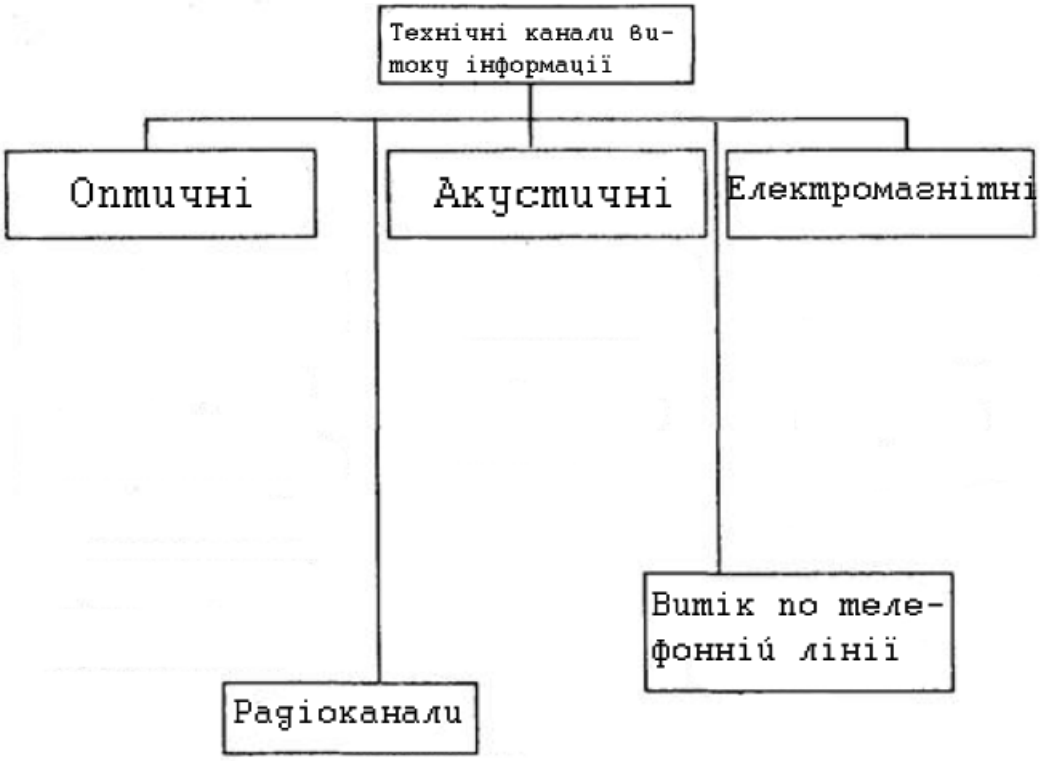

Рис. 1.1 Технічні канали витоку інформації

Типи каналів технічного витоку включають:

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

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.

Найбільш поширений і небезпечний з точки зору зберігання конфіденційної інформації – це акустичний канал витоку. Відомі тисячі випадків, коли конкурент намагався встановити пристрої для прослуховування телефонних розмов і звукозаписні пристрої на іншому об'єкті. За допомогою спрямованих мікрофонів ви можете отримати доступ до аудіоінформації в приміщенні на відстані до 300 метрів від будівлі. Іншими словами, зловмисникові потрібно всього лише сісти в машину в кількох кварталах від точки переговорів, щоб легко отримати доступ до конфіденційної інформації.

Практично універсальним каналом витоку інформації являэться акустоелектричний, оскільки його можна використовувати на будь-якому рівні електричної мережі; зловмиснику не потрібно використовувати додаткові мікрофони чи радіоплати для читання даних. Інформація збирається без прямого підключення до мережі; використовується випромінювання у вигляді електромагнітних хвиль. У деяких випадках жучки-підсилювачі можуть бути встановлені в будівлі компанії. Під час їх роботи конкурент легко зчитує магнітні хвилі на відстані до 300 метрів від джерела даних. Захист від впливу на акустоелектричний канал забезпечує так звана транспортна розв'язка, яка здатна створювати перешкоди, так що зловмисники не можуть повністю прочитати інформацію.

Зловмисник може прослуховувати телефонні розмови на підприємстві. Для реалізації цього каналу витоку використовуються пристрої високочастотного накладення. В результаті телефонна лінія генерує модульований сигнал, який перехоплюється зловмисником.

Оптичний канал доступний, якщо робочий процес компанії можна візуально контролювати, робити фотографії або відео. Завдяки отриманню «картини» етапів роботи зловмиснику не складе труднощів розкрити конфіденційну інформацію, яка охороняється підприємством.

Витоки через акусторадіоелектронний канал реалізуються шляхом використання радіозакладок або радіомікрофонів – надмаленьких пристроїв, які ви-

користовують фізичні особливості радіохвиль, які зловмисник конвертує в зручний для себе вигляд інформації, який, в основному, являється акустичним.

1.2 Загальні заходи по забезпеченню безпеки

Компанії, які працюють з конфіденційною інформацією будь-якого типу, потребують власної комплексної системи безпеки, яка є перешкодою для зловмисника на всіх рівнях обробки даних.

Систему захисту слід створювати з урахуванням усіх виявлених каналів витоку. Також варто створити службу безпеки, яка буде відповідати за підтримку автоматизованої системи захисту.

Факт крадіжки інформації виявляється двома основними способами. У першому випадку працівник стає свідком інциденту і може розповісти про те, хто і як викрав інформацію. У цьому випадку ймовірність зловити злодія завжди вища, перш ніж він передасть важливі дані конкуренту. Важливо не допустити, щоб організація отримала збитки, тому вони завжди намагаються ідентифікувати інсайдера «по гарячих слідах».

У другому сценарії факт крадіжки стає відомим після того, як зловмисник вже використав вкрадену інформацію у власних цілях. Згідно з цим сценарієм, події розвиваються в переважній більшості випадків. Факт крадіжки, про яку власник інформації не знав, стався через використання зловмисником отвору безпеки або через відсутність системи безпеки як такої.

Витік даних – це, в першу чергу, результат порушення методу захисту конфіденційних даних та головна причина фінансових та «нематеріальних» збитків для компанії. Коли виявлено витік, основним завданням служби безпеки є якнайшвидше розпочати дії з ідентифікації зловмисника.

Розслідування проводиться в рамках закону. Першим кроком є використання організаційних заходів та наближений доступ до даних, оскільки існує ризик повторного викрадення. Далі слід розпочати провадження. На тех-

нічному рівні DLP-системи можуть запобігати витокам, автоматично виявляючи спробу несанкціонованої передачі інформації поза захищеним середовищем.

На першому етапі розслідування служба безпеки визначає тип і метод витоку: випадковий або запланований. Як правило, факт втрати через необережність або ненавмисний витік даних легко виявити на етапах аналізу звіту DLP-системи, розмови з персоналом або після перегляду відео.

Як результат витоку інформації, компанія може зазнати серйозних збитків. Це може бути пов’язане з різними причинами: крадіжка технології виготовлення продукції, крадіжка важливих документів, розголошення секретної інформації тощо. Тому на етапі розробки системи безпеки слід враховувати всі можливі канали витоку, за допомогою яких зловмисник може отримати доступ до захищеної інформації.

Якщо витік вже стався, компанія може лише спробувати встановити особу, яка викрала дані або мимоволі стала співучасником крадіжки. Крім того, якщо дані надходять від конкурентів, вам слід вирішити, як знецінити інформацію, щоб запобігти можливим втратам у майбутньому.

1.3 Поняття DLP-систем та їх значення в безпеці

Запобігання витоків інформації (DLP) – це практика виявлення та запобігання порушень даних, поширенню або небажаному знищенню конфіденційних даних. Організації використовують DLP для захисту та обробки своїх даних та дотримання норм взаємодії співробітників з інформацією.

Термін DLP означає захист організацій від втрати даних та запобігання їх витоку. Витік даних відноситься до події, в якій важливі дані виносяться за межі підприємства. Запобігання втраті даних зосереджується на запобіганні незаконної передачі даних за межі корпоративної мережі.

Організації зазвичай використовують DLP для:

-Захисту персональної інформації (ідентифікації особи) та дотримання вимог відповідно нормативним документам.

-Захисту інтелектуальної власності, що має важливе значення для організації.

-Досягнення видимості даних у великих організаціях.

-Захисту даних на віддалених хмарних системах.

Підприємства можуть використовувати стандартні засоби безпеки для захисту від втрати та витоку даних. Наприклад, система виявлення вторгнень (IDS) може попереджати про спроби зловмисників отримати доступ до конфіденційних даних. Антивірусне програмне забезпечення може перешкодити зловмисникам порушити чутливі системи. Брандмауер може заблокувати доступ будь-якої несанкціонованої сторони до систем, що зберігають конфіденційні дані, але все популярнішим рішенням стають DLP-системи.

Великі організації можуть використовувати вузькоспеціалізовані інструменти або рішення DLP для захисту даних. Наприклад, можна використовувати інструменти Центру безпеки операцій (SOC), щоб підсилити DLP. Наприклад, ви можете використовувати систему захисту інформації та подій (SIEM) для виявлення та кореляції подій, які можуть становити витік даних.

Найбільш популярні рішення для запобігання втрати даних:

Захист даних у русі – технологія, встановлена на межі мережі, може аналізувати трафік для виявлення конфіденційних даних, що надсилаються з порушенням політики безпеки.

Захист кінцевих точок – система заходів на основі кінцевих точок (вузлів) можуть контролювати передачу інформації між користувачами, групами користувачів та зовнішніми сторонами. Деякі системи, що базуються на кінцевих точках, можуть блокувати спроби зв’язку в режимі реального часу та надавати зворотний зв’язок із користувачем.

Захист даних у стані спокою – політика контролю доступу, шифрування та збереження даних може захистити заархівовані дані організації.

Захист даних, що використовуються – деякі системи DLP можуть відстежувати та позначати несанкціоновані дії, які користувачі можуть навмисно чи ненавмисно виконувати під час їх взаємодії з даними.

Ідентифікація даних – надзвичайно важливо визначити, чи потрібно захищати дані чи ні. Дані можна визначити як конфіденційні або вручну, застосовуючи правила, або автоматично за допомогою таких методів, як машинне навчання.

Виявлення витоку даних – рішення DLP та інші системи безпеки, такі як IDS, IPS та SIEM, визначають передачі даних, які є аномальними або підозрілими. Ці рішення також попереджають співробітників служби безпеки про можливий витік даних.

Рішення DLP та рішення для захисту файлів.

Рішення щодо захисту файлів, такі як брандмауер файлів, є важливою частиною стратегії DLP. Такі рішення захищають дані, що перебувають у стані спокою, і дані, що використовуються, та виявляють витоки даних на основі файлів.

Брандмауер файлів допомагає запобігти витоку даних шляхом:

-Моніторингу доступу до всіх конфіденційних файлів та запис детальних даних про використання, таких як користувач, відділ, файл, до якого здійснюється доступ, тип файлу та час відгуку на операцію.

-Попередження та автоматичне блокування дій із файлами, що порушують політику безпеки.

-Виявлення ненормальної або підозрілої поведінки користувачів за допомогою машинного навчання для виявлення інсайдерських загроз.

-Пом’якшення атак Ransomware шляхом виявлення та блокування типових шаблонів доступу до файлів.

-Аудит і звітування про всі файлові операції для відповідності та розслідування.

