Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Пащенко Тимофія Валерійовича*

академічної групи *125-17-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему **Розробка засобів захисту інформації інформаційно-телекомунікаційної системи підприємства «TravelTeam» на основі DLP технології**

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф.-м.н.,проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Пащенко Тимофію Валерійовичу* **академічної групи** *125-17-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему **Розробка засобів захисту інформації інформаційно-телекомунікаційної системи підприємства «TravelTeam» на основі DLP системи**

затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № 317-С

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Постановка задачі. Проаналізували дію систем захисту від витоку конфіденційної інформації. Порівняли найактуальніші системи.	29.03.2021
Розділ 2	Оцінили ризики , виявили модель порушника. Впровадили систему протидії витоку даних в існуючу мережу	24.05.2021
Розділ 3	Розрахували економічну цінність та актуальність впровадження системи протидії витоку інформації	07.06.2021

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2021р.

Дата подання до екзаменаційної комісії: 12.06.2021р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 83 ст, 21 рис., 14 табл., 4 додатка, 15 джерел.

Об’єкт дослідження: DLP системи McAfee, DeviceLock DLP, Falcongaze SecureTower.

Мета роботи: впровадити систему протидії витоку конфіденційної інформації в мережу існуючої організації.

Методи розробки: спостереження , порівняння , аналіз, опис.

У першому розділі було проаналізована необхідність DLP систем , та їх розвиток в сучасному світі. Проаналізували можливі загрози та їх протидію на декількох системах. Визначили яку проблему вирішуюсь данні системи , провели статистичний та морфологічний аналіз DLP систем.

У спеціальній частині було визначено найкращі системи DLP , їх можливості та зручність використання. За мету є впровадження системи для всіх можливих та популярних витоків конфіденційної інформації для середньої компанії.

В економічному розділі визначено економічну доцільність розробки та впровадження рекомендацій для проведення ідентифікації інформаційних активів. Проведено розрахунок капітальних (фіксованих) витрат, поточних (експлуатаційних) витрат, загального збитку від атаки на ІТС та загального ефекту від впровадження рекомендацій.

Практичне значення роботи полягає в аналізі систем протидії витоку конфіденційної інформації, їх покращення та впровадження в систему для аналізування можливих загроз та їх виявлення зазделегідь. Тестування систем на загрозах в реальному часі.

ІНФОРМАЦІЙНА БЕЗПЕКА, DATA LOSS PREVENTION, КОНФІДЕНЦІЙНІСТЬ,ЗАСОБИ ІНФОРМАЦІЇ, АВТОМАТИЗОВАНІ СИСТЕМИ, ОБЛІК ІНФОРМАЦІЇ

РЕФЕРАТ

Пояснительная записка: 83 стр, 21 рис., 14 табл., 4 приложения, 15 источников.

Объект исследования: DLP системы McAfee, DeviceLock DLP, Falcongaze.

Цель работы: внедрить систему противодействия утечки конфиденциальной информации в сеть существующей организации.

Методы разработки: наблюдение, сравнение, анализ, описание.

В первой главе было проанализирована необходимость DLP систем, и их развитие в современном мире. Проанализировали возможные угрозы и их противодействие на нескольких системах. Определили какую проблему решаюсь данные системы, провели статистический и морфологический анализ DLP систем.

В специальной части были определены лучшие системы DLP, их возможности и удобство использования. Главной идеи является создание системы для всех возможных и популярных истоков конфиденциальной информации для средней компании.

В экономическом разделе определена экономическая целесообразность разработки и внедрения рекомендаций для проведения идентификации информационных активов. Проведен расчет капитальных (фиксированных) расходов, текущих (эксплуатационных) расходов, общий ущерб от атаки на ИТС и общего эффекта от внедрения рекомендаций.

Практическое значение работы состоит в анализе систем противодействия утечки конфиденциальной информации, их улучшение и внедрение в систему для анализа возможных угроз и выявление заранее. Тестирование систем на угрозах в реальном времени.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, DATA LOSS PREVENTION, КОНФИДЕНЦИАЛЬНОСТЬ,СРЕДСТВАИНФОРМАЦИИ,АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ, УЧЕТ ИНФОРМАЦИИ

ABSTRACT

Explanatory note: 83p, 21 figures, 14 tables, 4 appendices, 15 sources.

Object of research: DLP of McAfee system, DeviceLock DLP, Falcongaze SecureTower.

Purpose: to implement a system for counteracting the leakage of confidential information into the network of the existing organization.

Development methods: observation, comparison, analysis, description.

The first section analyzed the need for DLP systems, and their development in the modern world. We analyzed the possible threats and opposition to several systems. Determined the problem solving data systems, conducted statistical and morphological analysis of DLP systems.

The best DLP system has been identified in the special part, their capabilities and use of use. The most important idea is to create a system for all possible and popular sources of confidential information for the average company.

The economic partition defines the economic expediency of developing and implementing recommendations for identification of information assets. Calculation of capital (fixed) costs, current (operating) costs, total damage from ITS attacks and the overall effect on the introduction of recommendations has been carried out.

The practical importance of the work is to analize systems of counteraction to the origin of confidential information, improving and introducing into the system to analyze possible threats and their detection of evil. Testing systems in real-time threats.

INFORMATION SECURITY, DATA LOSS PREVENTION, PRIVACY, INFORMATION TOOLS, AUTOMATED SYSTEMS, ACCOUNTING OF INFORMATION

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

ДСТУ - Державні стандарти України;

ЕОТ - електронно-обчислювальна техніка;

ІТС - Інформаційно-телекомунікаційнасистема;

КМ - комп'ютернамережа;

КС - комп'ютерна система;

МП - модель порушника;

ОБ - офіцер безпеки;

ПК - персональний комп'ютер;

РМ - Робоче місце;

API - Application Programming Interface;

DLP - Data Loss Prevention;

HTTP - Hyper Text Transfer Protocol;

HTTPS - Hyper Text Transfer Protocol Secure;

MIME - Multipurpose Internet Mail Extension;

PPPoE - Point-to-point protocol;

IDS - Intrusion Detection Systems;

IPS - Intrusion Prevention Systems.

ЗМІСТ

ВСТУП

Сучасне життя суспільства неможливе без постійного застосування інформаційних технологій. Комп'ютерні системи обслуговують банківські системи, контролюють роботу на заводах, стежать за розкладом потягів і літаків. Інформаційна індустрія перетворилась на один із найголовніших секторів світової економіки, що динамічно розвивається та має великі перспективи подальшого росту. Інформаційна діяльність сьогодні стала необхідною умовою ефективної діяльності у всіх сферах життя. Спочатку зовнішні загрози вважались більш небезпечними. Протягом останніх років почались змінюватись тенденції, щодо особливостей, місць та обставин роботи та . І тому в останні роки на внутрішні загрози стали звертати більше уваги, і популярність DLP-систем зросла. Ситуація, коли працівник намагається надіслати таку конфіденційну інформацію конкуруючим компаніям, є прикладом витоку, який може мати погані наслідки для компанії, наприклад, втрата клієнтів, призведення до судових справ та ін. Щоб запобігти подібним витокам, системи, призначені для виявлення та захисту конфіденційних даних, були запроваджені в 2006 році і стали називатись Data Leakage (Loss) Prevention (DLP) – запобігання витоків інформації. Їх мета полягає в тому, щоб закупорювати існуючі точки витоку і блокувати несанкціоновані дії з конфіденційними даними.

Мета роботи: впровадити систему протидії витоку конфіденційної інформації в мережу існуючої організації.

Актуальність роботи зумовлюється тим, що в ній було впроваджено рішення, що до вибору найефективнішої системи протидії витоку інформації для середньої організації, а також можливі програмні нововведення які дозволяли б покращити показники роботи системи.

Для досягнення даної мети було поставлено такі завдання:

- встановлення систем DLP на віртуальні машини та їх налаштування;
- тестування систем, яке полягає в тому, щоб передати конфіденційні дані за допомогою веб-поштових клієнтів (Gmail), локальних поштових клієнтів (Windows Live Mail), соціальних мереж (Facebook), програмного забезпечення для обміну миттєвими повідомленнями (Skype), програмного забезпечення для синхронізації хмар (Google диск), програмного забезпечення для дистанційного керування (Teamviewer), принтери (мережеві та локальні) та пристрої USB;
- підведення підсумків тестування, які наведені в таблицях;

Методами дослідження обрано: опрацювання літератури за даною темою, аналіз технічної документації, тестування систем.

Практичне значення результатів роботи випливає з можливості використання створенного доповнення для покращення результатів роботи систем DLP, яке дозволить підвищити показники якості виявлення загроз витоку інформації.

Таким чином об’єктом дослідження є такі популярні системи DLP, як McAfee, DeviceLock DLP, Falcongaze SecureTower.

Предмет досліджень – здатність систем DLP реагувати на інциденти, пов'язані з витоком інформації.

РОЗДІЛ 1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

У цій главі буде проведене коротке ознайомлення з системами DLP, перераховано їх недоліки та переваги.

1.1 Ситеми протидії витоку інформації

Основним завданням DLP-систем, є запобігання передачі конфіденційної інформації за межі інформаційної системи. Така передача (витік) може бути навмисною або ненавмисною. Практика показує, що більша частина витоків (близько 3/4) відбувається не через злі наміри, а через помилки, неуважність, безтурботність, недбалість працівників. Виявляти подібні витоки простіше. Інша частина пов'язана зі злим умислом операторів і користувачів інформаційних систем.

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 обумовлено тим, що велика частина традиційних засобів захисту таких як антивіруси, міжмережеві 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 - продажу, передачі третім особам, опублікування у відкритому доступі і т.д. Вирішити проблему випадкових і навмисних витоків конфіденційних даних, покликані системи запобігання витоків даних (DLP—Data Loss Prevention).

Подібного роду системи створюють захищений «цифровий периметр» навколо організації, аналізуючи всю витікаючу, а в ряді випадків і вхідну інформацію. Контрольованої інформацією виступає не тільки інтернет-трафік, але і ряд інших інформаційних потоків: документи, які виносяться за межі захищається контуру безпеки на зовнішніх носіях, роздруковуються на принтері, що відправляються на мобільні носії через Bluetooth, WiFi і т.д.

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

1.2 Аналіз системи

Розпізнавання конфіденційної інформації DLP-системою проводиться двома способами: аналізом формальних ознак (наприклад, грифа документа, спеціально введених міток, порівнянням хеш-функції) та аналізом вмісту. Перший спосіб дозволяє уникнути похибок , натомість вимагає попередньої класифікації документів, впровадження міток, збору сигнатур тощо. Пропуски конфіденційної інформації при цьому методі цілком імовірні, якщо конфіденційний документ не зазнав попередньої класифікації. Другий спосіб дає помилкові спрацьовування, проте дозволяє виявити пересилку конфіденційної інформації не тільки серед документів під грифом. У добрих DLP-системах обидва способи поєднуються.