1.4 Висновок до першого розділу

В сьогоденні проблема витоків інформації є чи не найголовнішою для будь-яких підприємств. З кожним роком вартість інформації зростає, а шляхів нелегально добути її стає все більше. У зв'язку з цим, актуальність використання систем запобігання витоків інформації нестримно зростає.

Роль технології DLP полягає у виявленні, моніторингу та захисті даних у фізичних сховищах, а також у русі по корпоративній мережі. Системи DLP використовуються для забезпечення застосування політик безпеки інформації підприємства з метою запобігання несанкціонованому доступу або використанню конфіденційних даних. Витік даних може статися через навмисне неправильне використання, необережність, атаки через канали витоку інформації.

В першій частині роботи було розглянуто такі питання:

-Розподілення факторів витоку інформації на групи і детальний їх опис.

-Загальна класифікація каналів витоку інформації.

-Рекомендаційні заходи по забезпеченню захисту від витоків інформації.

-Принцип дії DLP-систем.

-Роль DLP-систем у захисті інформації підприємств.

РОЗДІЛ 2. КОНЦЕПЦІЯ ВИКОРИСТАННЯ DLP-СИСТЕМ

2.1 Види DLP-систем і принципи їх функціонування

Технологічні засоби, що застосовуються для вирішення випадків витоку даних, можна розділити на категорії: стандартні заходи безпеки, розширені заходи безпеки, контроль доступу та шифрування та призначені системи DLP.

Стандартні заходи безпеки, такі як брандмауери, системи виявлення вторгнень (IDS) та антивірусне програмне забезпечення, є загальнодоступними продуктами, що захищають комп'ютери від сторонніх та інсайдерських атак. Наприклад, використання брандмауера перешкоджає доступу сторонніх людей до внутрішньої мережі, а система виявлення вторгнень виявляє спроби вторгнення сторонніми особами. Внутрішнім атакам можна запобігти за допомогою антивірусного сканування, яке виявляє троянських коней, які надсилають конфіденційну інформацію, та за допомогою тонких клієнтів, які працюють в архітектурі клієнт-сервер без персональних або конфіденційних даних, що зберігаються на клієнтському пристрої.

Розширені заходи безпеки використовують алгоритми машинного навчання та часових міркувань для виявлення нетипового доступу до даних (наприклад, до баз даних або систем пошуку інформації) або нетипового обміну електронною поштою, для виявлення уповноваженого персоналу зі зловмисними намірами та перевірка на основі активності (наприклад, розпізнавання динаміки натискання клавіші) та моніторинг активності користувачів для виявлення ненормального доступу до даних.

Призначені системи виявляють і запобігають несанкціонованим спробам копіювання або надсилання конфіденційних даних, навмисно чи ненавмисно, переважно персоналом, який уповноважений отримати доступ до конфіденційної інформації. Для того, щоб класифікувати певну інформацію як чутливу, вони використовують такі механізми, як точне узгодження даних, відбитки струк-

турованих даних, статистичні методи, узгодження правил та регулярних виразів, опубліковані лексикони, концептуальні визначення, ключові слова та контекстна інформація, така як джерело даних.

Розділяють два рівні, на яких працюють системи DLP.

Мережевий рівень контролю при цьому повинен забезпечувати максимально можливе охоплення мережевих протоколів і сервісів. Мова йде не тільки про «традиційні» канали (поштові протоколи, FTP, HTTP-трафік), але і про більш нові системи мережного обміну (Instant Messengers, хмарні сховища). На жаль, на мережевому рівні неможливо контролювати зашифрований зв'язок, але дана проблема в DLP-системах вирішена на рівні хоста.

Контроль на хостовому рівні дозволяє вирішувати більше завдань з точки зору моніторингу та аналізу. Фактично служба інформаційної безпеки підприємства отримує інструмент повного контролю за діями користувача на робочій станції. DLP з хостовою архітектурою дозволяє відстежувати, що копіюється на знімний носій, які документи відправляються на друк, що набирається на клавіатурі, записувати аудіоматеріали, робити знімки екрану. На рівні кінцевої робочої станції перехоплюється зашифрований зв'язок (наприклад, Skype), а для перевірки відкриті дані, які обробляються в режимі реального часу і які тривалий час зберігаються на ПК користувача.

Крім вирішення звичайних завдань, DLP -системи з контролем на хостовому рівні забезпечують додаткові заходи щодо забезпечення інформаційної безпеки: контроль установки і зміни програмного забезпечення, блокування портів введення-виведення тощо.

Мінуси хостової реалізації в тому, що системи з великим набором функцій складніше адмініструвати, вони більш вимогливі до ресурсів самої робочої станції. Керуючий сервер регулярно звертається до модулю- «агенту» на кінцевому пристрої, щоб перевірити доступність і актуальність налаштувань. Крім того, деяка частина потужності машини користувача буде завжди використовуватися програмним модулем DLP. Тому ще на етапі підбору рішення для запобігання витоку важливо звернути увагу на апаратні вимоги.

На даний момент, більшість систем DLP працюють одразу на двох рівнях.

Залежно від архітектури, заходи захисту інформації від витоків поділяють на технічні та адміністративні.

До технічних заходів відносяться: захист даних у русі, у стані спокою та у використанні.

Метою DLP є захист інформації протягом усього циклу її використання. DLP-системи розрізняють за способом виявлення витоку даних:

Захист даних у русі (Data At Rest) включає сканування сховища, щоб визначити, де знаходиться конфіденційний вміст.

Це називається виявленням вмісту. Можна, наприклад, використовувати продукт DLP для сканування ваших серверів та ідентифікації документів з номерами кредитних карток. Якщо сервер не авторизований для такого роду даних, файл можна зашифрувати або видалити, або надсилати попередження власнику файлу.

Дані у русі (Data In Motion) - це сканування трафіку в корпоративній мережі (пасивно або вбудовано через проксі-сервер) для ідентифікації вмісту, що надсилається через певні канали зв'язку. Наприклад, сюди входить розпізнавання електронних листів, миттєвих повідомлень та веб-трафіку на фрагменти конфіденційного вихідного коду. Інструменти захисту даних у русі часто можуть блокувати витоки інформації на основі трафіку, в залежності від основних політик захисту конфіденційної інформації.

Дані, що використовуються, зазвичай захищаються рішеннями кінцевих точок, які контролюють дані, коли користувач взаємодіє з ними. Наприклад, вони можуть ідентифікувати, коли ви намагаєтесь перенести конфіденційний документ на USB-накопичувач і заблокувати його. Дані, що використовуються, також можуть виявляти такі речі, як копіювання та вставлення, або використання конфіденційних даних у незатвердженому додатку. Наприклад, спроба зашифрувати дані і переслати їх через месенджер для обходу різного роду датчиків.

До адміністративних відносяться: центральне адміністрування, управління політикою безпеки та відслідковування робочого процесу.

До центрального адміністрування входить: ієрархічне управління, інтеграція каталогів та адміністрування на основі ролей.

Створення та керування політиками

Створення та управління політиками є важливою функцією в основі DLP. Інтерфейс вироблення політики повинен бути доступним як технічним, так і нетехнічним користувачам, хоча технічні знання майже завжди потрібні для створення впорядкованих політик.

Для створення політик система повинна дозволити вам вказати тип даних, що захищаються, якщо це можливо, джерело даних, пункти призначення, які канали контролюють і захищають, які дії потрібно вжити у разі порушень, що потрібно зробити користувачам, щоб застосувати політику , і які можливості доступу до політики та порушень мають менеджери та адміністратори. Оскільки не всі політики створені однаковими, порогові показники чутливості та серйозності слід призначати кожному на основі кількості порушень. Політики повинні використовуватися як шаблони для нових політик, і якщо система містить категорії політик, пов’язані зі створюваною категорією. Також шаблони та створені політики повинні редагуватися та оновлюватися, щоб протидіяти новим загрозам витоків.

Більшість користувачів віддають перевагу користувальницьким інтерфейсам, які використовують чіткі графічні макети для політик, максимально прості у використанні сітку відстежуваних каналів та порушення цього каналу. Чим складніша політика, тим простіше помилитися при призначенні каналу тощо.

В основному кожна політика вимагає певного рівня модифікації та хороший інструмент дозволяє вам створити політику, яка показує, як вона буде реагувати у виробництві, не заповнюючи рядки обробника подій та не вживаючи жодних заходів щодо примусового застосування. Деякі пристрої можуть перевірити контурну політику щодо раніше зафіксованого трафіку.

Політика містить дуже конфіденційну інформацію і повинна захищатися хешем, шифруванням або іншими засобами в системі. Деякі підрозділи можуть мати високочутливі політики, які потрібно захищати від адміністраторів без спеціального дозволу для перегляду певної політики.

Важливою складовою відслідковування робочого процесу є поточне відслідковування інцидентів та система управління справами.

Процес відслідковування інцидентів є найбільш широко використовуваною частиною системи DLP. Тут повідомляється про порушення, здійснюється управління інцидентами та проводяться розслідування.

Головна частина системи - це черга обробки інцидентів, яка є підсумком усіх інцидентів, або інцидентів в визначеній області корпоративної мережі. Статус інциденту повинен бути чітко вказаний певним кольором на основі порушеної політики та серйозності порушення. Кожен інцидент повинен відображатися в одному рядку та мати функціїї сортування або фільтрування у будь-якому полі, як зображено на рисунку 2.1.

Канал, порушена політика, користувач, статус інциденту (відкритий, закритий, призначений, непризначений, розслідування) та обробник також повинні бути вказані та легко змінені для миттєвого розподілу.

Кожен користувач повинен мати можливість налаштовувати що завгодно, щоб краще відповідати його стилю роботи.

Інциденти з численними порушеннями політики чи кількома порушеннями однієї політики повинні з’являтися лише один раз у черзі інцидентів. Електронний лист із 10 вкладеннями не повинен відображатись як 10 різних випадків, за винятком випадків, коли кожне вкладення порушує іншу політику.

Коли відкривається один інцидент, у ньому повинні бути перелічені всі деталі події, включаючи (якщо не обмежено інше) висвітлення, які дані у документі або трафік порушували яку політику. Цінною особливістю є короткий опис інших нещодавніх порушень, здійснених цим користувачем, та інших порушень із цими даними (що може свідчити про більшу подію). Інструмент по-

винен дозволяти обробнику коментувати, призначати додаткові обробники, повідомляти управління та завантажувати будь-яку допоміжну документацію.

ID	Time	Policy	Channel	Severity	User	Action	Status
1138	1625	PII	Email	1.2 M	rmogull	Blocked	Open
1139	1632	HIPAA	IM	2	jsmith	Notified	Assigned
1140	1702	PII	HTTP	1	192.168.0.213	None	Closed
1141	1712	R&D/Product X	USB	4	bgates	Notified	Assigned
1142	1730	Financials	Storage	4	192.168.1.94	Encrypt	Escalated
1143	12/1/08	Source Code	Cut/Paste	12	sjobs	Confirm	Open

Рис 2.1 Приклад черги інцидентів

Більш досконалі інструменти включають управління справами для детального відстеження інциденту та будь-яку допоміжну документацію, включаючи позначки часу та хеші даних. Це цінно у випадках, коли вживаються юридичні дії, і слід керувати доказами в системі управління справою , щоб підвищити її придатність для прийому до суду.