До складу DLP-систем входять компоненти (модулі) мережевого рівня і компоненти рівня хосту. Мережеві компоненти контролюють трафік, що перетинає межі інформаційної системи. Зазвичай вони стоять на проксі-серверах, серверах електронної пошти, а також у вигляді окремих серверів. Компоненти рівня хосту стоять зазвичай на персональних комп'ютерах працівників і контролюють такі канали, як запис інформації на компакт-диски, флеш-накопичувачі тощо. Хостові компоненти також намагаються відстежувати зміни мережевих налаштувань, інсталяцію програм для тунелювання стеганографії та інші можливі методи для обходу контролю. DLP-система повинна мати компоненти обох зазначених типів плюс модуль для централізованого управління.

Крім основного, перед DLP-системою можуть стояти і вторинні (побічні) завдання. Вони такі:

1) архівування повідомлень, які пересилаються, на випадок можливих у майбутньому розслідувань інцидентів;

2) запобігання передачі зовні не тільки конфіденційної, але й іншої небажаної інформації (образливих повідомлень, спаму, еротики, зайвих обсягів даних тощо);

3) запобігання передачі небажаної інформації не тільки зсередини назовні, але й ззовні всередину інформаційної системи;

4) запобігання використанню працівниками державних інформаційних ресурсів в особистих цілях;

5) оптимізація завантаження каналів, економія трафіку;

6) контроль присутності працівників на робочому місці;

7) відстеження лояльності співробітників, їх політичних поглядів, переконань, збір компромату.

1.3 Основні функції DLP-систем

Основні функції DLP-систем візуалізовані на малюнку нижче (рис.1)

- контроль передачі інформації через Інтернет з використанням E-Mail, HTTP, HTTPS, FTP, Skypeі інших додатків і протоколів;
- контроль збереження інформації на зовнішні носії - CD, DVD, flash, мобільні телефони і т.п .;
- 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 і файлових серверах за ключовими словами, мітках документів, атрибутам файлів і цифровим відбитками
- запобігання витокам інформації шляхом контролю життєвого циклу і руху конфіденційних відомостей.

Рисунок 1.1 – Основні функції DLP систем

Захист конфіденційної інформації в DLP-системі здійснюється на трьох рівнях:

1 рівень - Data-in-Motion - дані, що передаються по мережевим каналам:

- web (HTTP/HTTPS протоколы);
- служби миттєвого обміну повідомленнями (QIP, Skype, MSN и т.д.);
- корпоративна і особиста пошта (POP, SMTP, IMAP и т.д.);
- бездротові системи (WiFi, Bluetooth, 3\4\5G и т.д.);
- ftp - з'єднання.

2 рівень - Data-at-Rest - дані, статично зберігаються на:

- серверах;
- робочих станціях;
- ноутбуках;
- системах зберігання даних.

3 рівень - Data-in-Use - дані, що використовуються на робочих станціях.

Система класу DLP включає в себе наступні компоненти:

- центр управління та моніторингу;
- мережевий шлюз DLP, що встановлюється на Інтернет-периметр.
- агенти на робочих станціях користувачів;

У DLP-системах конфіденційна інформація може визначатися по ряду різних ознак, а також різними способами, основними з них є:

- морфологічний аналіз інформації;
- статистичний аналіз інформації;
- регулярні вирази (шаблони);
- метод цифрових відбитків;
- метод цифрових міток.

Впровадження DLP-систем давно стало вже не просто модою, а необхідністю, адже витік конфіденційних даних може привести до величезного збитку для компанії, а головне надати не одномоментна, а тривалий вплив на бізнес компанії. При цьому збиток може носити не тільки прямий, але й непрямий

характер. Тому що крім основного збитку, особливо в разі розголошення відомостей про інцидент, Ваша компанія «втрачає обличчя». Збиток від втрати репутації оцінити в грошах вельми і вельми складно! А адже кінцевою метою створення системи забезпечення безпеки інформаційних технологій, є запобігання або мінімізація збитку (прямого або непрямого, матеріального, морального чи іншого), що наноситься суб'єктам інформаційних відносин за допомогою небажаного впливу на інформацію, її носії та процеси обробки.

1.4 Методи аналізу потоків даних для DLP

Завдання аналізу потоку даних з метою виявлення конфіденційної інформації можна сміливо назвати нетривіальною. Оскільки пошук потрібних даних ускладнений безліччю факторів, що вимагають обліку. Тому, на сьогоднішній день розроблено декілька технологій для детектування спроб передачі конфіденційних даних. Кожна з них відрізняється від інших своїм принципом роботи.

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

Морфологічний аналіз

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

Головною перевагою даного методу 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 Skype, соціальних мережах, а з іншого - з його допомогою можуть аналізуватися будь-які тексти і відслідковуватися будь-яка інформація.

При цьому конфіденційні документи не потребують будь-якої попередньої обробки. А захист починає діяти відразу після включення правил обробки і поширюється на всі задані канали зв'язку.

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

Статистичний аналіз

Принцип роботи статистичних методів полягає в імовірнісному аналізі тексту, який дозволяє припустити його конфіденційність або відкритість. Для їх роботи зазвичай потрібне попереднє навчання алгоритму. В ході нього обчислюється ймовірність знаходження тих чи інших слів, а також словосполучень в конфіденційних документах.

Перевагою статистичного аналізу є його універсальність. При цьому варто відзначити, що дана технологія працює в штатному режимі тільки в рамках підтримки постійного навчання алгоритму. Так, наприклад, якщо в процесі навчання системі було запропоновано недостатня кількість договорів, то вона не зможе визначати факт їх передачі. Тобто якість роботи статистичного аналізу залежить від коректності його налаштування. При цьому необхідно враховувати імовірнісний характер даної технології.

Регулярні вирази (шаблони)

Принцип роботи статистичних методів полягає в імовірнісному аналізі тексту, який дозволяє припустити його конфіденційність або відкритість. Для їх роботи зазвичай потрібне попереднє навчання алгоритму. В ході нього обчислюється ймовірність знаходження тих чи інших слів, а також словосполучень в конфіденційних документах.

Перевагою статистичного аналізу є його універсальність. При цьому варто відзначити, що дана технологія працює в штатному режимі тільки в рамках підтримки постійного навчання алгоритму. Так, наприклад, якщо в процесі

навчання системі було запропоновано недостатня кількість договорів, то вона не зможе визначати факт їх передачі. Тобто якість роботи статистичного аналізу залежить від коректності його налаштування. При цьому необхідно враховувати імовірнісний характер даної технології.

Цифрові відбитки

Під цифровим відбитком в даному випадку розуміється цілий набір характерних елементів документа, за яким його можна з високою вірогідністю визначити в майбутньому. Сучасні DLP-рішення здатні детектувати не тільки цілі файли, але і їх фрагменти. При цьому можна навіть розрахувати ступінь відповідності. Такі рішення дозволяють створювати диференційовані правила, в яких описані різні дії для різних відсотків збігу.

Важливою особливістю цифрових відбитків є те, що вони можуть використовуватися не тільки для текстових, але і для табличних документів, а також для зображень. Це відкриває широке поле для застосування даної технології.

Цифрові мітки

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

До недоліків даної технології відноситься, в першу чергу, обмеженість сфери її застосування. Захистити з її допомогою можна тільки текстові документи, причому вже існуючі. На новостворювані документи це не поширюється. Частково цей недолік нівелюється способами автоматичного створення міток, наприклад, на основі набору ключових слів. Однак даний аспект зводить технологію цифрових міток до технології морфологічного аналізу, тобто, по суті, до дублювання технологій.

Іншим недоліком технології цифрових міток є легкість її обходу. Досить вручну набрати текст документа в листі (НЕ скопіювати через буфер обміну, а саме набрати), і даний спосіб буде безсилий. Тому він гарний тільки в поєднанні з іншими методами захисту.

Наведемо декілька прикладів нижче на рисунках 1.2 та 1.3:

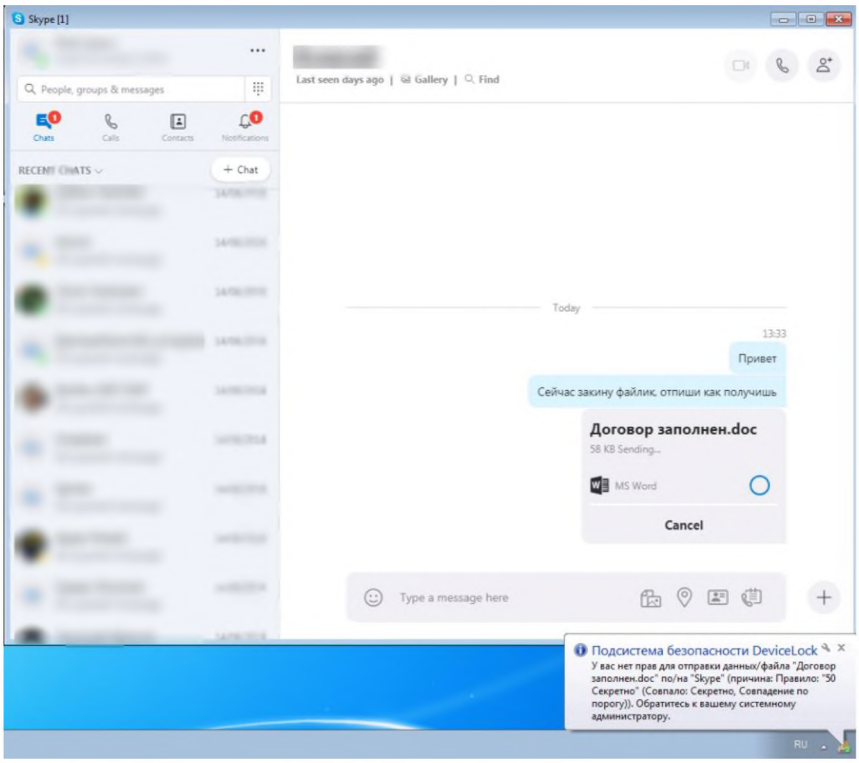

Рисунок 1.2 - Метод регулярних виразів

Рисунок 1.3 - Метод морфологічний аналізу

1.5 Порівняння систем

Для аналізу обрали найбільш актуальні системи протидії витоку інформації для малого та середнього бізнесу, а саме McAfee, DeviceLock DLP, Falcongaze SecureTower.

Перша система DeviceLock DLP.

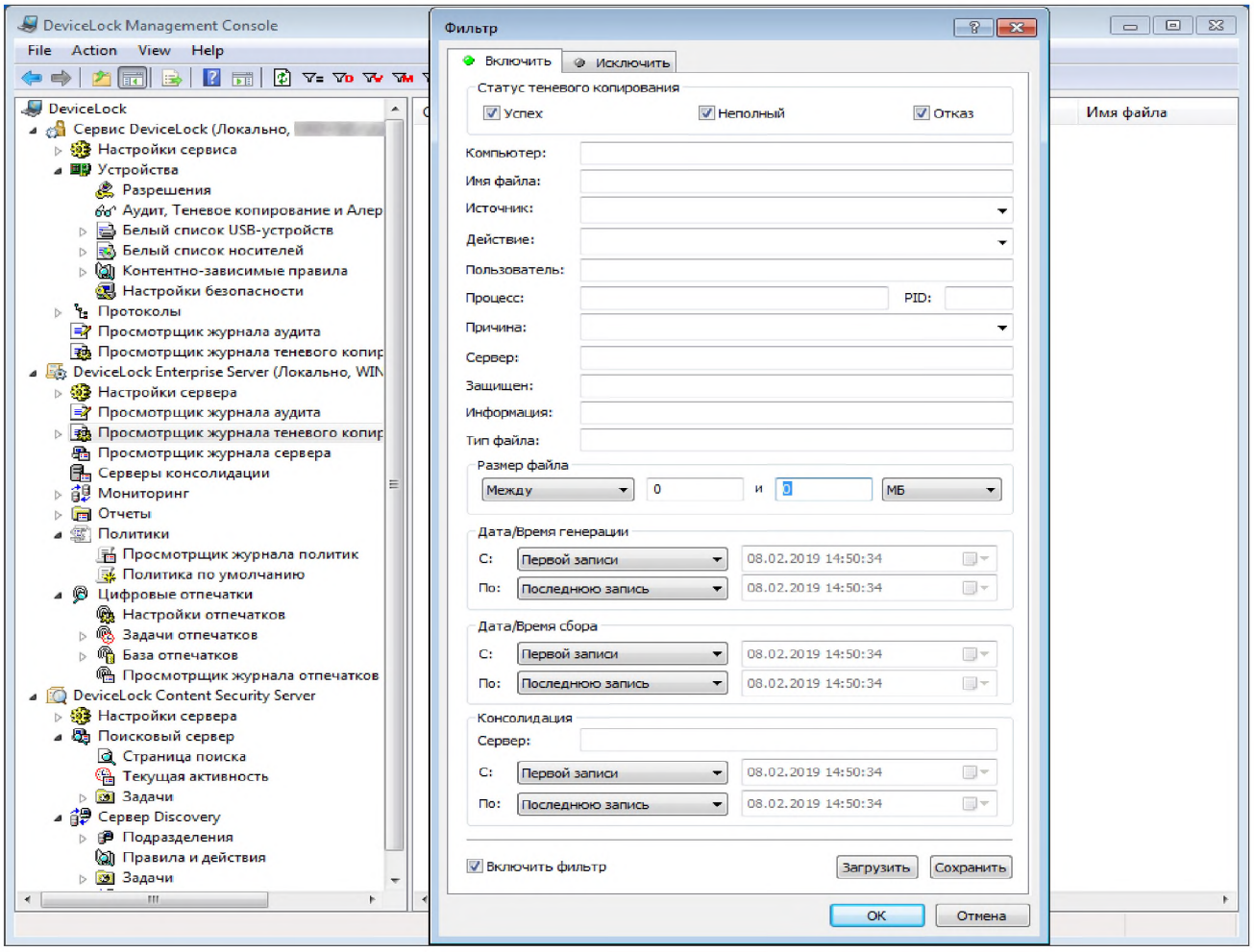

Рисунок 1.4. - DeviceLock DLP для Windows інтерфейс системи

На рисунку 1.4 зображено інтерфейс хостової системи DeviceLock DLP для Windows. На тести була обрана версія 8. Переваги: деталізація в налаштуваннях контролів. Агенти абсолютно незалежні по відношенню до серверної частини, можуть жити власним життям, скільки буде потрібно. Зроблено автоматичне перемикання режимів - можна сміливо відпускати співробітника з ноутбуком, політики переключаться самі на інші налаштування. Блокування і моніторинг в системі розведені на рівні консолі - немає ніякої складності для якихось каналів включити заборону для окремих користувачів, а іншим користувачам задати налаштування тільки для моніторингу. Також самостійними виглядають правила аналізу вмісту і працюють як на заборону, так і навпаки на дозвіл передачі при закритому в принципі каналі.

Друга система McAfee.

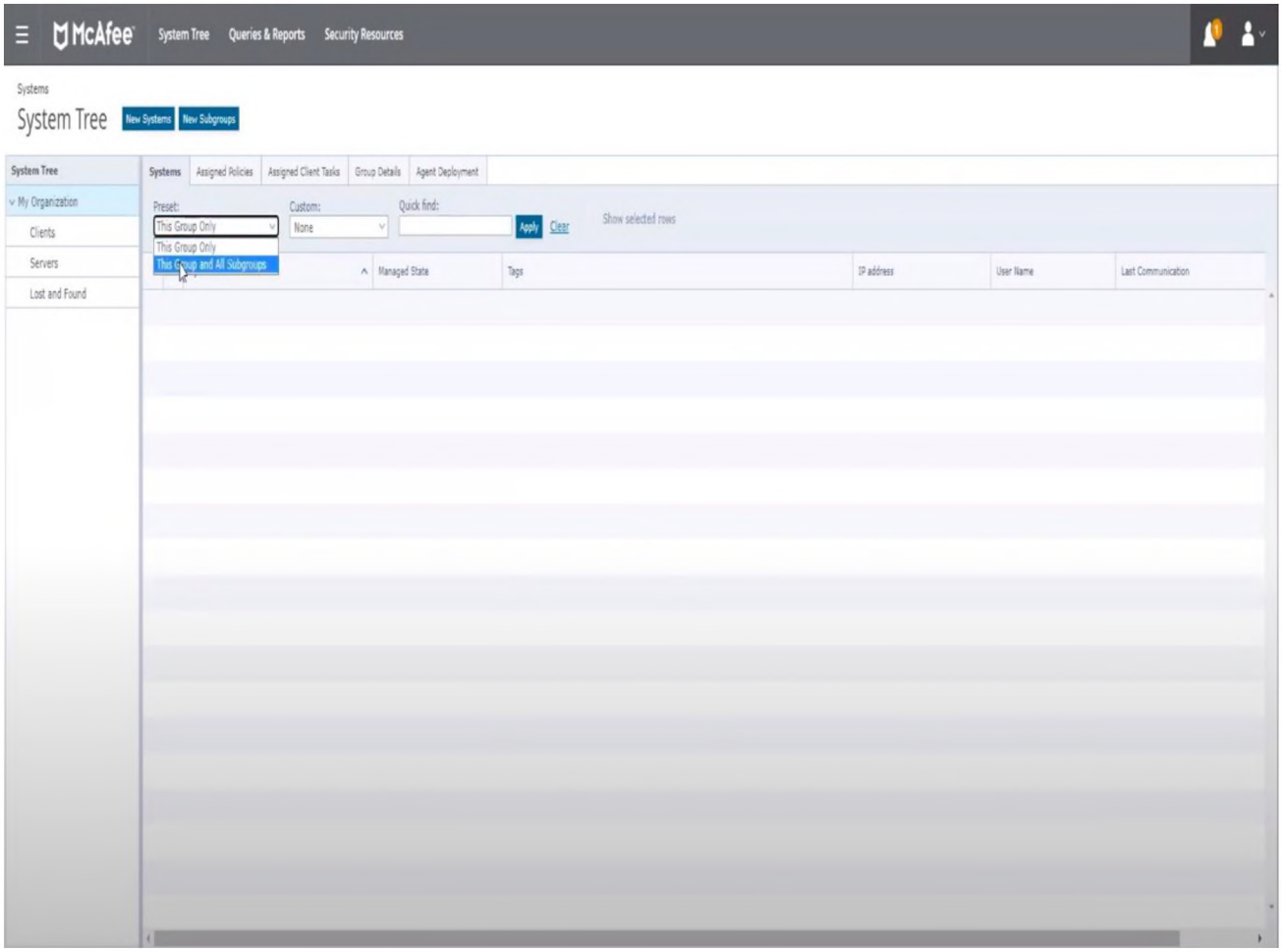

Рисунок 1.5. - McAfee інтерфейс системи

На тестах була шлюзова версія McAfee Data Loss Prevention 10.0.100 (Рис. 1.5).

Відзначимо , що ця система важка і в установці, і в налаштуванні. Щоб її завантажити і використовувати, треба спочатку розгорнути McAfee ePolicy Orchestrator як власну платформу управління. Відзначимо те , що є призначена для користувача документація вельми продумана і описує весь порядок установки, а інсталятор сам ставить всі необхідні йому зовнішні компоненти.

Переваги: можливість задати умовні пріоритети для правил, а потім використовувати ці пріоритети як параметри фільтрації подій в журналі. Сама фільтрація зроблена вельми приємно і зручно. Можливість дати користувачеві переслати файл при заборону, якщо надасть якесь пояснення (user-justification).

Третя система Falcongaze SecureTower.

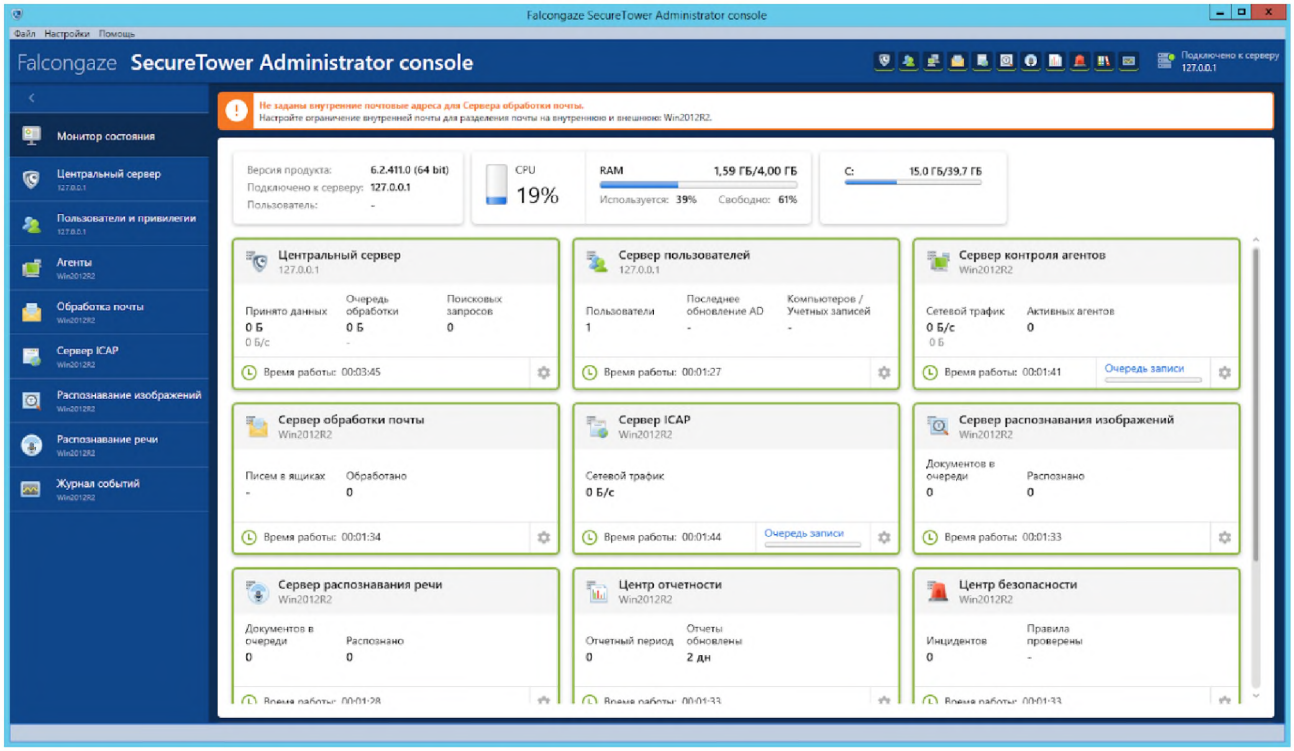

Рисунок 1. 6. - SecureTower інтерфейс системи

На тести обрали шлюзову DLP систему Falcongaze (Рис. 1.6). Перехоплення тут - для моніторингу, тобто створюється тіньова копія, про блокування мови практично не йде (крім HTTP, SMTP і MAPI). Є створення скріншотів з робочих станцій і деякі інші функції моніторингу активності користувачів.