2.2 Порівняння і аналіз сучасних DLP-систем

Сучасні DLP-системи крім основних вміщують в себе також функції виявлення інформації (eDiscovery), шифрування (Encryption), а також контролю дій персоналу і підвищення його продуктивності (Employee Management Software і Productivity Control). Цей факт, поряд з початковою складністю DLP-систем і сильною закритістю документації, значно ускладнюють процес їх усвідомленого вибору для замовника. Найчастіше у відкритому доступі можна знайти лише маркетингову інформацію, зв'язок якої з реальним станом справ, часом, невелика. Частина виробників і зовсім не зацікавлені в тому, щоб досту-

пно і зрозуміло розповідати про технічні тонкощі роботи своїх продуктів, очевидно, побоюючись зайвої обізнаності клієнтів, партнерів і прямих конкурентів.

Найважливішим моментом будь-якого порівняння є набір критеріїв, за яким воно проводиться. Їх кількість залежить від ряду факторів: ступеня глибини дослідження, а також ступенем відмінностей між системами, яку ми хочемо підкреслити. У той же час важливо не тільки кількість обраних в рамках порівняння критеріїв, але і розгорнуті відповіді по кожному з них, так як порівнювані системи можуть серйозно відрізнятися навіть на цьому рівні. До деяких із критеріїв були додані пояснення.

На основі результатів проведеного аналізу, я вибрав 6 найпопулярніших в світі комплексних DLP-систем: InfoWatch Traffic Monitor Enterprise, Falcongaze SecureTower, SearchInform, GTB DLP Suite, Symantec Data Loss Prevention, McAfee.

Розпочнемо з огляду режимів роботи даних систем.

Режим моніторингу – звичайний режим роботи DLP-системи.

Режим копіювання – режим перехвату подій, при якому режим, при якому система лише записує дані порушень, не попереджуючи витоку.

Режим блокування – режим, при якому система блокую передачу даних до тих пір, доки адміністратор служби безпеки не вирішить, що робити у випадку цієї події.

Як видно з таблиці 2.1, всі вибрані системи DLP можуть працювати в однакових режимах.

Огляд запобіганню різним режимам перехоплення інформації показано на таблиці 2.2.

Усі вибрані DLP-системи мають однаковий функціонал в плані відстежування трафіку мережі як через хоста на робочій станції, так і через сторонні сервіси (VPN,Аналізатори мережевих пакетів).

Функція перехвату в режимі розриву каналів відсутня у DLP-системах Falcongaze та SearchInform.

Таблиця 2.1

Огляд режимів роботи DLP-систем

Режим роботи	Fal-congaze	GTB	In-foWatch	SearchInfor m	Syman-tec	McAfe e
В режимі моні-торингу	ТАК	ТАК	ТАК	ТАК	ТАК	ТАК
В режимі бло-кування	ТАК	ТАК	ТАК	ТАК	ТАК	ТАК
Режим копію-вання	ТАК	ТАК	ТАК	ТАК	ТАК	ТАК

Таблиця 2.2

Порівняння фукції перехоплення трафіку DLP-систем

Режим перехвату	Falcongaze	GTB	InfoWatch	SearchInform	Symantec	McAfee
Перехват трафіку через хо-ста	ТАК	ТАК	ТАК	ТАК	ТАК	ТАК
Перехват трафіку через сторонні сервіси	ТАК	ТАК	ТАК	ТАК	ТАК	ТАК
Перехват в розриві	НІ	ТАК	ТАК	НІ	ТАК	ТАК

Однією з найважливіших функцій DLP-системи є моливість інтеграції з іншим програмним забазпеченням, в основному з базами даних, системами об-

міну повідомлення, програмаи захисту мережі, програмами серверного управління тощо. Після проведення аналізу можливостей інтеграції вибраних систем стало зрозуміло, що найбільше можливостей у американських продуктів.

Вірогідно, це викликано тим, що в американських комплексних системах використовуться більш надійний і “розумний” штучний інтелект, який допомогає створювати підприємству правила та регулювання навіть найновішого програмного забезпечення для файлообміну, серверних процесів, месенджерів на нових та старих каталогах та плагінах.

У таблиці 2.3 я надав список найважливіших функцій інтеграціїї DLP-систем з різним програмним забезпеченням.

Таблиця 2.3

Можливості інтеграції з іншим програмним забезпеченням

Можливі інтеграції	Falcongaze	GTB	InfoWatch	SearchInform	Symantec	McAfee
Інтеграція з почтовими серверами	Microsoft Exchange, IBM Lotus Domino	Microsoft Exchange, IBM Lotus Domino	Microsoft Exchange, IBM Lotus Domino	Microsoft Exchange	Microsoft Exchange, IBM Lotus Domino	Microsoft Exchange, IBM Lotus Domino
Інтеграція з будь-якими Proxy-серверами по ICAP	ТАК	ТАК	ТАК	ТАК	ТАК	ТАК
Інтеграція з системами документообігу	НІ	SECLORE IRM	ORACLE IRM, Microsoft Sharepoint	НІ	Microsoft RMS, ORACLE IRM, Microsoft Sharepoint, Documentum, Liquid Machines Document Control	Microsoft RMS, ORACLE IRM, Microsoft Sharepoint, Documentum, Liquid Machines Document Control

На всіх перелічених DLP-системах є можливість інсталяціїї та управління через групові політики, можливість підключення декількох баз даних, можли-

вість розгортання на віртуальній машині і працювати на декількох доменах, якщо в них довірча взаємодія.

Наступним кроком було детально розглянуто контроль основних каналів витоку інформації з корпоративної мережі. За основу бралися протоколи, на яких працюють найпопулярніші програми обміну інформацією. Роздивимось контроль каналів витоків інформації даних систем.

В таблиці 2.4 було розглянуто чи контролюють вибрані DLP-системи програми обміну повідомленнями, які працюють на базі протоколів SMTP (Gmail, Outlook, Thuderbird), POP3 (протокол завантаження нових повідомлень у клієнт пошти),IMAP(синхронізація поштового клієнту на різних машинах), MAPI(з'єднання різних поштових клієнтів), NNTP(інтеграція серверів. Які передають новини у клієнти пошти),S/MIME(відповідає за шифрування повідомлень).

Таблиця 2.4

Контроль протоколів електронної пошти

Архітектура протоколу	Falcongaze	GTB	InfoWatch	SearchInform	Symantec	McAfee
SMTP	SMTPs	SMTPs, SMTP	SMTP, eSMTP	SMTP,eSMPT	SMTP,eSMPT	SMTP,eSMPT
POP3	POP3,POP3s	POP3,POP3s	POP3,POP3s	POP3,POP3s	POP3,POP3s	POP3,POP3s
IMAP	IMAP4,IMAP4s	IMAP4,IMAP4s	IMAP4,IMAP4s	IMAP4,IMAP4s	IMAP4,IMAP4s	IMAP4,IMAP4s
MAPI	ТАК	ТАК	ТАК	ТАК	ТАК	ТАК
NNTP	НІ	ТАК	НІ	ТАК	ТАК	ТАК
S/MIME	ТАК	ТАК	ТАК	ТАК	НІ	ТАК

Далі порівнюється мжливість контролю протоколів програм миттєвого обміну повідомленнями, що являється одним з основних каналів витоку інформації з підприємств.

Таблиця 2.5

Контроль протоколів програм миттєвого обміну повідомленнями (Instant Messengers).

Архітектура протоколу	Falcongaze	GTB	InfoWatch	SearchInform	Symantec	McAfee
OSCAR	ТАК, текст і файли	ТАК, текст і файли	ТАК, текст і файли	ТАК, текст і файли	НІ	ТАК, текст і файли
MMP	ТАК, текст і файли	НІ	ТАК, текст і файли	ТАК, текст і файли	НІ	НІ
MSN	ТАК	ТАК	НІ	ТАК	ТАК	ТАК

Важливою функцією є контроль трафіку WEB програм, адже по статистиці 60% робочого часу працівники фірм проводять в мережі у власних цілях. Контроль допоможе вести облік виходу співробітниками в мережу, попередити проникнення вірусів у корпоративну мережу, оперативно реагувати на аномальну діяльність в корпоративній мережі і автоматизувати частину роботи адміністратора.

Таблиця 2.6

Контроль WEB мережі

Канал	Fal-congaze	GTB	In-foWatch	SearchInf orm	Syman-tec	McAfee
HTTP+	HTTP, HTTPs	HTTP, HTTPs	HTTP, HTTPs	HTTP, HTTPs	HTTP, HTTPs	HTTP, HTTPs
Web-mail	Будь-яка пошта	Будь-яка пошта	Будь-яка пошта	Будь-яка пошта	Будь-яка пошта	Будь-яка по-шта
Соціальні ме-режі	Будь-які соцмере-жі	Будь-які соцме-режі	Будь-які соцме-режі	Будь-які соцмере-жі	Будь-які соцме-режі	Будь-які соцме-режі
Відправка SMS	Сайти всіх моб. опреато-рів, веб-форми, Skype	Сайти всіх моб. опреа-торів, веб-форми, Skype	Сайти всіх моб. опреа-торів, веб-форми, Skype	Сайти всіх моб. опреато-рів, веб-форми, Skype	Сайти всіх моб. опреа-торів, веб-форми, Skype	Сайти всіх моб. опреа-торів, веб-форми, Skype
Контроль по-шукових за-питів	ТАК	ТАК	НІ	ТАК	ТАК	ТАК
Форуми	Будь-які	Будь-які	Будь-які	Будь-які	Будь-які	Будь-які
Файлообмін-ники	ТАК	ТАК, настро-ються вручну	ТАК	ТАК, на-строю-ються вручну	ТАК, настро-ються вручну	ТАК
Нестандартні протоколи	НІ	НІ	НІ	TCP	ТАК	ТАК

Виходячи з огляду систем, можна зробити висновок, що всі вони майже однакові по своєму функціоналу і для підприємства треба підбирати саме ту

DLP-систему, яка підійде для вузькоспеціалізованого моніторингу мережі і каналів витоку.

2.3 Висновок до другого розділу

Як і у випадку з будь-якими продуктами, часом важко прорізати маркетингові матеріали та з’ясувати, чи справді продукт відповідає потребам. Наступні кроки повинні звести до мінімуму ризики і допомогти з рішенням.

1. Відправити постачальникам топологію підприємства
2. Перш ніж залучати кого-небудь, зв’яжіть дані від постачальника з тим пректом, що ви маєте на думці. Вам також слід використовувати зовнішні джерела досліджень та порівняння продуктів.
3. Запросити до себе представника фірми-постачальника.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ DLP-СИСТЕМИ НА ПІДПРИЄМСТВІ

3.1 Модель розробки системи безпеки інформації на підприємстві

Безпека конфіденційної інформації при її обробці в інформаційних системах забезпечується за допомогою системи захисту, що включає організаційні заходи та засоби захисту (технічні) інформації, у тому числі шифрувальні (криптографічні засоби, засоби для забезпечення попередження несанкціонованого доступу, витокам по технічним каналам, програмні і технічні засоби впливу на технічні засоби обробки конфіденційної інформації, а також використання в інформаційній системі інформаційних технологій.

Технічні та програмні засоби, а також нормативні правила поведінки з конфіденційною інформацією співробітниками повинні відповідати вимогам законодавства України.