Переваги: дружній призначений для користувача інтерфейс. Все зроблено для зручності роботи. Інструмент перегляду та аналізу архіву, вдало реалізований граф зв'язків. Практично з будь-якого звіту можна перейти до зазначеного там події (інциденту). Інцидентів можна призначати категорії (досліджені, не досліджені, відкладені). Моніторинг Телеграма та Viber'a (що в наш час є дуже актуальним).

Перевірялися системи в основному на :

- запис на флешку;
- друк документів на принтері (локальний по USB і мережевий);
- відправка на SMTP і MAPI;

- відправка на вебпочту (дивилися Gmail);
- відправка в соцмережі (дивилися Facebook);
- заливка в хмари (дивилися Dropbox);
- відправка файлів через форми по HTTP;
- заливка на FTP сервер;
- месенджери: чат, відправка файлу, спілкування голосом або по відео (дивилися Skype, Whatsapp, Telegram);
- контроль в термінальній сесії (чи спрацьовування при висмикування документа з буфера обміну в термінальній сесії і при запису на диск, перекинутий з віддаленого робочого місця в термінальну сесію).

Результати базових тестів зводилися в таблицю №1.1 для порівняння.

Таблиця 1.1- Результати базових тестів

Назва	McAfee	DeviceLock DLP	Falcongaze SecureTower
Блокування для мережевих каналів	Добре , через контроль додатків	ТАК, повністю на агенті	Недостатньо
SMTP	ТАК, для певних поштових клієнтів	ТАК	ТАК
MAPI	Обмеження	ТАК	ТАК
Вебпошта	ТАК, для певних браузерів	ТАК	НІ
Gmail.com	ТАК,треба задати категорію	ТАК	НІ
Соц. мережі	ТАК, для певних браузерів	ТАК	НІ
Facebook	ТАК,треба задати категорію	ТАК	НІ
Хмарні сховища	ТАК	ТАК	Тільки через засоби синхронізації
DropBox	ТАК	ТАК	ТАК

Продовження таблиці 1.1

Назва	McAfee	DeviceLock DLP	Falcongaze SecureTower
HTTP	ТАК, для певних браузерів	ТАК	ТАК
Доступ	ТАК	ТАК	ТАК
Відправка файлів	ТАК	ТАК	ТАК
FTP	НІ	ТАК	ТАК
Доступ	НІ	ТАК	ТАК
Відправка файлів	НІ	ТАК	ТАК
Skype	Тільки файли	ТАК	НІ
Чат	НІ	ТАК	НІ
Відправка файлів	ТАК	ТАК	НІ
Аудіозаписи	НІ	ТАК	НІ
WhatsApp	НІ	Тільки заборона месенджеру	НІ
Чат	НІ	НІ	НІ
Відправка файлів	НІ	НІ	НІ
Аудіозаписи	НІ	НІ	НІ
Telegram	НІ	Тільки заборона месенджеру	НІ
Чат	НІ	НІ	НІ
Відправка файлів	НІ	НІ	НІ
Аудіозаписи	НІ	НІ	НІ
Блокування для пристроїв	ТАК	ТАК	Частково
Флешка	ТАК	ТАК	ТАК
Мережевий принтер	ТАК	ТАК	НІ
Локальний USB принтер	ТАК	ТАК	НІ
Блокування в термінальній сесії Citrix	Тільки для певних поштових клієнтів та браузерів (ТАК)	На тіньової копії для WhatsApp (ТАК)	ТАК

Продовження таблиці 1.1

Назва	McAfee	DeviceLock DLP	Falcongaze SecureTower
Тіньові копії	ТАК Для мережевих каналів:тільки для певних поштових клієнтів та браузерів	ТАК Немає запису дзвінків в мессенджерах, немає тіньової копії для WhatsApp	ТАК
Флешка	ТАК	ТАК	ТАК
Мережевий принтер	ТАК	ТАК	ТАК
Локальний USB принтер	ТАК	ТАК	ТАК
SMTP	ТАК, для певних поштових клієнтів	ТАК	ТАК
MAPI	ТАК	ТАК	ТАК
Вебпошта	ТАК, для певних поштових клієнтів	ТАК	ТАК
Соц. мережі	ТАК, для певних браузерів	ТАК	ТАК
Хмарні сховища	Частково	ТАК	ТАК
Яндекс Диск	НІ	ТАК	ТАК
DropBox	ТАК	ТАК	ТАК
HTTP	ТАК, для певних браузерів	ТАК	ТАК
FTP	НІ	ТАК	ТАК
Skype	НІ	ТАК немає запису аудіо	ТАК
Відправка файлів	НІ	ТАК	ТАК
Чат	НІ	ТАК	ТАК
Аудіозаписи	НІ	НІ	ТАК
WhatsApp	НІ	НІ	ТАК
Чат	НІ	ТАК	ТАК
Відправка файлів	НІ	НІ	ТАК
Аудіозаписи	НІ	НІ	ТАК

Продовження таблиці 1.1

Назва	McAfee	DeviceLock DLP	Falcongaze SecureTower
Telegram	НІ	ТАК немає запису аудіо	ТАК
Чат	НІ	ТАК	ТАК
Відправка файлів	НІ	ТАК	ТАК
Аудіозаписи	НІ	НІ, проте показує факт дзівнка	НІ

В таблицю №1.2 ми внесемо загальні параметри , при роботі з DLP системою, їх кошторис та оцінемо зручність при використанні.

Таблиця 1.2 - Загальні параметри DLP

	McAfee	DeviceLock DLP	Falcongaze SecureTower
Інтерфейс	Вузькоспеціалізована система - специфічна	Складний	Дуже зручний
Можливість отримання демо-версії для тестування всередині організації	Частково	ні	Так , 1 місяць
Ролі	Адміністратор системи	Будь-яка кількість	Адміністратор системи, офіцер безпеки
Лінгвістичний аналіз	ТАК	ТАК	ТАК
Аналіз за словником	ТАК	ТАК	ТАК
Режими сповіщень	Консоль, пошта	Консоль, пошта, графіки	Консоль, пошта, графіки

Продовження таблиці 1.2

	McAfee	DeviceLock DLP	Falcongaze SecureTower
Запис звітів в локальне сховище в разі недоступності сервера	ТАК , в про версії	ТАК	ТАК
Можливість тестування продукту на серверах розробника	НІ	ТАК	На сервері дистриб'ютора
Ціна	32 000грн	40 000грн	55 000грн

1.6 Діяльність та опис організації

Ефективність DLP систем будемо перевіряти на основі вже існуючої мережі компанії «TravelTeam», яка на ринку вже понад 3-х років. Компанія займається продажем сформованих туроператором турів по найбільш вигідним цінам для клієнта. Наразі вже нараховують більше 1000-чі клієнтів. Тому постає питання, щодо захисту інформації своїх клієнтів та репутації. Робота офіційна , тому кожний працівник ознайомився та підписав «положення про конфіденційну інформацію та комерційну таємницю».

У таблицю 1.3 для ознайомлення внесено апаратне обладнання та його характеристики , що використовується працівниками. А також самих працівників , що працюють в організації у таблицю 1.4.

Таблиця 1.3 - Апаратне обладнання , що використовується

Обладнання	Характеристика	Кількість
Wi-fi роутер (TP-Link Archer AX10)	802.11 g/n/ac/ax (WiFi 6) AX1500	1

Продовження таблиці 1.3

Обладнання	Характеристика	Кількість
Коммутатор локальної мережі (Switch) TP-Link TL-SG1008D	Комутатор локальної мережі (Switch) IEEE 802.3 IEEE 802.3u IEEE 802.3ab IEEE 802.3x	1
Монітор Samsung S22F350FHI	Full HD (1920x1080) 60 Гц TN матриця діагональ 21,5	30
Миша дротова Esperanza EM102S	800 dpi Дротова	30
Клавіатура дротова Ergo K-230USB	USB	30
ПК (1-30)	Виробник процесора: Intel. Модель центрального процесора: Core i5-9400F Кількість ядер: 6 ядер Частота центрального процесора: 2,9 (4,1) ГГц	30

Таблиця 1.4 - Відомості про персонал

Вид діяльності	Доступ до ПК	Рівень обізнаності	Кількість осіб
Прибиральниця	Не має	Недостатньо	2
Користувач (оператор)	Має тільки за своїм обліковим записом	Достатньо	25
Адміністратор ІТС	Має	Дуже добре	3
Наймані працівники (техніки ІТС)	Не має	Достатньо	2
Супервайзер	Має	Достатньо	3
Директор	Має	Достатньо	1

Персонал, а саме оператори повинні працювати з клієнтами на робочих ПК. Супервайзери допомагають операторам та стежать за виконанням плану, а також роблять звіти для директора. За технічними питаннями на базовому рівні стежать адміністратори. Прибиральці(ки) повинні стежити за чистотою в офісі , не мають права дивитись або користуватися робочими ПК.

Компанія займається продажем турів, а отже допомагає туристу вибрати і придбати відповідний тур. Для цього встановлені спеціальні програми на ПК співробітників, а саме CRM Columbis, Sender та cisco Jabber. Сервіс Columbis дозволяє менеджерам турагенств вести базу клієнтів в CRM, швидко обробляти заявки клієнтів, підбирати і бронювати тури, роздруковувати путівки, договору, контролювати стадії відправки і відпочинку клієнта. А керівник бачить перед собою повну картину діяльності туристичної компанії. Для зв'язку з клієнтами в чаті , було розроблено та встановлено Sender, який запрограмований отримувати та відсилати смс повідомлення клієнтам з найпопулярніших месенджерів , а саме Telegram, Viber, Whats App, Facebook messenger. А також зручний програмний комплекс cisco Jabber для телефонії, дана технологія використовує протокол передачі даних XMPP, тому ніяких проблем з обміном даних немає, хоч би яким клієнтським додатком не користувався абонент.