Технічні засоби, що дозволяють здійснювати обробку конфіденційної інформації на об'єктах інформації це засоби вичислювальної техніки, інформаційно-вимірні комплекси та мережі, засоби та системи передачі, прийняття та обробки конфіденційної інформації і програмні засоби захисту інформації, які застосовуються в інформаційній системі.

Для забезпечення безпеки конфіденційної інформації при її обробці в інформаційних системах підприємства необхідно захищати усі можливі канали витоку та втрати інформації.

Для створення ідеальної системи захисту від витоків інформації і організації робіт по захисту конфіденціальної інформації портібно зробити наступне:

-Визначити загрози безпеці інформаціїї при її обробці і транспортуванні і формуванню на їх основі моделі загроз.

-Розробити систему захисту інформації, яка забезпечує нейтралізацію загроз, визначених в моделі.

-Перевірити готовність встановлення нових правил і програм на пристрої обробки інформації.

-Забезпечити співробітників служби безпеки підприємства правилами роботи.

-Створити систему слідкування за співробітниками, які допущенні до роботи з конфіденційною інформацією.

-Створити систему захисту апаратно-програмного забезпечення.

-Створити систему фізичної безпеки співробітників.

3.2 Опис існуючого підприємства

За існуюче підприємство мною була взята вигадана фірма ‘Kondratenko’, топологія якого зображена на рисунку 3.1.

Всі пристрої (в тому числі і мережеві), необхідні для функціонування локальної та глобальної мережі:

Cisco switch 2960 – 2;

Cisco router 2911 – 2;

Sico Server-PT – 2;

PC – 10;

Система організована за топологічною системою ‘Зірка’.

Топологія Зірка - це топологія з явно виділеним центром, до якого підключаються всі інші абоненти. Весь обмін інформацією йде винятково через центральний комп’ютер, на який у такий спосіб лягає дуже більше навантаження, тому нічим іншим, крім мережі, воно займатися не може. Зрозуміло, що мережне устаткування центрального абонента повинне бути істотно більше складним, чим устаткування периферійних абонентів. Про рівноправність абонентів у цьому випадку говорити не доводиться. Як правило, саме центральний комп’ютер є самим потужним, і саме на нього покладають всі функції по керуванню обміном.

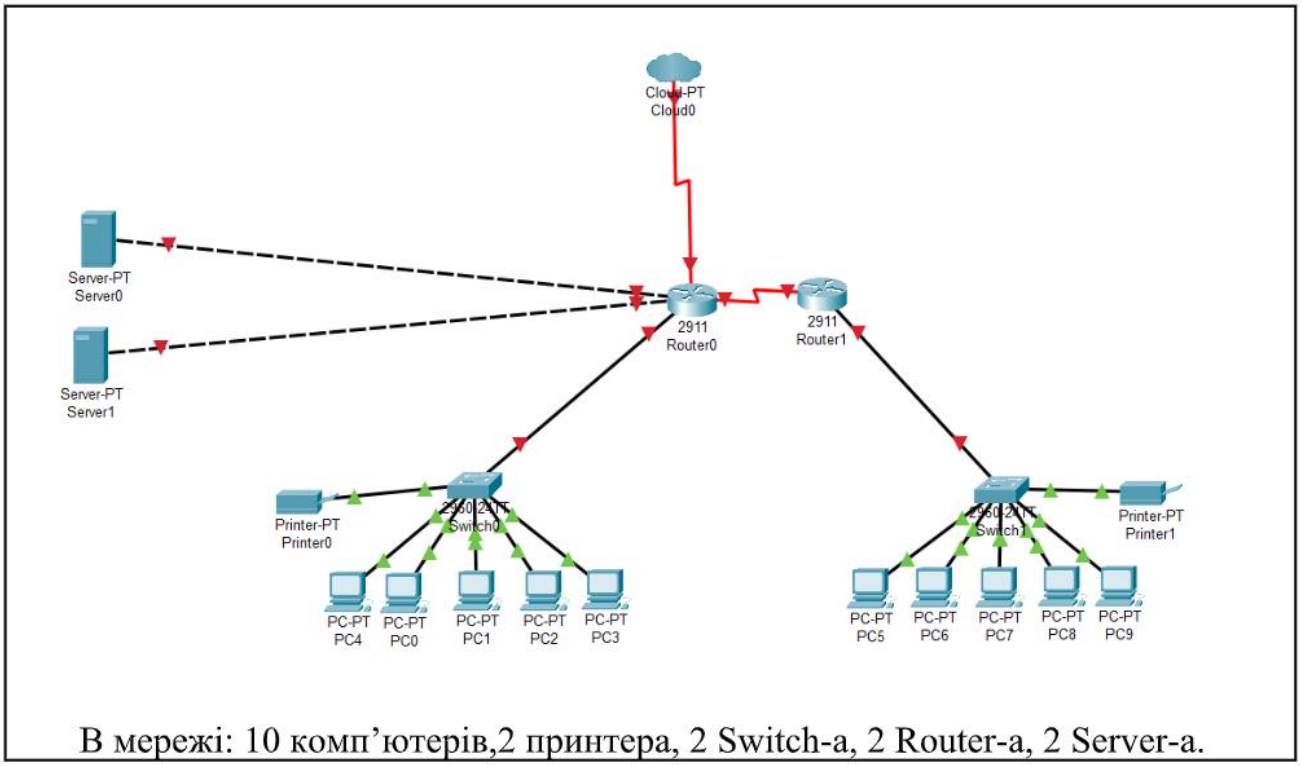

Рис. 3.1 Топологія локальної мережі фірми ‘Kondratenko’

Фізичний проект можна побачити на рисунку 3.2. В офісі підприємства знаходяться 4 кімнати, дві з яких відведені для кімнат персоналу, одна являється серверною і кімната начальника відділу з роутерами. Усі кімнати обладнані скляними розсувними дверима, в кожній с них є по дві розетки, вікон немає, бо приміщення підвальне.

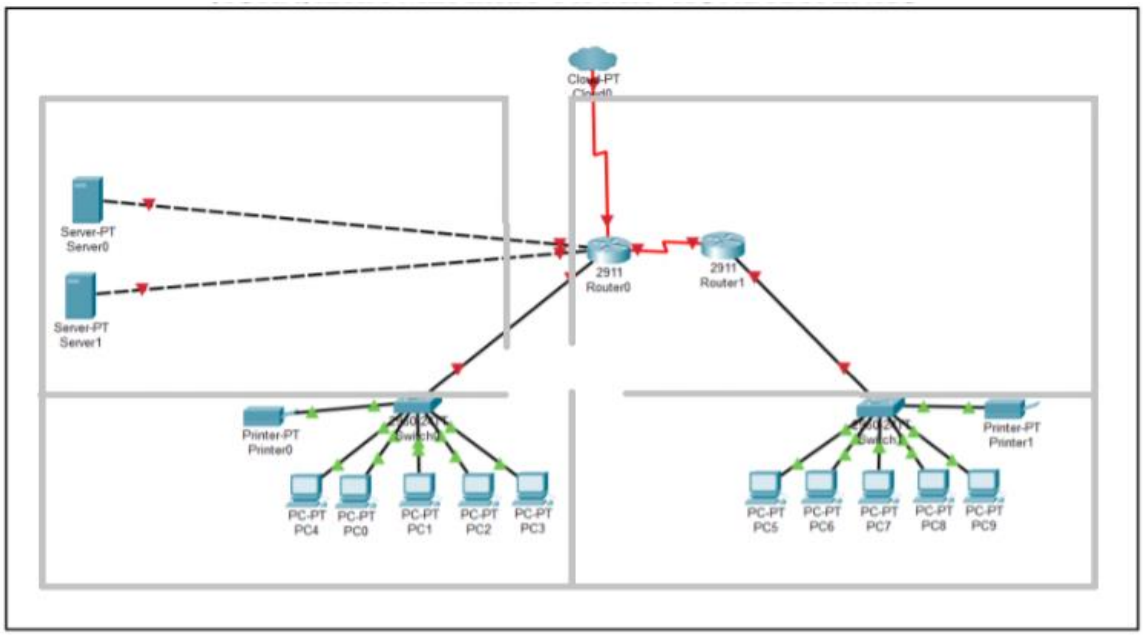

Рис.3.2 Фізична модель кімнати.

На роутерах встановлено IDS система та Firewall. На кожному пк встановлено антивірус. При взламі серверів можна будет виконати Backup.

Вид діяльності-збереження та обробка даних користувачів інтернет-магазину цифрових послуг.

Зберігаються та оброблюються: Повні імена, e-mails, адреси, ip, історія купівель, номери телефонів клієнтів. Оброблятися будуть у вигляді таблиць баз даних Oracle.

Приблизний об’эм обробки даних за місяць - 100 Гб.

На фірмі працює 12 працівників, які відносяться до різних відділів.

Технічне відділення – 4 особи (повний допуск), відділ управління - 4 особи (повний допуск), відділ офісних працівників – 4 особи (обмежений допуск).

Характеристики використованої техніки:

Роутер: Cisco 2911 router

-WAN інтерфейс : 3x10/100/1000 BASE-T Gigabit Ethernet

-LAN інтерфейс: 3x10/100/1000 BASE-T Gigabit Ethernet

-Стандарти Wi-Fi : 802.11b/g/n

-Функції безпеки: Cisco Security Manager; VPN encryption; Cisco IOS Firewall; Cisco IOS Zone-Based Firewall; Cisco IOS IPS; Cisco IOS, Content Filtering; AAA; DES; 3DES; AES.

-Додаткові інтерфейси :

1 консольний порт управління, роз’єм RJ-45;

1 консольний порт управління, коннектор Mini-USB тип B;

1 послідовний допоміжний порт, роз’єм RJ-45;

2 порти USB 4-пін USB тип A.

-Пам’ять:

Стандартна пам’ять:512 МБ

Максимум пам’яті: 2 Гб

Технологія пам’яті: DRAM

Флеш-пам’ять: 256 МБ

Switch: Cisco switch 2960

-Тип портів: Gigabit Ethernet (10/100/1000)

-Кількість портів: 24

-Розміри: 445 × 45 × 279 мм

-Кількість портів Gigabit Ethernet 24

-Інші порти CON порт RJ-45, SFP (mini GBIC) - 4 шт.

-Додаткові характеристики: Внутрішня пропускна здатність - 216 Гбіт /с

Auto-MDI / MDI-X

IEEE 802.1q (VLAN)

Максимальна кількість VLANs - 1023

Підтримка роботи в стеку

-Частота процесора - 600 МГц

-Об’єм оперативної пам’яті - 512 МБ

-Обсяг Flash пам’яті - 128 МБ

-Web-інтерфейс

-Підтримка операційних систем MacOS, NetWare, UNIX or Linux, Windows 98 / NT / 2000 / XP / Vista / 7/8/10

Сервер: Cisco UCS C240 M5

-Процесор Intel Xeon Scalable

-Кількість ядер до 28 ядер

-Форм-фактор 2U

-Максимально процесорів 2

-Тип памяти DDR4

-Максимально слотів пам’яті 24

-Формат дисків SFF 2,5, LFF 3,5

-Максимальна кількість дисків 26

-Піддтримка модулей пам’яті 8, 16, 32, 64, 128 Гб

-RAID-контроллер 12 Гбит/с SAS.