Таблиця 1.5 – Програмне забезпечення

Назва програмного забезпечення	Характеристика та можливості	ПК користувача	ПК адміністратора
Windows 10 Home (Ліцензійна версія)	• Вбудовані функції безпеки, серед яких захист за допомогою антивірусу, брандмауера та захист в Інтернеті • Щоб швидко та безпечно розблоковувати ПК без пароля, відскануйте своє обличчя або відбитки пальців за допомогою Windows Hello.*	+	+

Продовження таблиці 1.5

Назва програмного забезпечення	Характеристика та можливості	ПК користувача	ПК адміністратора
Columbis CRM	Ведення бази Заявок і Клієнтів Робота з Потенційними Клієнтами Нагадування Менеджерам по термінах і оплатах	+	-
Sender	Обмін текстовими повідомленнями Унікальні смайли і стікери. Шифровані групові та p2p чати. Канал комунікації клієнта і компанії Мультифункціональні роботи і бот-платформа	+	-
ESET NOD32	Ліцензійна версія Виробник «Словакія»	+	+
Nmap (Network Mapper)	Сканер безпеки, який використовується для виявлення хостів та сервісів в комп'ютерній мережі, який створює таким чином «карту» мережі.	-	+
cisco Jabber	Клієнт, що підтримує відео та аудіо дзвінки, сервіси відправки коротких повідомлень, корпоративні та персональні адресні книги з відображенням "присутності" абонента, управління настільним телефоном(CTI),відображення повідомлень голосової пошти (Visual voice mail).	+	-

Організація використовує мережу без додаткових файрволів, а отже співробітники мають прямий доступ до Інтернету. Використовується інтернет від компанії «СоюзТелеком», який підключається через мережевий протокол PPPoE через оптоволоконний кабель, та має швидкість передавання даних 100 Мбіт/сек. Схематично зображена мережа на рисунку № 1.7

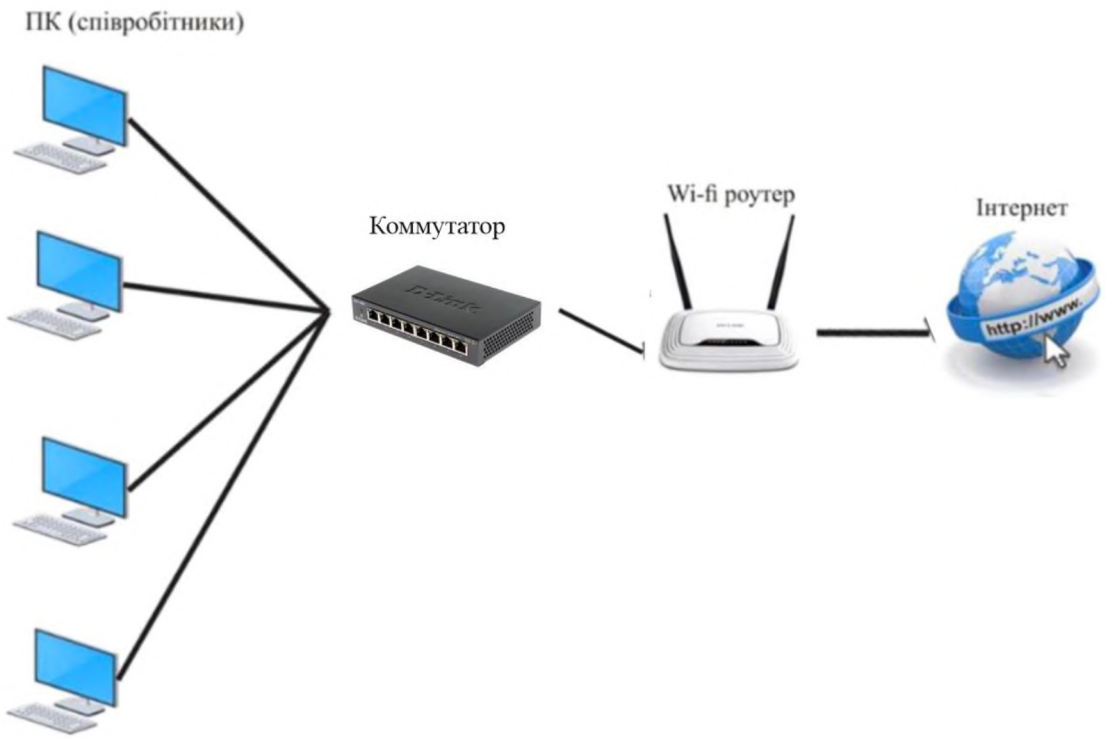

Рисунок 1.7 - Зображення мережі в компанії до інсталяції DLP системи.

1.7 Висновок

Сьогодні системи DLP широко застосовуються для захисту від витоку інформації, які з розвитком інформаційних технологій трапляються все частіше. Є багато рішень, які різняться ціною і функціоналом. Компанії обирають системи залежно від своїх потреб і можливостей.

Системи DLP не забезпечують цілковитий захист інформації в мережі, на яку направлені. Інформація може поширюватися за межі компанії навмисно або ненавмисно, це можуть бути співробітники компанії, які за своєю необережністю

втрачають контроль над даними за межами компанії, співробітники, які хочуть свідомо спричинити шкоди компанії або працівники компанії-конкурента, проникаючи в компанію під виглядом нового працівника вивідують необхідну для них інформацію

Задача цієї роботи полягає в наступних діях:

- тестування і аналіз роботи існуючих DLP систем;
- ознайомлення з існуючими проблемами системи та шляхами, через які можуть відбуватися витоки інформації;
- пошук найкращого рішення;

Практично у всіх країнах охороняється законом право на таємницю зв'язку і право на таємницю приватного життя (приватність, privacy). Використання DLP-систем може суперечити місцевим законам в деяких режимах або вимагати особливого оформлення відносин між працівниками і роботодавцем. Тому при впровадженні DLP-системи необхідно залучати юриста на самому ранньому етапі проектування.

РОДІЛ 2 СПЕЦІАЛЬНА ЧАСТИНА

У цьому розділі розділі розглянемо потенційні загрози, виявимо та оцінемо порушника, інсталюємо DLP систему в мережу компанії «TravelTeam» для інформаційної безпеки даних, розглянемо користь даних систем та їх актуальність у сучасному світі.

2.1 Оцінювання ризиків

Для середовища ІТС , необхідно визначити всі можливі потенційні загрози. Походження загроз може бути випадковим і навмисним.

Випадкове походження обумовлюється спонтанними і не залежними від волі людей обставинами, що виникають в ІТС в процесі її функціонування. Найбільш відомими випадковими загрозами є стихійні лиха, відмови, збої, помилки та побічні впливи.

Сутність цих загроз (окрім стихійних лих, сутність яких незрозуміла):

–відмова – порушення працездатності системи, що призводить до неможливості виконання нею основних своїх функцій;

– збій – тимчасове порушення працездатності системи, наслідком чого може бути неправильне виконання у цей момент своїх функцій;

–помилка – неправильне виконання системою своїх функцій, що відбувається внаслідок її специфічного стану;

Навмисне походження загроз обумовлюється зловмисними діями співробітників.

Передумови появи таких загроз можуть бути об'єктивними та суб'єктивними. Об'єктивні передумови можуть бути спричинені кількісною або якісною недостатністю елементів системи тощо. До суб'єктивних передумов відносяться різновиди людської діяльності: розвідка (агенти конкурентів), злочинні дії, неякісна робота персоналу ІТС.

В даному випадку джерело загрози – співробітники компанії , які навмисно або випадково можуть завдати шкоди інформації , яка обробляється ІТС. Спираючись на обране джерело загроз, визначаємо кількість загроз, потенційно

можливих у сучасних ІТС. При цьому врахуємо не лише всі відомі загрози, але й ті загрози, що раніше не виявлялися, але потенційно можуть виникнути. В даному випадку акцентується увага на антропогених загрозох.

Модель загроз визначає:

– перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);

– перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об’єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

Загрози для інформації, що обробляється в ІТС, залежать від характеристик ОС, апаратного складу, програмних засобів, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу.

Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у моделі загроз, наприклад:

– зміна умов фізичного середовища (стихійні лиха і аварії,пожежа або інші випадкові події);

– збої та відмови у роботі технічних або програмних засобів ІТС;

– наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);

– помилки персоналу (користувачів) ІТС під час експлуатації;

– навмисні дії (спроби) потенційних порушників.

Випадкові загрози суб’єктивної природи – це помилкові дії персоналу по неуважності, недбалості, незнанню тощо, але без навмисного наміру.

До них відносяться:

– дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм тощо);

– ненавмисне пошкодження носіїв інформації;

– неправомірна зміна режимів роботи ІТС , ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

– неумисне зараження ПЗ комп'ютерними вірусами;

– невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;

– помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

– будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

– неправомірне впровадження та використання заборонених політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення тощо);

– наслідки некомпетентного застосування засобів захисту тощо.

Навмисні загрози суб'єктивної природи – це дії порушника, спрямовані на проникнення в систему та одержання можливості НСД до її ресурсів або дезорганізацію роботи ІТС та виведення її з ладу.

До них відносяться:

– порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

– порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, кондиціонування тощо.);

– порушення режимів функціонування ІТС (обладнання і ПЗ);

– впровадження та використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

– використання (шантаж, підкуп тощо) з корисливою метою персоналу ІТС;

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

– несанкціоноване копіювання носіїв інформації;

– читання залишкової інформації з оперативної пам'яті ЕОТ, зовнішніх накопичувачів;

– одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача;

– неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

Для кожної з загроз необхідно визначити її спрямованість, джерело, механізм реалізації та можливі наслідки.

По-перше, на порушення яких властивостей інформації або ІТС загроза спрямована:

– конфіденційності – несанкціоноване ознайомлення з інформацією;

– цілісності – несанкціонована модифікація (спотворення, фальсифікація, викривлення) інформації;

– доступності – порушення можливості використання ІТС або оброблюваної інформації (відмова в обслуговуванні користувача);

По-друге, джерела виникнення загрози (які суб'єкти ІТС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу):

– персонал і користувачі;

– технічні засоби;

– моделі, алгоритми, програми;

– технологія функціонування;

– зовнішнє середовище.

«Модель загроз» сформавана у вигляді системи таблиць (№2.1) , визначенням порушень властивостей інформації та ІТС.

Таблиця 2.1 – Загрози для ІТС

	Потенційні загрози для ІТС	Ризики для ІТС		
		К	Ц	Д
Загрози природних явищ(місто)				
1.1	Пожежа, затоплення	+	+	+
1.2	Втрата електроживлення	-	+	+
1.3	Втрата / пошкодження комунікаційних каналів	-	-	+
1.4	Перенавантаження системи	-	-	+
1.5	Збої та відмови обчислювальної техніки, програмного забезпечення	-	+	+
Порушення нормального режиму роботи				
2.1	Зараження ПК вірусами	-	+	+
2.2	Пошкодження носіїв інформації	-	-	+
2.3	Вхід у систему сторонніх осіб	+	+	+
2.4	Впровадження та доступ до ситему агентів інших компаній	+	+	+
Помилки співробітників				
3.2	Встановлення сторонніх програм , що не є необхідними для виконання обов'язків	+	+	+
3.3	Помилки адміністраторів у роботі	+	+	+
3.4	Порушення технології обробки, введення та експлуатації інформації	+	+	+

Зробимо аналіз загроз з урахуванням 3-х рівнів ризиків і збитків за 5-ти бальною шкалою. Отримаємо «Модель загроз з визначенням рівня ризиків і збитків» у вигляді 3-х таблиць в системі таблиць 2.2 (загрози конфіденційності, цілісності, доступності).