Характеристики ПК:

-Модель: Logicpower 2013-400 Tower new

-Процесор: Intel Core i5-4440 (4 ядра по 3.1-3.3GHz), 6 MB cache

-Материнська плата: MSI H81M-P33

-Оперативна пам’ять: 8 GB DDR3

-Постійна пам’ять: 240 GB SSD + 500 GB HDD

-Графіка: інтегрована Intel HD Graphics 4600

-Блок живлення: Logicpower 400W new

-Порти: 6 x USB 2.0, 2 x USB 3.0, VGA, DVI, 2 x PS/2, LAN (RJ-45), 5 xAudio, FireWire.

-Оптичний привід: нема.

Система запобігання витоків інформації представлена лише використанням фаерволу Outpost firewall Pro, вбудованим в Windows 10 антивірусом Windows Defender, функціями роутерів Cisco: Cisco Security Manager; VPN encryption; Cisco IOS Firewall; Cisco IOS Zone-Based Firewall; Cisco IOS IPS; Cisco IOS, Content Filtering; AAA; DES; 3DES; AES.

Є обмеження доступу звичайних співробітників до серверної кімнати і до адміністративних вункцій управління інформацією в базах даних.

Комплексна система DLP не розгорнута.

Усі дії співробітників фірми з даними відбуваються згідно з Законом України ‘Про захист персональних даних’. Цей Закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.

Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

3.3 Розгортання комплексоної DLP-системи і перевірка працеспроможності

Найважливішим кроком для підвищення ефективності DLP являється розгортання на підприємстві комплексної системи запобігання витоків інформації. Оскільки для такої системи потрібен адміністратор, потрібно буде вирішити юридичні питання, бо в його руках опиниться одразу вся інформація, перехоплена даною системою, а також всі дані серверів. Тому, треба буде виконати такі юридичні дії:

-Додаткові пункти для трудовоих договорів.

-Зміни до робочого розпорядку працівників.

-Додаткові політики для використання систем обробки інформації.

Наступним кроком буде вибір комплексної DLP-системи.

Облік даних ведеться з використанням Oracle. Основуючись на даних, які було розглянуто в другій частині роботи, оптимальним варіантом буде рішення від McAfee, тому розгортати будемо саме її.

Для початку, треба налаштувати місце системного адміністратора, який буде керувати політиками безпеки і обробляти дані по інцидентам. На його робочу станцію встановлюється компонент ePolicy Orchestrator (ePO).

Далі на робочі місця співробітників фірми встановлюється DLP Endpoint. Це сервіс, який і виконує основний контроль даних на машинах співробітників. Саме він відстежує трафік на каналах витоків інформації через, наприклад, пошту, файлообмінники, хмарні сервіси, сервіси моментального обміну повідомленнями тощо.

Наступним встановлюється DLP Prevent, який призначений для контролювання HTTP/HTTPs/SMTP, тобто різних варіацій пошти, мессенджери, блоги. При виявленні порушень політик безпеки, програма дозволяє зашифрувати дані, заблокувати їх передачу і перемістити документ, який передають, в карантин. McAfee DLP Prevent інтегрується з сервером MTA або веб-проксі-сервером

для відстеження трафіку електронної пошти та веб-трафіку для запобігання інцидентів потенційної витоку даних.

На рисунку 3.3 зображено принцип дії перехоплення і моніторингу інформації за допомогою DLP Prevent.

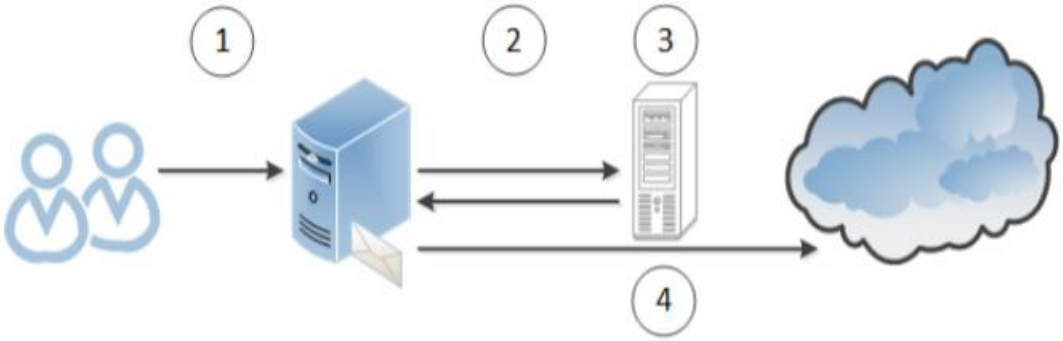

Рис. 3.3 Принцип дії захисту трафіку електронної пошти за допомогою DLP Prevent.

1. Користувачі - вхідні або вихідні повідомлення електронної пошти надходять на сервер MTA (агент трансферу повідомлень).

2. Сервер MTA - перенаправляє електронну пошту в McAfee DLP Prevent.

3. McAfee DLP Prevent - отримує підключення SMTP від сервера MTA і:

-Розбирає повідомлення електронної пошти на компоненти

-Витягує текст для ідентифікації вмісту по його відбиткам і аналізу за допомогою правил

-Аналізує повідомлення електронної пошти на предмет порушення політик

-Додає заголовок X-RCIS-Action

-Відправляє повідомлення на налаштований проміжний узел. В цьому прикладі в якості проміжного вузла виступає вихідний сервер MTA.

4. Сервер MTA - на основі інформації , отриманої із заголовка X-RCIS-Action, сервер MTA виконує з електронною поштою відповідні дії.

Принцип дії захисту веб-трафіку за допомогою DLP Prevent зображено на рисунку 3.4.

McAfee DLP Prevent приймає підключення ICAP від веб-проксі-сервера, аналізує вміст і визначає, чи пропустити трафік або заблокувати його.

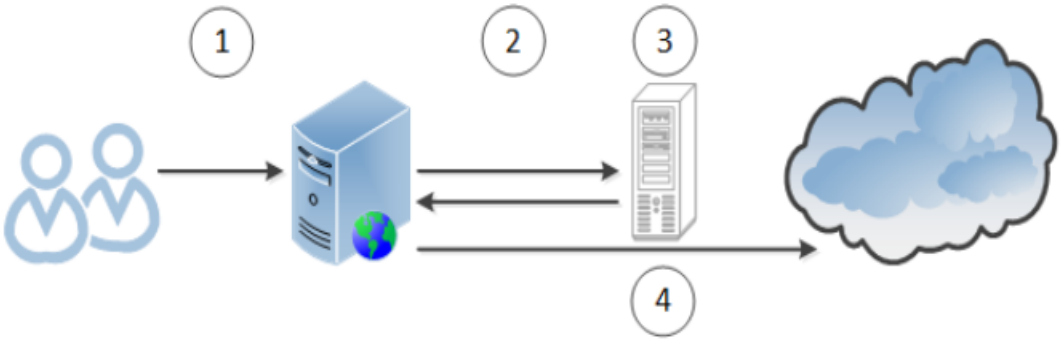

Рис. 3.4 Принцип дії захисту web-трафіку за допомогою DLP Prevent.

1. Користувачі відправляють веб-трафік на веб-проксі-сервер.

2. Веб-проксі-сервер перенаправляє веб-трафік на McAfee DLP Prevent.

3. McAfee DLP Prevent перевіряє веб-трафік і повертає його на веб-проксі-сервер, щоб дозволити його передачу через сервер призначення або заборонити доступ.

4. Веб-проксі-сервер відправляє перевірений веб-трафік на відповідний адрес призначення.

Далі встановлюється DLP Monitor, який відслідковує корпоративної мережі в реальному часі, проводить розслідування інцидентів. Сканує та аналізує трафік, підтримує пртоколи:

1. FTP - мережевий протокол для пересилання файлів між клієнтом та сервером в корпоративній мережі.

2. HTTP - найпоплуярніший протокол передачі даних.

3. IMAP – протокол доступу до елетронної пошти.

4. IRC – протокол обміну повідомленнями в реальному часі.

5. LDAP – протокол доступу до дерикторій і каталогів.

6. POP3 - стандартний поштовий протокол.

7. SMB - мережевий протокол для віддаленого доступу до файлів і пристроїв в мережі.

8. SMTP - простий протокол для зв’язку серверів при передачі пошти.

Також проводить аналіз даних в усій базі даних на сервері.

McAfee DLP Monitor використовується, щоб дізнатися обсяг і типи даних, що переміщуються через мережу. McAfee DLP Monitor не блокує і не змінює мережевий трафік, тому можлива інтеграція в мережеве середовище підприємства без впливу на реальний трафік.

Останнім встановлюэться DLP Discoverer. Це програмне забезпечення для серверів, використовуться для пошуку критичних даних, співпрацює з SharePoint, Microsoft SQL, MySQL, Oracle.

Після встановлення всіх цих рішень система вважається розгорнутою.

Далі її треба налаштувати.

Першим, що треба зробити – класифікувати файли на кожній з робочих станцій та створити політику правил. На рисунку 3.3 зображено меню програми DLP Endpoint. Там ми обираємо вкладку ‘Classification’.

Класифікація даних - це процес, який використовується для оптимізації програм, процедур та процесів захисту даних.

Дані потрібно класифікувати на основі їх типу чутливості та рівня впливу на організацію, якщо ці дані будуть знищені, змінені або розкриті.

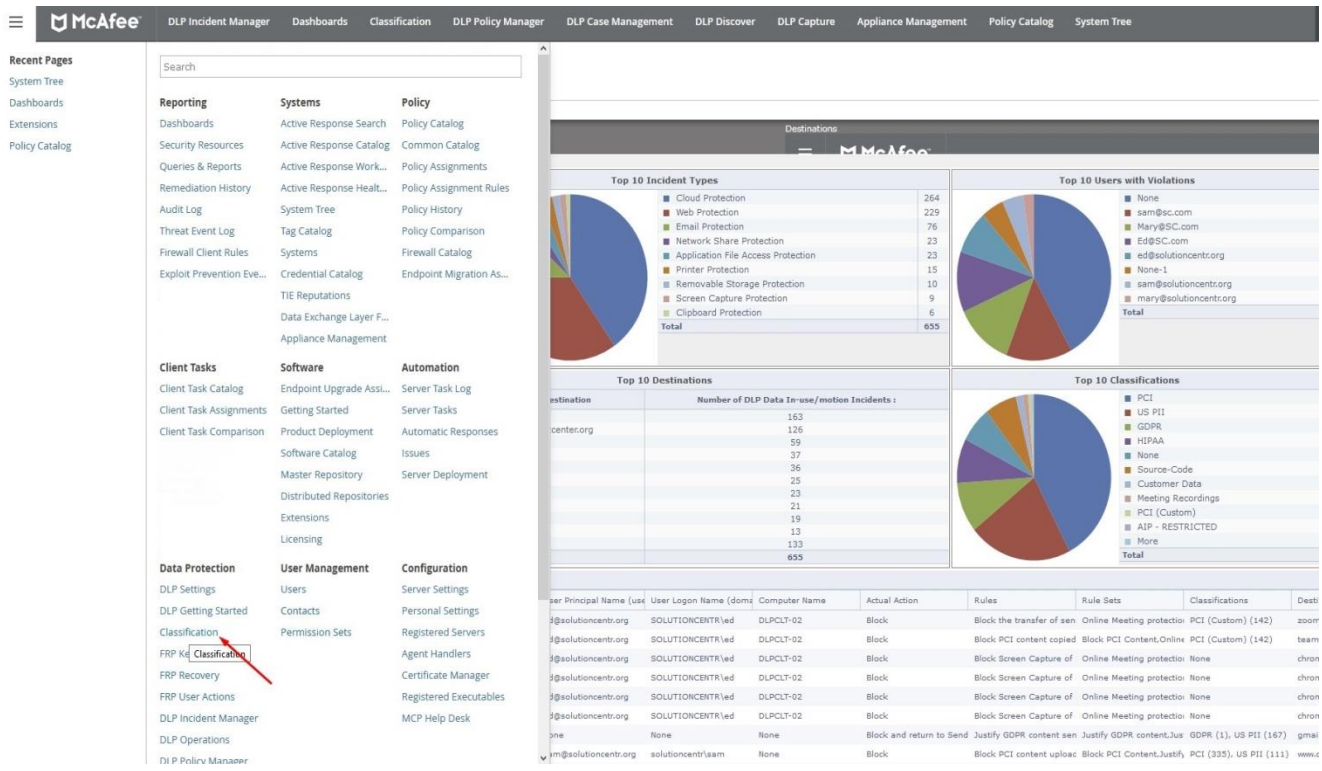

Рис. 3.5 Головне меню

Далі вводимо тип даних для розпізнавання, наприклад номери телефонів чи домени електронних пошт. Відбуваться це у меню Actions → New Classification Criteria → Advenced Pattern, як показано на рисунку 3.5, 3.6.