- Великий – якщо реалізація загрози надає великих збитків (5 бали);
- Середній – якщо реалізація загрози надає помірних збитків (3 бали);
- Низький – якщо реалізація загрози надає незначних збитків (1 бал).

Таблиця 2.2 - Модель загроз з визначенням рівня ризиків і збитків

	Механізм реалізації	Рівень		Сума загроз
		ризиків	збитків	
Загроза конфіденційності				
К.1	Викрадення носіїв з метою несанкціоновагого ознайомлення сторонніх осіб	3	5	8
К.1	Передавання співробітниками конфіденційної інформації стороннім особам	3	5	8
К.3	Агенти конкуруючих компаній	5	5	10
Загроза цілісності				
Ц.1	Навмисна модифікація або створення інформації персоналом ІТС на жорсткому диску або зовнішніх носіях	3	3	6
Ц.2	Прояви помилок системного ПЗ, в наслідок яких стала можливою модифікація ІзОД(інформація з обмеженим доступом)	3	3	6
Ц.3	Безпосередній доступ до інформації сторонніми особами	1	3	4
Загроза доступності				
Д.1	Помилки співробітників ІТС, які призвели до знищення інформації або доступу до неї	3	5	8
Д.2	Помилки системного ПЗ ІТС, які призвели до знищення інформації або доступу до неї	3	5	8
Д.3	Некоректне налагодження засобів захисту, яке призвело до втрати доступу до інформації	3	3	6

Таблиця 3 – Загальний рівень ризиків

№	Види загроз	1	2	3	Сума загроз
1	Конфіденційності	8	8	10	26
2	Цілісності	6	6	4	16
3	Доступності	8	8	6	22

Порушення конфіденційності інформації співробітниками (топ-менеджерами напрямків) шляхом несанкціонованого копіювання на зовнішні носії, передавання конфіденційної інформації через месенджери або ftp. Це можливо із-за відсутності обліку та контролю, відсутності протоколювання роботи зі змінними носіями або діями співробітників . Це може привести до значних фінансових втрат, а також зіпсувати репутацію. Саме ці проблеми розглядаються, а також аналізуються для впровадження системи контролю DLP.

2.2 Модель порушника

Порушниками називають осіб, які реалізують загрози. Порушник – фізична особа (у загальному випадку не обов'язково користувач системи), яка здійснює порушення політики безпеки системи. Існують терміни «порушник» та «зловмисник». Останній термін підкреслює умисність порушення, тоді як у загальному випадку порушник може здійснювати порушення неумисно (наприклад, через необережність або недостатню обізнаність).
В першу чергу розглянемо модель порушника –абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо. В нашому випадку порушник розглядається, як особа, яка має доступ до роботи з включеними до складу ІТС засобами.

Метою порушника можуть бути:

– отримання конфіденційної інформації для конкуруючих компанії;

– отримання необхідної інформації у потрібному обсязі та асортименті;

– мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами;

– нанесення збитків компанії шляхом знищення матеріальних та інформаційних цінностей.

Існує три типи засобів отримання інформації: людина, апаратура, програма. В нашому випадку ми розглядаємо загрози з боку людини - розкрадання носіїв, читання та запис інформації з екрану, читання інформації з роздруківок , збереження та передавання конфіденційних даних.

В компанії «TravelTeam» працюють 2 прибиральниця , 3 адміністратори , 2 техніки , 25 операторів , 3 супервайзера та 1 директор. Доступ до ЕОТ операторів мають лише самі оператори (в кожного діє свій обліковий запис , захищений паролем) та у адміністратора. До ПК адміністратора має доступ лише сам адміністратор та директор.

Модель порушників можна відобразити на таблицях №2.1.1-2.1.6

Для побудови моделі використовуються усі можливі категорії, ознаки та характеристики порушників для більш точного їх аналізу, причому рівень загрози кожної з них оцінюється за 5-бальною шкалою.

Таблиця 2.1.1 - Модель порушника

Таблиця 1. Категорії порушників , визначених у моделі		
Позначення	Визначення категорії	Рівень загроз (1-5)
Внутрішні по відношенню до ІТС		
ВП1	Технічний персонал, який обслуговує приміщення (електрики,прибиральниці тощо)	1
ВП2	Персонал , який обслуговує технічні засоби ІТС (інженери)	3
ВП3	Користувачі ІТС (оператори)	4

Продовження таблиці 2.1

Позначення	Визначення категорії	Рівень загроз (1-5)
ВП4	Співробітники служби безпеки установи та керівники різних рівнів	5
Зовнішні по відношенню до ІТС		
ЗП1	Відвідувачі	1
ЗП2	Представники комунальних організацій (енерго-,тепло-,водопостачання тощо)	2
ЗП3	Хакери	4
ЗП4	Агенти конкурентів	5

Таблиця 2.1.2 - Модель порушника

Таблиця 2. Специфікація МП за мотивами		
Позначення	Мотив порушення	Рівень загроз (1-5)
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	4
М4	Професійний обов'язок (ЗП4)	5

Таблиця 2.1.3 - Модель порушника

Таблиця 3. Специфікація МП за рівнем кваліфікації та обізнаності щодо ІТС		
Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз (1-5)
К1	Володіє низьким рівнем знань, але вміє працювати з ПК	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	3
К3	Володіє високим рівнем знань у галузі програмування та ЕОТ	4
К4	Повністю ознайомлений зі структурою , функціями та механізмами дії організації.	5

Таблиця 2.1.4 - Модель порушника

Таблиця 4. Специфікація МП за показником можливостей використання засобів та методів подолання системи захисту		
Позначення	Характеристика можливостей порушника	Рівень загроз (1-5)
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікацій інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання, а також компактні носії інформації, які можуть бути приховано пронесені крізь охорону	4
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	5

Таблиця 2.1.5 - Модель порушника

Таблиця 5. Специфікація МП за часом дії		
Позначення	Характеристика часу дії порушника	Рівень загроз (1-5)
Ч1	Під час повної бездіяльності ІТС	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування	2
Ч3	Під час функціонування ІТС (або компонентів системи)	4
Ч4	Під час функціонування ІТС, так і під час призупинки компонентів системи	5

Таблиця 2.1.6 - Модель порушника

Таблиця 6. Специфікація МП за місцем дії		
Позначення	Характеристика місця дії порушника	Рівень загроз (1-5)
Д1	Усередині приміщень, але без доступу до засобів ІТС	1
Д2	З робочих місць операторів ІТС	3
Д3	З доступом у зону зберігання баз даних , архівів тощо	4
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	5

Після аналізу МП у таблиці, є можливість звезти у загальну таблицю №2.8 мінімальні загрози з причини безвідповідального ставлення до виконання своєї роботи та посадових обов'язків.

Таблиця 2.8 - Модель внутрішнього порушника політики безпеки інформації

Категорія порушн-ика (ВД)	Мотив порушення	Можлив-ості щодо подалання захисту	Можлив-ості за часом дії	Можлив-ості за місцем дії	Рівень обізнаності щодо ІТС	Сума загроз
Прибира-льниця	М1	З1	Ч4	Д1	К1	9
Користу-вач (оператор)	М1+(ЗП4)	З3	Ч4	Д2	К2	20
Адміністратор ІТС	М1	З3	Ч4	Д3	К4	19
Наймані працівники (техніки ІТС)	М1	З3	Ч3	Д4	К2	17
Супервайзер компанії	М1	З3	Ч4	Д2	К4	18

З фінальної таблиці ми бачимо , що найбільша загроза по відношенню до проблеми захисту , становить адміністратор ІТС та користувачі ,які майже щодня працюють з конфіденційною інформацією без контролю. У цьому випадку робота цих осіб повинна бути найбільш контрольованою, тому що вона є основним потенційним порушником безпеки інформації.

Те, що основною загрозою для безпеки інформації в ІТС є персонал ІТС, підтверджують і дані, опубліковані у 2010 році американським інститутом комп'ютерної безпеки (Сан-Франциско, штат Каліфорнія), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

– несанкціонований доступ – 2%;

– ураження вірусами – 3%;

– технічні відмови апаратури мережі – 20%;

– цілеспрямовані дії персоналу – 20%;

– помилки персоналу (недостатній рівень кваліфікації) – 55%.

Таким чином, основною потенційною загрозою для інформації в ІТС слід вважати цілеспрямовані або випадкові деструктивні дії персоналу, оскільки вони становлять 75% усіх випадків.

2.3 Профіль захищеності

Обраний профіль згідно НД-ТЗІ-2.5-005—99 (https://tzi.ua/assets/files/НД-ТЗІ-2.5-005--99.pdf):

Стандартні функціональні профілі захищеності в КС, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:

3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1,НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

КД (Довірча конфіденційність) – 2: Частково реалізовано

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. У системі офісу встановлено розмежування доступу лише до системних файлів, доступ до яких має лише локальний адміністратор робочої станції. Потрібно встановити обмеження на використання ПЗ, що не зазначене адміністратором, та закрити доступ в мережі інтернет до сервісів, що не належать до корпоративних.

КО (Повторне використання) – 1: Не Реалізовано

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

КВ (Конфіденційність при обміні) – 1: Не реалізовано

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

Файли шифруються системними засобами операційної системи Windows під час передавання їх через не захищені канали.

ЦД (Цілісність Довірча) – 1: Реалізовано

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування. Користувач може надати права на доступ до об’єктів, які обробляє користувач. (На поширені об’єкти будуть накладені права звичайного користувача, що дозволить мати доступ до них без підвищених атрибутів доступу)

ЦО– 1- Відкат: Не реалізовано

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ран жируються на підставі множини операцій, для яких забезпечується відкат.

ЦВ (Цілісність при обміні) – 1: Не реалізовано

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

Цілісність забезпечується за допомогою системних засобів операційної системи, що звіряє повноту переданої інформації за допомогою хеш-функції sha256.

ДР (Використання ресурсів) – 1: Не реалізовано

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Користувачі не мають обмеження до використання ресурсів або послуг окрім системних файлів операційної системи.

ДВ (Стійкість до відмов) – 1: Не реалізовано

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

НР (Реєстрація) – 2: Частково реалізовано

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ран жируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Повинно бути реалізовано за допомогою вбудованого системного журналу подій ОС Windows і знаходитись під контролем відповідального адміністратора.

НИ (Ідентифікація і автентифікація) – 2: Реалізовано

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ран жируються залежно від числа задіяних механізмів автентифікації. Реалізовано за допомогою облікових записів на ПК користувачів.

НК (Достовірний канал) – 1: Не реалізовано

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ран жируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін. Достовірним каналом взаємодії виступає клавіатура робочої станції.

НО (Розподіл обов-язків) – 2: Частково реалізовано

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ран жируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Користувач може нашкодити системі через доступ до використання портативних версій програм, що не встановлюються до кореневої файлової системи, але можуть на неї вплинути, наприклад через віруси, що будуть міститись у програмі.
Потрібно вдосконалити обмеження прав користувачів і заборонити можливість до скачування та запуску будь-яких програм, що не будуть дозволені адміністратором або будуть знаходитись поза кореневою директорією Windows.