Існують варіанти точного співпадіння інформації, співпадіння з бібліотеками, пошук за основним словом і за схожістю.

Зберігаємо наш вибір і переходимо до створення політики правил.

Будь-яка розроблена політика безпеки DLP-системи є зведенням певних правил, які неухильно виконуються програмою.

На етапі проектування та середовища виконання разом оцінюються всі набори правил, що застосовуються до середовища, в якому перебуває програма або цикл. Це робиться для того, щоб вирішити, чи відповідає ресурс політиці DLP або чи порушує цю політику.

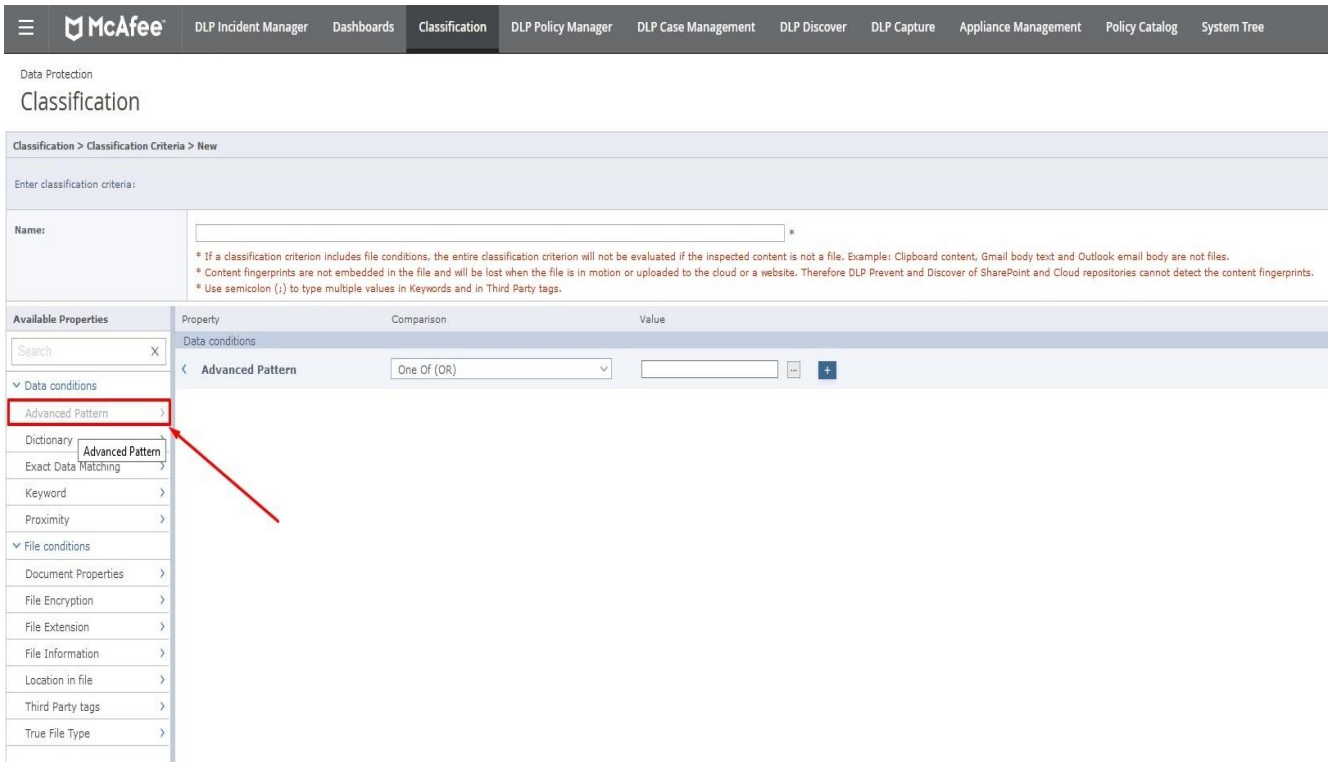

Рис 3.6 Меню підбору класифікації

Зберігаємо наш вибір і переходимо до створення політики правил.

Для створення нової політики слід перейти в менеджер політик, потім Actions → New Rule Set і створити набір правил, як показано на рисунку 3.7.

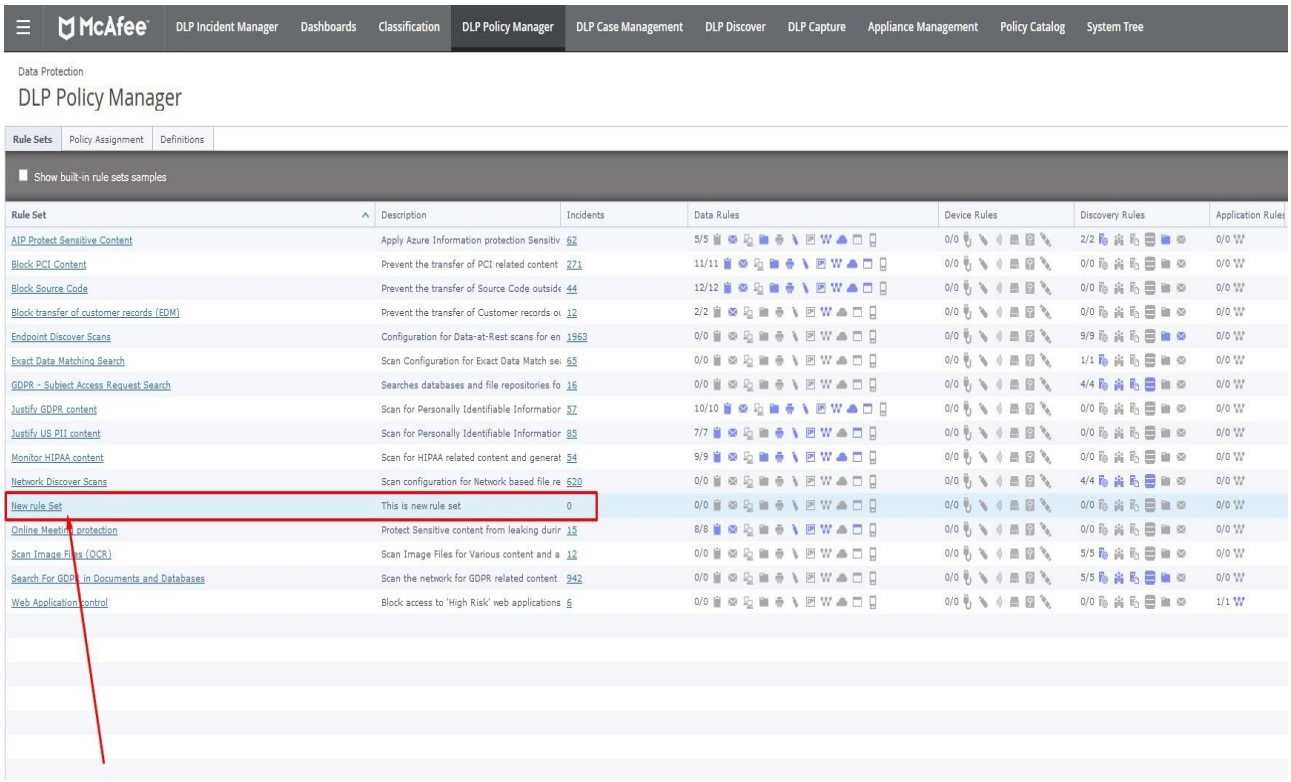

Рис 3.7 Створення набору правил

Далі треба вказати шлях до охороняємого файлу чи папки. Після цього вибираємо, як саме повинна реагувати на порушення правила. Можна виставити Блокування передачі і доповісти про цей інцидент адміністратору,рисунок3.8

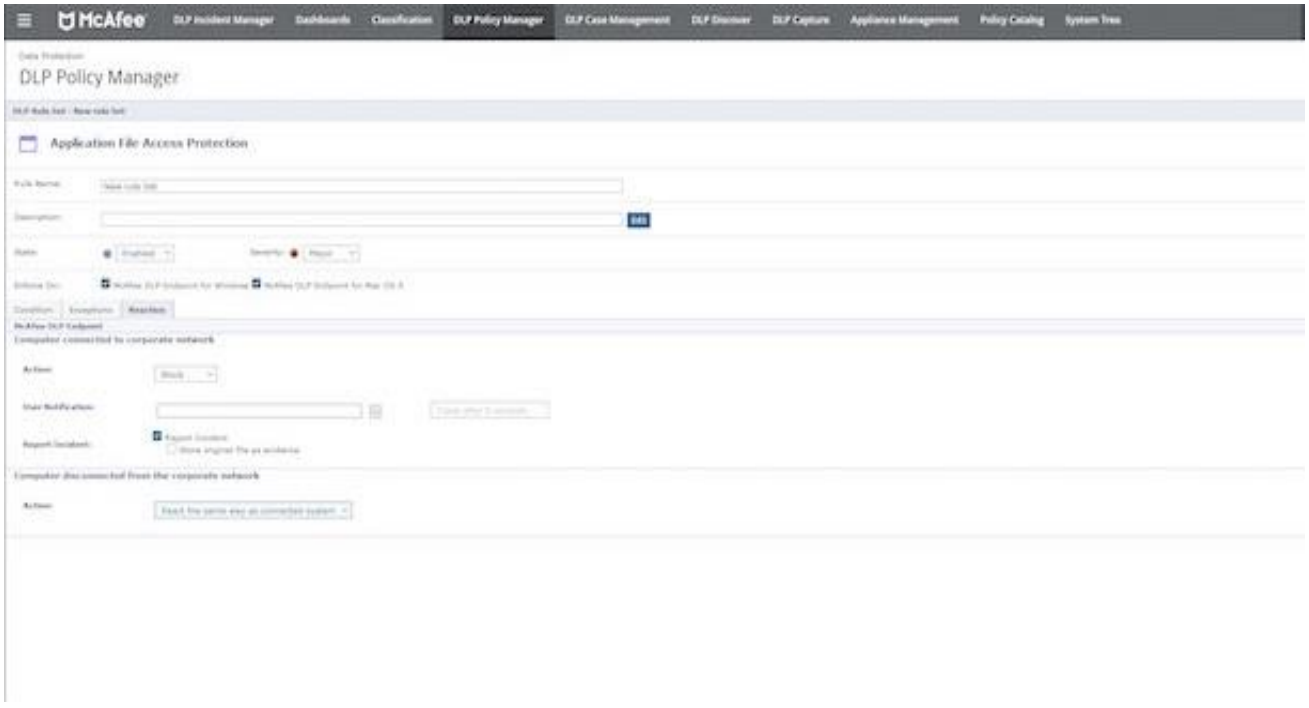

Рис. 3.8 Установки реакції системи на порушення правила

За даною схемою встановлюються усі правила, які можуть бути корисним для ефективного попередження витоків інформації.