НЦ (Цілісність КЗЗ) – 2: Частково реалізовано

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Влаштовано антивірус на робочих станціях (ESET NOD32 Antivirus).

НТ (Самотестування) – 2: Частково реалізовано

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ран жируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

Система має можливість до самотестування лише системних файлів, а не користувальних.

НВ (Автентифікація при обміні) – 1: Не реалізовано

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ран жируються на підставі повноти реалізації.

2.4 Впровадження DLP в мережу

На основі вже існуючої мережі, інсталюємо DLP систему.

DLP використовує мережеву архітектуру, яка поділяється на дві групи: шлюзова і хостова.

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

Хостова архітектура заснована на використанні спеціальних програм - агентів, які встановлюються на кінцевих вузлах мережі - робочих станціях, серверах додатків та ін.

Шлюзові DLP - системи засновані на використанні шлюзів - централізованих серверів обробки пересилається на них мережевого трафіку. Область використання таких рішень обмежена самим принципом їх роботи. Іншими словами, шлюзові системи дозволяють захищатися лише від витоків інформації через протоколи, використовувані в традиційних інтернет-сервісах: HTTP, FTP, POP3, SMTP та ін. При цьому контролювати те, що відбувається на кінцевих точках корпоративної мережі з їх допомогою неможливо. Даний підхід має цілу низку переваг, а саме легкість введення в експлуатацію, обслуговування і управління. Шлюз зазвичай розгортається на окремому сервері або звичайному ПК (в невеликих мережах), який може встановлюватися між робочими станціями корпоративної мережі і проксі-сервером. В цьому випадку весь мережевий трафік спочатку надходить в DLP-систему, яка може або пропустити, або заблокувати його. Пропущені пакети передаються на проксі-сервер і далі в Інтернет. Таким чином, від IT-персоналу потрібно тільки налаштувати DLP-продукт і перенаправити трафік з робочих станцій на нього. Функціональна схема шлюзового рішення, що працює в режимі блокування, представлена на рисунку №2.1.

Рисунок 2.1 - Функціональна схема шлюзового рішення, в режимі блокування

Також є варіант впровадження шлюзової DLP-системи, згідно з яким вона обробляє не прямий, а дубльований трафік. При цьому система захисту може працювати тільки в режимі моніторингу. В ній підозрілий трафік не блокується, а зберігається в журналі для подальшого його аналізу співробітниками відділу інформаційної безпеки. В цьому випадку процес впровадження виявляється ще простіше. Потрібно лише налаштувати DLP-систему і направити на нього трафік, наприклад, за допомогою керованого комутатора з портом дублювання. Функціональна схема шлюзового рішення, що працює в режимі моніторингу, представлена на рисунку №2.2.

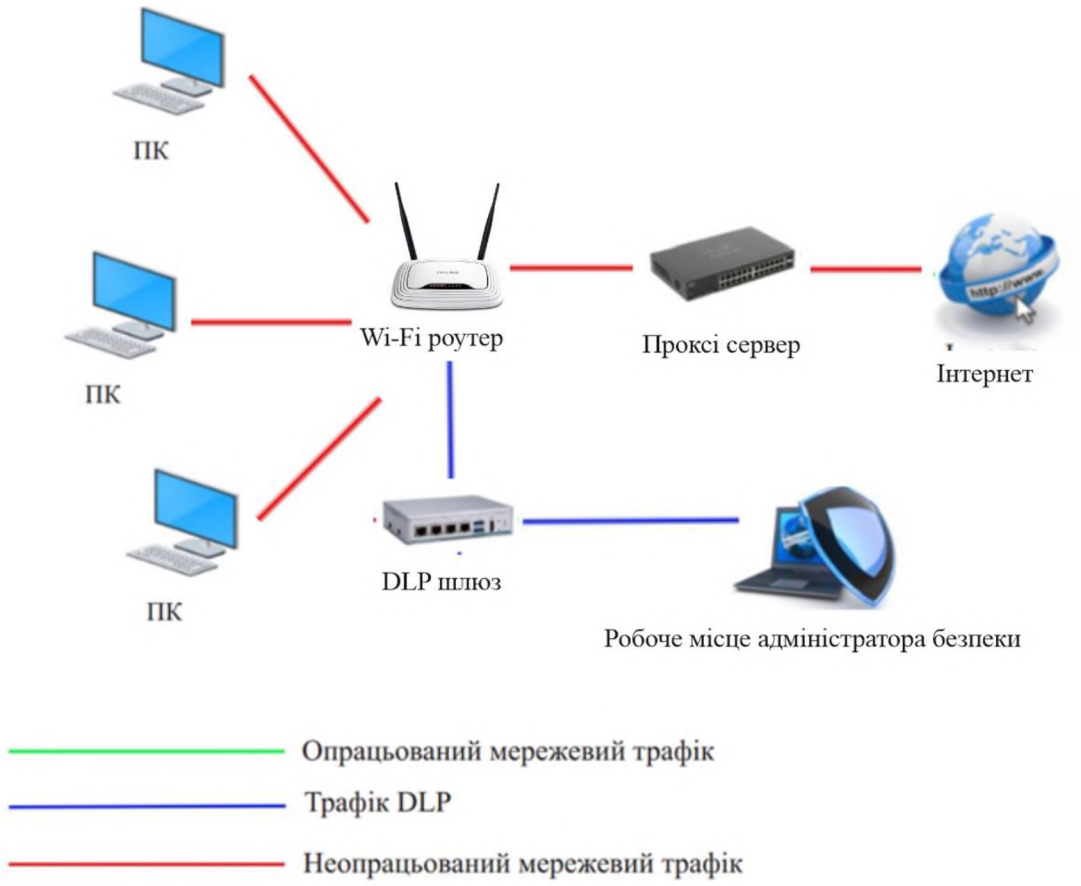

Рисунок 2.2 - Функціональна схема шлюзового рішення, що працює в режимі моніторингу.

Хостові DLP-системи засновані на використанні спеціальних агентів, які встановлюються на кінцевих точках корпоративної мережі. Ці програми грають відразу дві ролі. З одного боку вони контролюють діяльність користувачів комп'ютерів, не дозволяючи їм виходити за рамки встановленої політики безпеки (наприклад, забороняючи копіювати будь-які файли на "флешки"). А, з іншого, реєструють всі дії операторів і передають їх в централізоване сховище, дозволяючи співробітникам відділу інформаційної безпеки отримати повну картину того, що відбувається. Використання програм-агентів обмежує сферу застосування хостових DLP-систем: вони здатні бачити лише локальні або мережеві пристрої, підключені безпосередньо до тих комп'ютерів, на яких вони працюють. Функціональна схема хостового DLP-рішення представлена на рисунку№2.3

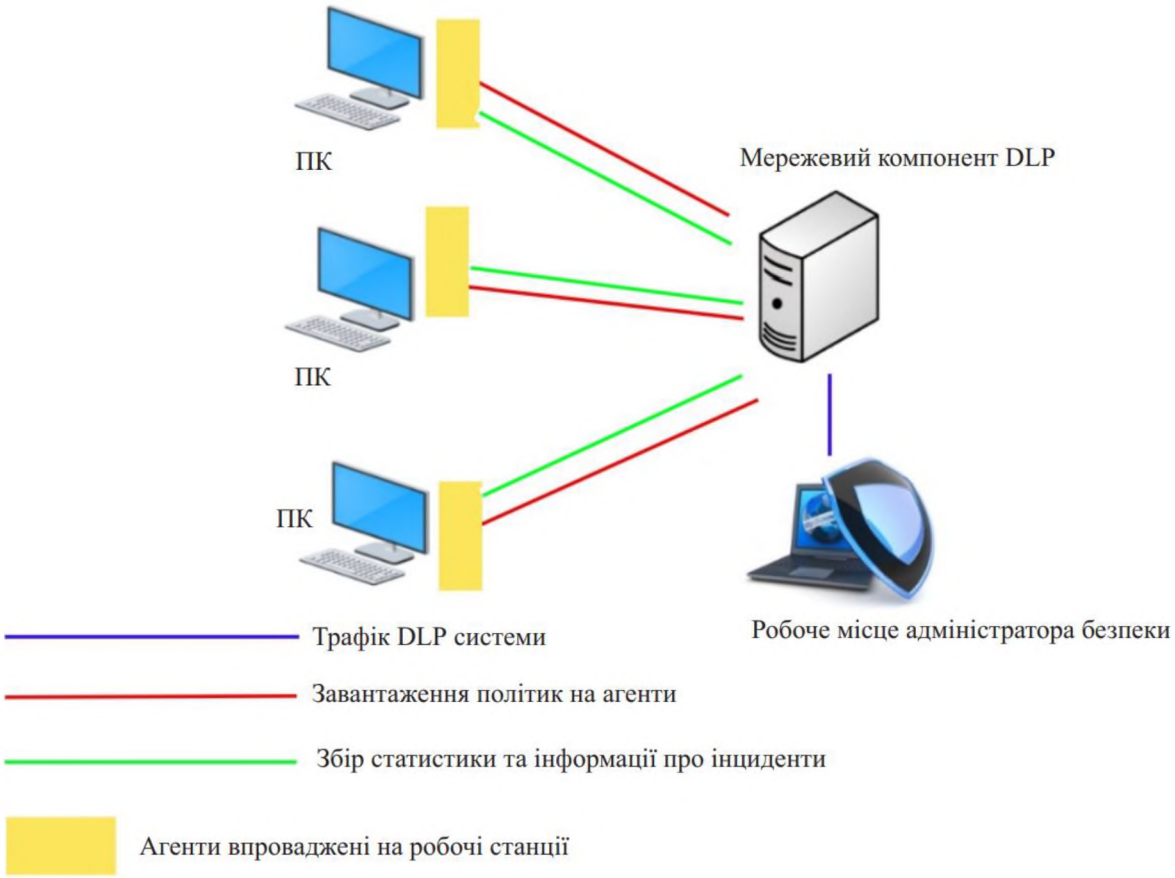

Рисунок 2.3 - Функціональна схема хостового DLP-рішення

До переваг хостових DLP-систем відносяться широкі можливості по контролю користувачів. Працюючи безпосередньо на кінцевих станціях корпоративної мережі, вони можуть не тільки контролювати «не пов'язані з роботою» канали витоку конфіденційної інформації, а й виконувати цілий набір інших функцій. Деякі розробники DLP-систем використовують цю можливість, наприклад, для виявлення випадків нецільового використання комп'ютерів працівниками. Основним недоліком хостових DLP-систем є більш складний процес впровадження в експлуатацію та подальше адміністрування. При їх розгортанні необхідно не тільки встановити і налаштувати серверний компонент, але і встановити програму-агента на кожен комп'ютер корпоративної мережі. Звичайно, обходити кожен ПК і вручну запускати на ньому дистрибутив не доведеться. Розробники DLP-систем пропонують способи автоматизованої установки агентів. Найчастіше використовуються можливості серверного

компонента або групові політики Windows. Для роботи агенти використовують політики, завантажені безпосередньо на локальні комп'ютери, на яких вони встановлені. Таким чином, при будь-якій зміні правил безпеки адміністратор повинен забезпечити їх поширення на всі кінцеві станції мережі. Здійснюється це зазвичай знову ж за допомогою серверного компонента або групових політик Windows. Також можна відзначити меншу захищеність хостових DLP-систем від несанкціонованого втручання в їх роботу з боку користувачів мережі. Працюючи на комп'ютері, до якого співробітник організації має безпосередній доступ (а часто ще й права локального адміністратора), програма-агент потенційно може бути вивантажено з пам'яті. В цьому випадку ПК випадає зі сфери контролю DLP-системи. Природно, розробники намагаються захистити свої продукти від подібного втручання. Для цього використовуються різні інструменти моніторингу завантаження та безперервності роботи всіх встановлених агентів з відправкою повідомлень адміністраторам безпеки при виникненні потенційно небезпечної ситуації. Проте, повністю виключити ризик втручання все одно не можна.