Усі правила можна переглянути у вікні rule sets, як зображено на рис.3.9.

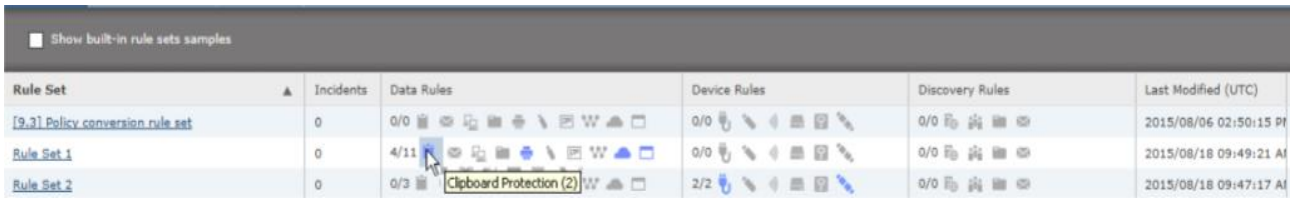

Рис. 3.9 Список створених правил.

Далі важливо перевірити, чи не відбулася помилка при створенні правил. Шляхом спроби провести крадіжку інформації перевіряємо найбільш поширені канали витоку.

На рис 3.10 зображений приклад повідомлення при спробі ввести захищаєму інформацію на веб-сторінці.

Рис 3.10 Блокування спроби вивести дані на веб-ресурс.

Далі розглянуто спробу відправити файл через месенджер. Правило спрацювало, що видно на повідомленні з рисунку 3.11

На жаль, в месенджері Telegram використовується криптографічний протокол MTProto, моніторинг якого не підтримується у даному рішенні запобігання витоків інформації.

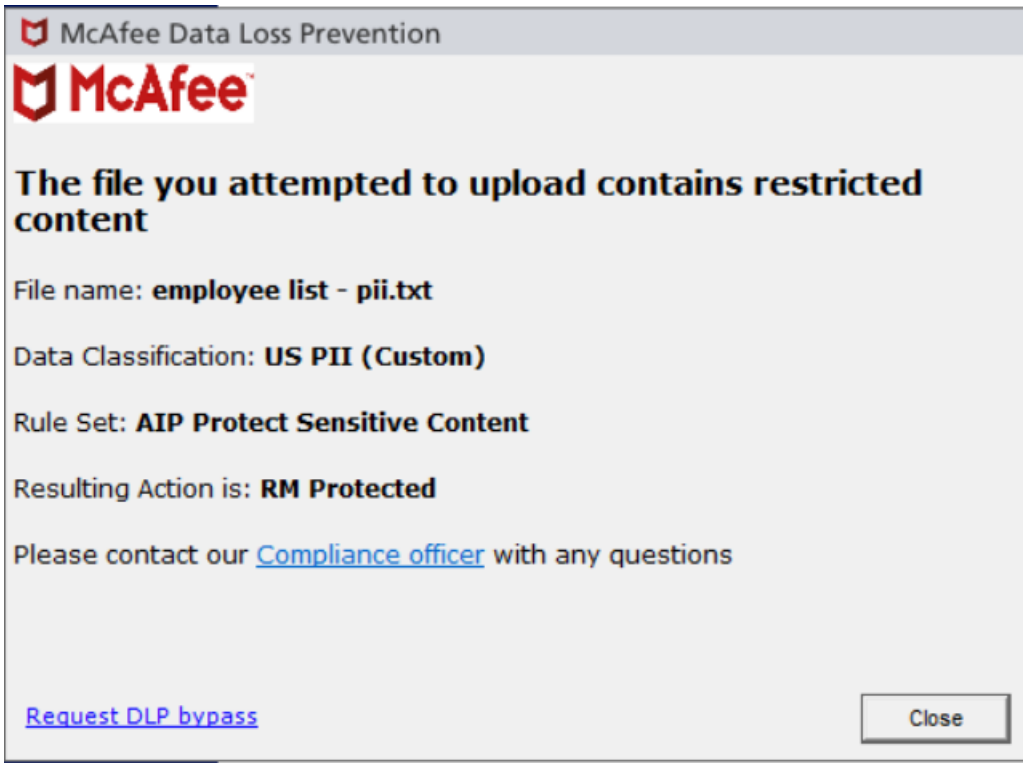

Рис 3.11 Спрба відправити файл через сервіс моментальних повідомлень.

На рис 3.12 зображений приклад повідомлення при спробі вивести захищаєму інформацію через електронну пошту.

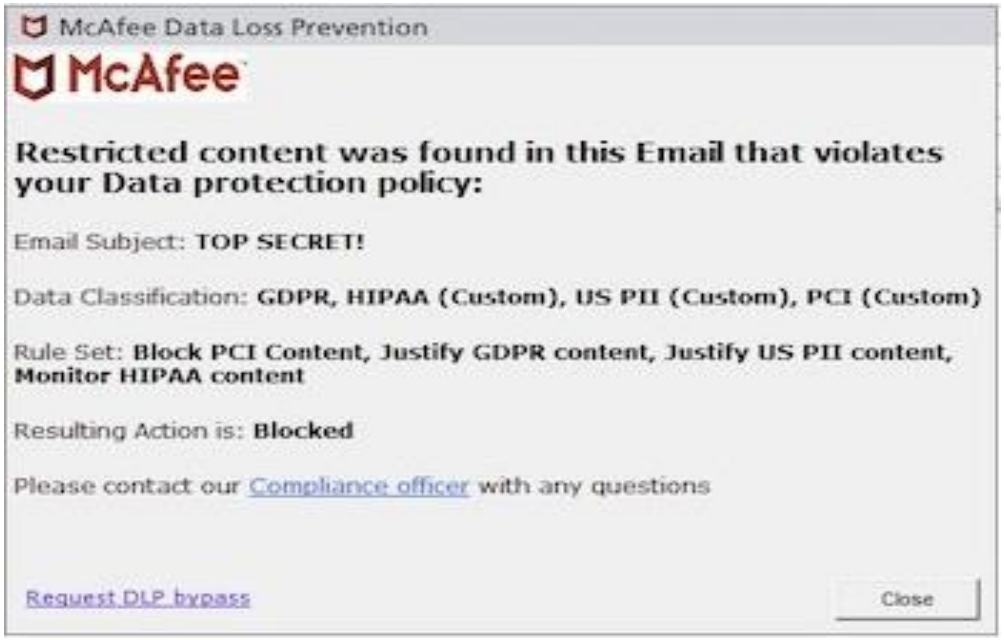

Рис 3.12 Блокування спроби вивести дані через пошту.

Також не треба забувати про спроби скопіювати інформацію на фізичний носій. З цим система впоралась теж без проблем, що показано на рисунку 3.13.

Рис 3.13 Блокування спрби копіювання інформації на фізичний носій.

Усі спроби нелегальних дій відображаються на інтерфейсі даних про інциденти, що спрощує роботу адміністратору системи інформаційної безпеки. Інтерфейс показано на рисунку 3.14.

McAfee DLP представляє різні інструменти для перегляду інцидентів і робочих подій.

-Інциденти - на сторінці Диспетчер інцидентів DLP відображаються інциденти, які відповідають встановленим політикам.

-Робочі події - на сторінці Операції DLP відображаються помилки і адміністративна інформація.

-Проблеми - сторінка управління проблемами DLP містить проблеми, створені з метою групування пов'язаних інцидентів і управління ними.

-Коли встановлено кілька продуктів McAfee DLP, в консолях відображаються інциденти і події усіх продуктів.

Рис 3.14 Інтерфейс даних про інцеденти.

Окрім цього, в інтерфейсі показуються поточні дані навантаження на мережу, використання потужностей кожної машини в межах корпоративної мережі і інші функції, які спрощують відстежуування за трафіком. Важливим є екран працеспроможності системи. Приклад зображено на рисунку 3.15.

Інформація, яку показує даний екран:

-Evidence Queue (Черга підтверджень) - кількість файлів, очікуючих на копіювання в сховище підтверджень. Розмір черги вказується в режимі реального часу.

-Emails (Електронна пошта) - кількість доставлених, остаточно чи тимчасово відхилених повідомлень, а також кількість повідомлень, які не вдалося проаналізувати. Лічильники відображають актуальні дані заостанні 60 секунд.

-Web Requests (Веб-запити) - кількість отриманих веб-запитів, а також кількість веб-запитів, які не вдалося проаналізувати. Відображаються актуальні дані за останні 60 секунд.

-CPU usage (Завантаження ЦП) - використання ресурсів центрального процесора.

-Memory (ОЗУ) - частота підкачки оперативної пам'яті.

-Disk (Диск) - використання диска в процентах.

-Network (Мережа) - відомості про обсяг отриманих та переданих дани через мережеві пристрої. Лічильники відображають актуальні дані за останні 60 секунд.

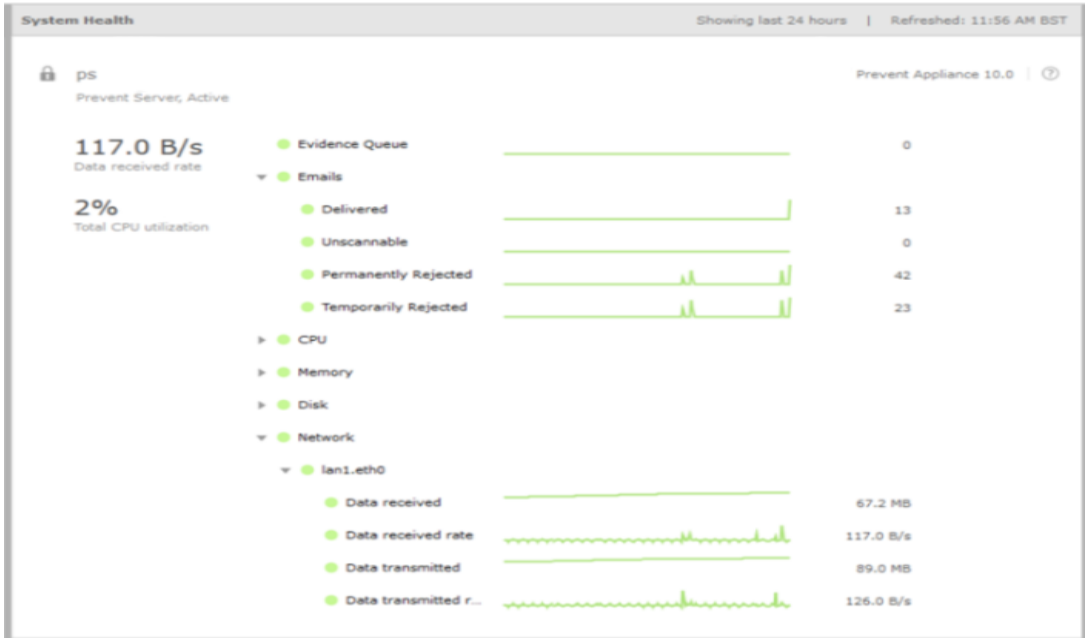

Рис 3.15 Екран працеспроможності системи.

Провівши порівняльний аналіз ступеней ризику витоків інформації через основні канали, створив таблицю 3.1

Аналіз проводив на основі власних спостережень і даних з різних сайтів.

Значно знилися ризики:

-витоку через веб-додатки

-витоку через пошту

-витоку через моментальні повідомлення

-витоку через копіювання на фізичні носії

Отже, ризики витоку через інсайдерів взагалом знизилися, але зовнішні ризики досі є.

Табл. 3.1

Порівняння ризиків витоків інформації основними каналами.

Канал витоку інформації	Ступінь ризику до розгортання DLP-системи	Ступінь ризику після розгортання DLP-системи
WEB портали	Високий	Низький
Пошта	Високий	Низький
Моментальні повідомлення	Високий	Низький
Через інсайдерів	Високий	Середній
Копіювання на фізичні носії	Високий	Низький
Взлом серверів	Високий	Середній

3.4 Додаткові рекомендації для підвищення рівня захисту

Захист від витоків інформаціїї не завершується на встановленні серверних та агентських рішень. Завжди залишається шанс проникнення на територію підприємства сторонніх осіб і у співробітників є можливість зняти дані з моніторів на власні пристрої, наприклад, на камеру мобільного телефону. Для унеможливлення цих дій потрібно зробити наступні кроки.

-Провести адміністративно-організаційні заходи.

Мається на увазі створення політики безпеки, що являє собоє сукупність документальних рішень, які приймаються директором фірми і начальником служби безпеки підприємства. Базуватися вона повинна, основуючись на аналіз ризиків інформаційної системи підприємства.

-Розробити документацію.

Уся документація стосовно захисту конфіденційності оброблюваної інформації повинна строго відповідати державним нормативно-правовим актам що-

до захисту інформації. Також, треба отримати державну ліцензію, що спростить вирішення питань в суді, якщо витік інформації таки станеться.

-Провести роботу з персоналом.

Витки через персонал являються найпоширенішими, тому приділяти увагого роботі з персоналом треба найбільше. При роботі з базами даних обов'язково повинна розробитися політика допусків до інформації і розмежування працівників по ролям.

-Створити пропускний режим на підприємстві.

Необхідність контролювати територію підприємства від сторонніх осіб є у всіх підприємст будь якого роду діяльності. Відбувається контроль через створення контрольно-пропускного пункту.

Після завершення будівництва (реконструкції, ремонту) на вікнах об'єкту необхідно встановити пристрої, які не дозволяють оглядати приміщення ззовні (штори, жалюзі тощо) незалежно від поверху і наявності будівель, розташованих навпроти.

Вимоги, спрямовані запобіганню несанкціонованого доступу до об'єкту або до окремих його елементів:

1. Вхідні двері зали для проведення секретних нарад з коридору обладнуються надійним замком, а також пристроєм, що сигналізує про доступ до об'єкту (чашка для опечатування, лічильник відкривання дверей, петлі для опломбування або використання плашок для опечатування тощо).

2. Кришки оглядових люків, інші елементи доступу до ніш, шахт тощо, в яких прокладені комунікації, обладнуються засобами замикання та пристроями для опломбовування.

3. Об'єкт оснащується охоронною сигналізацією, яка повинна бути виведена на пульт централізованого спостереження підрозділу охорони. Для живлення охоронної сигналізації в аварійних випадках має передбачатися автономне джерело живлення. Переключення на автономне джерело живлення має бути автоматичним.

Типи та види охоронної сигналізації повинні відповідати встановленим вимогам і мати відповідний сертифікат.

Вимоги, спрямовані запобіганню витоку ІзОД каналом паразитних електромагнітних випромінювань і наведень:

1. Телекомунікаційні мережі та мережі електроживлення прокладати в металевих рукавах з обов'язковим заземленням.

2. Транзитні трубопроводи, повітроводи та інші металеві елементи інженерних комунікацій не повинні проходити через ОІД, але якщо цього не уникнути, то вони обладнуються вставками з ізоляційного матеріалу.

3. Виключити транзитне проходження будь-яких кабелів (комп'ютерної мережі, сигналізації, голосового оповіщення, силових мереж тощо) через ОІД, а також спільний пробіг в одному каналі кабельних ліній різного призначення (силові та сигнальні). Відстань між ними повинна складати не менше 0,8 м.

Вимоги, спрямовані на забезпечення протипожежної безпеки на ОІД:

1. Опорядження стін, матеріали підвісних стель, розсіювачі світильників повинні бути із негорючих матеріалів.

2. Як засоби шумопоглинання повинні застосовуватися негорючі (НГ) або низької горючості (Г1) спеціальні перфоровані плити, панелі, мінеральна вата з максимальним коефіцієнтом звукопоглинання у межах частот 31,5 - 8000 Гц або інші матеріали аналогічного призначення, дозволені для оздоблення приміщень органами державного санітарно-епідеміологічного нагляду.

3. Об'єкт оснащується автоматичною пожежною сигналізацією. Тип та вид пожежної сигналізації має відповідати встановленим вимогам і мати відповідний сертифікат.

3.5 Висновок до третього розділу

Після аналізу ринку послуг DLP-систем, в ході роботи було підібрано комплексну систему запобігання витоків інформації, яка максимально підійшла

для даного підприємства. Після розгортання вибраної DLP-системи, ризики витоку інформації зменшилися до мінімальних, що свідчить про успішну її інтеграцію в мережу підприємства. Не зважаючи на це, ризики витоку через необачність працівників завжди залишається, адже вони можуть видати важливу інформацію в звичайній бесіді з товаришем.

ВИСНОВКИ

З кожним роком в світі стається все більше витоків конфіденційної інформації з баз даних підприємств, що завдає величезних збитків компаніям. Йдеться не лише про гроші і втрачені можливості, але й про авторитет фірми. Тому нині найважливішим кроком для кожної фірми, яка зберігає будь-яку інформацію, є системи запобігання витокам інформації.

Практика показує, що найбільше витоків відбувається через самих співробітників фірм, як через інсайдерів, так і за звичайною необачністю.

Системи захисту від витоків інформації призначені для відстежування і блокування передачі даних за межі корпоративної мережі, але окрім цього дані системи можуть відстежувати дії співробітників даного підприємства в мережі.

В ході дипломної роботи були розглянуті імовірні загрози витоку інформації на підприємстві, їх було класифіковано і знайдено шлях мінімізувати ці ризики. Було проведено порівняльний аналіз комплексних систем запобігання витоків інформації і обрано оптимальний варіант для попередження найпопулярніших загроз. На практиці перевірено працеспроможність системи McAfee, і досліджено її функціонал, а саме:

-Запобігання витоку через WEB-портали.

-Запобігання витоку через месенджер.

-Запобігання витоку через копіювання даних на фізичний носій.

-Запобігання витоку через пошту.

Перевагами цієї комплексної системи являються: легкий інтерфейс, легкість створення та налаштування правил, велика кількість інтегрованих програм, можливість відстежувати працеспроможність усіх систем в корпоративній мережі, велика кількість різних рішень, які підійдуть для будь-якої фірми.

Після розгортання системи запобігання витокам інформації можливість витоків через основні канали максимально зменшилася, але це не дає змоги ска-

зати, що ситсема на 100% захищає інформацію від витоків, адже з кожним роком з’являються нові технології, які полегшують крадіжки.

Останнім часом вимоги до функціональних можливостей DLP-систем постійно зростають, що призводить до перетворення їх в один з найефективніших, комплексних і системних рішень в сфері захисту конфіденційної корпоративної інформації. В роботі був проведений аналіз найпопулярніших DLP-систем, розглянуті їх функції та характеристики.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Аверченков, В.И. Криптографические методы защиты информации/ В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак, –Брянск: БГТУ, 2010. –216 с.9.

2. Аверченков В.И. Организационная защита информации: учеб. Пособие для вузов / В.И. Аверченков, М.Ю. Рытов. –Брянск: БГТУ, 2005. –184 с.10.Болдырев

3.А.И. Методические рекомендации по поиску и нейтрализации средств негласного съема информации: практ. Пособие/ А. И. Болдырев –М.: НЕЛК, 2001. –137 с.11

4.Большая энциклопедия промышленного шпионажа / Ю.Ф. Каторин., Е.В.Куренков, А.В. Лысов. -СПб.: Полигон, 2000. –886 с.13.

5.Малюк, А.А. Введение в защиту информации в автоматизированных системах/ А.А. Малюк, С.В. Пазизин, Н.С. Погожин. –М.: Горячая линия Телеком, 2001. –178 с.

6. Астахов А.М. Искусство управления информационными рисками / А.М. Астахов – М : ДМК Пресс, 2010. – 314 с.

7. Рассел Д., Локальная вычислительная сеть / — М.: Книга по Требованию, 2012. — 102 с.

8. Джонс К.Д., Шема М., Джонсон Б.С., Инструментальные средства обеспечения безопасности/К.Д. Джонс, М. Шема, Б.С. Джонсон.-ИНТУИТ, 2007.-1028 с.

9. Мазеркин Д. Защита коммерческой тайны на предприятиях различных форм собственности //Частный сыск и охрана.-1994г.

10. Торокин А.А. «Основы инженерно-технической защиты информации». – М.: Издательство «Ось-89» 1998 г. стр. 143

11. Информационная безопасность современного коммерческого предприятия: Монография. – Старый Оскол: ООО «ТНТ», 2005. – 448.

12. Нестеров С. А. Информационная безопасность и защита информации: Учеб. пособие. Санкт Петербург: Изд-во Политехн. ун-та, 2009. 126 с.

13. Домарев В. В. Безопасность информационных технологий. Системный подход. Киев.: ДиаСофт, 2004.

14. Infowatch. Глобальні дослідження витоків інформації починаючи з 2007 ро-ку. 2018. – Режим доступу: https://www.infowatch.ru/analytics/leaks_monitoring

15. Можливості Falcongaze DLP – Режим доступу: https://falcongaze.com/ru/product/capabilities/data-leaks.html

16. Можливості GTB DLP – Режим доступу: https://gttb.com/

17. Можливості Infowatch DLP – Режим доступу: https://www.infowatch.ru/products/traffic-monitor

18. Можливості SearchInform DLP – Режим доступу: https://searchinform.ru/products/kib/

19. Можливості Symantec DLP – Режим доступу: https://www.anti-malware.ru/products/symantec-dlp

20. Можливості McAfee DLP – Режим доступу: https://www.mcafee.com/enterprise/ru-ru/products/total-protection-for-data-loss-prevention.html

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