Отже для нашої мережі ми обрали хостовий спосіб системи DeviceLock DLP, тому що система виконує поставлені перед нею завдання щодо контролю співробітників , також є перевага щодо функції контролю над соціальними мережами , що в наш час є дуже необхідним, оскільки кожен користується соціальними мережами (Telegram,Viber тощо). Першим етапом було встановлення програмного забезпечення на кінцеві точки, налаштування політик відповідно до документів і посібників. Володіючи правами, отримаємо роль "шпигуна", перехоплюючи не тільки текст повідомлень, а й голосовий трафік і передаватимемо все це безпосередньо в базу DLP-системи.

За допомогою мануалів інсталюємо систему DLP на всі ПК користувачів з наданням певнив правил.

Запускаємо програму установки setup.exe і дотримуємося інструкцій на сторінках майстра установки (рисунок №2.4).

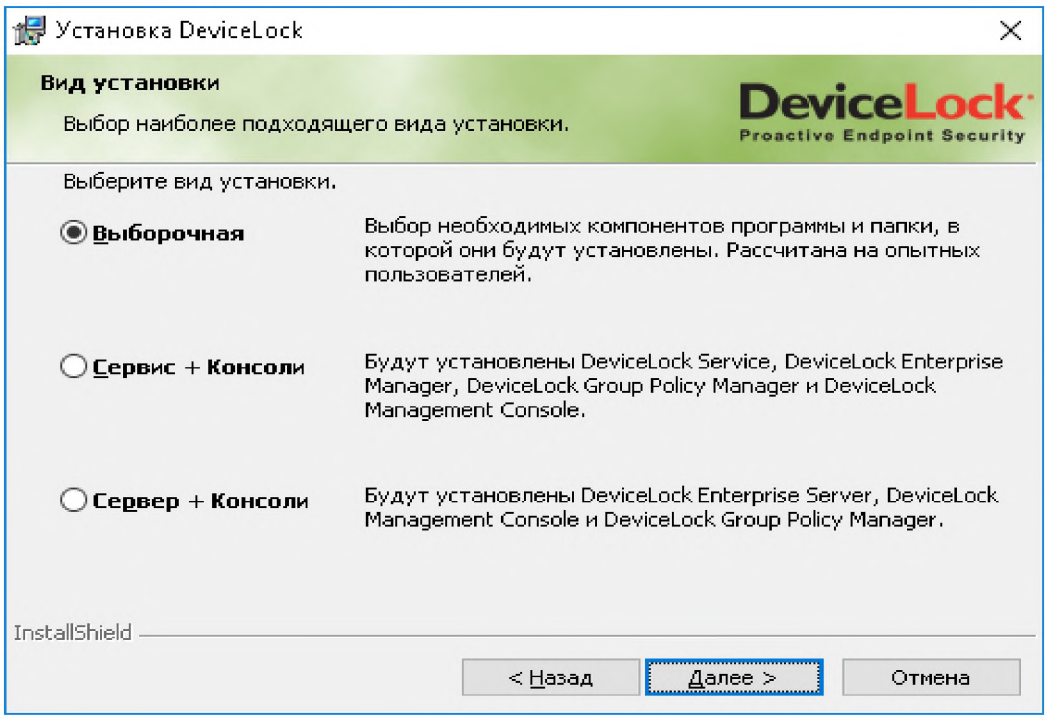

Рисунок 2.4 - Інсталяція DLP системи.

Далі на сторінці (рисунок №2.5) «Система готова до установки» програми натискаємо кнопку Встановити, щоб почати установку. Встановили прапорець «Додати ярлики запуску консолей DeviceLock на робочий стіл», щоб додати ярлики запуску консолей DeviceLock Management Console, DeviceLock Enterprise Manager і DeviceLock Service Settings Editor на робочий стіл.

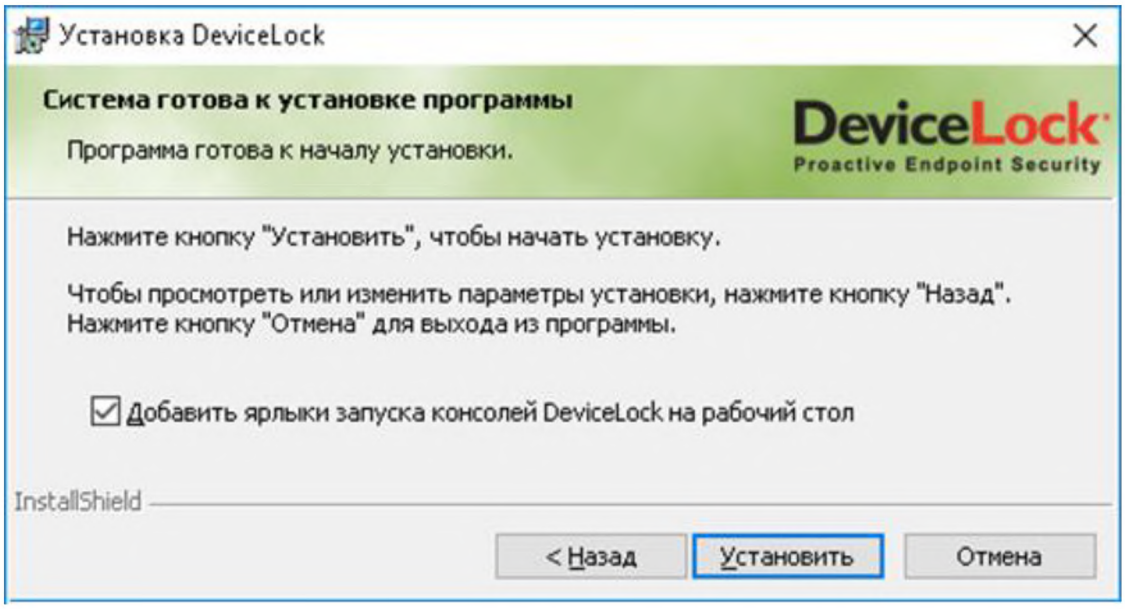

Рисунок 2.5 - Інсталяція DLP системи

В ході інсталяції , обираємо необхідні та популярні канали передачі даних (рисунок №2.6)

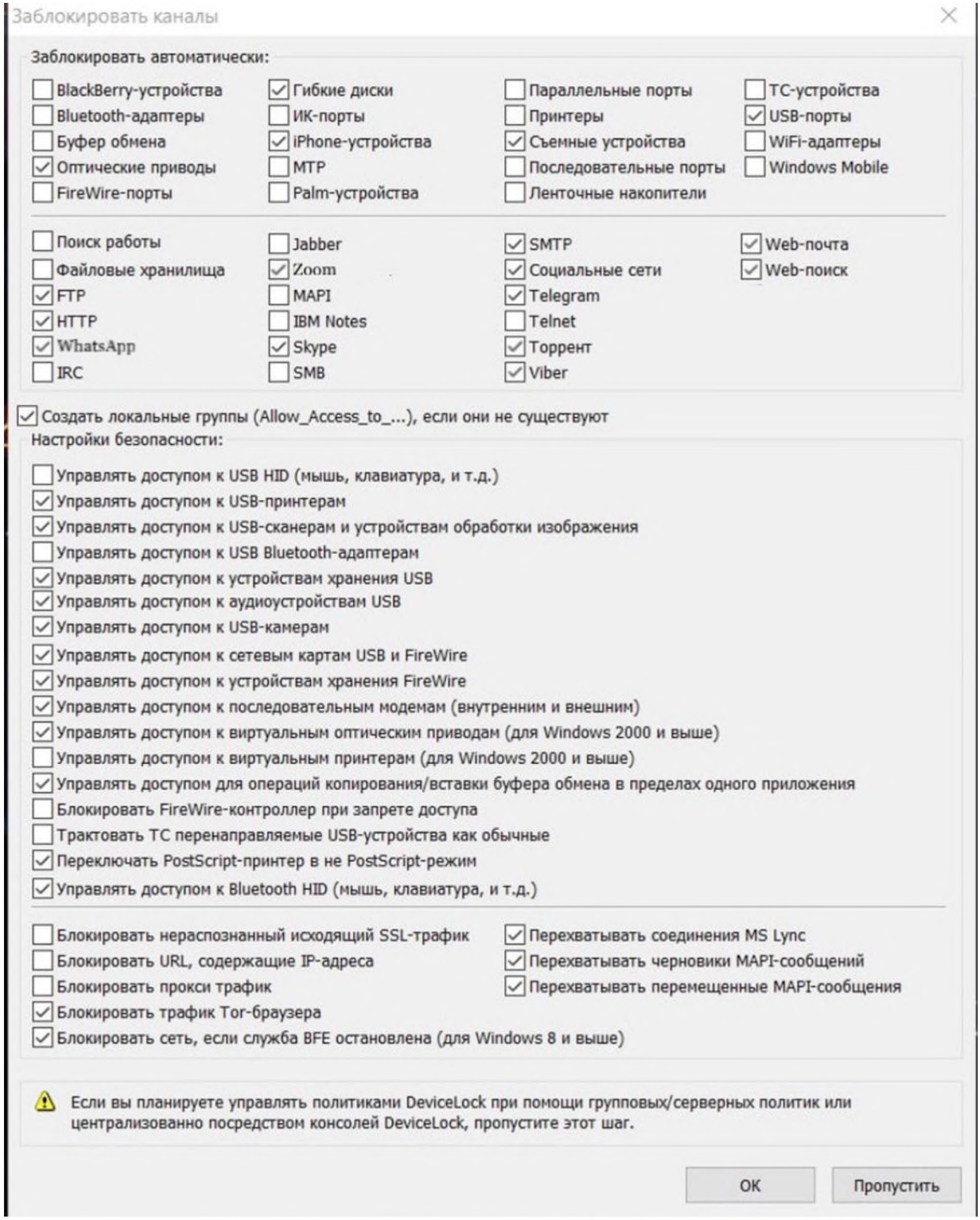

Рисунок 2.6 - Налаштування системи

Для завершення задаємо список адміністраторів серверу DeviceLock Enterprise Server (рисунок №2.7), а також інсталюємо секретний ключ сертифіката DeviceLock.

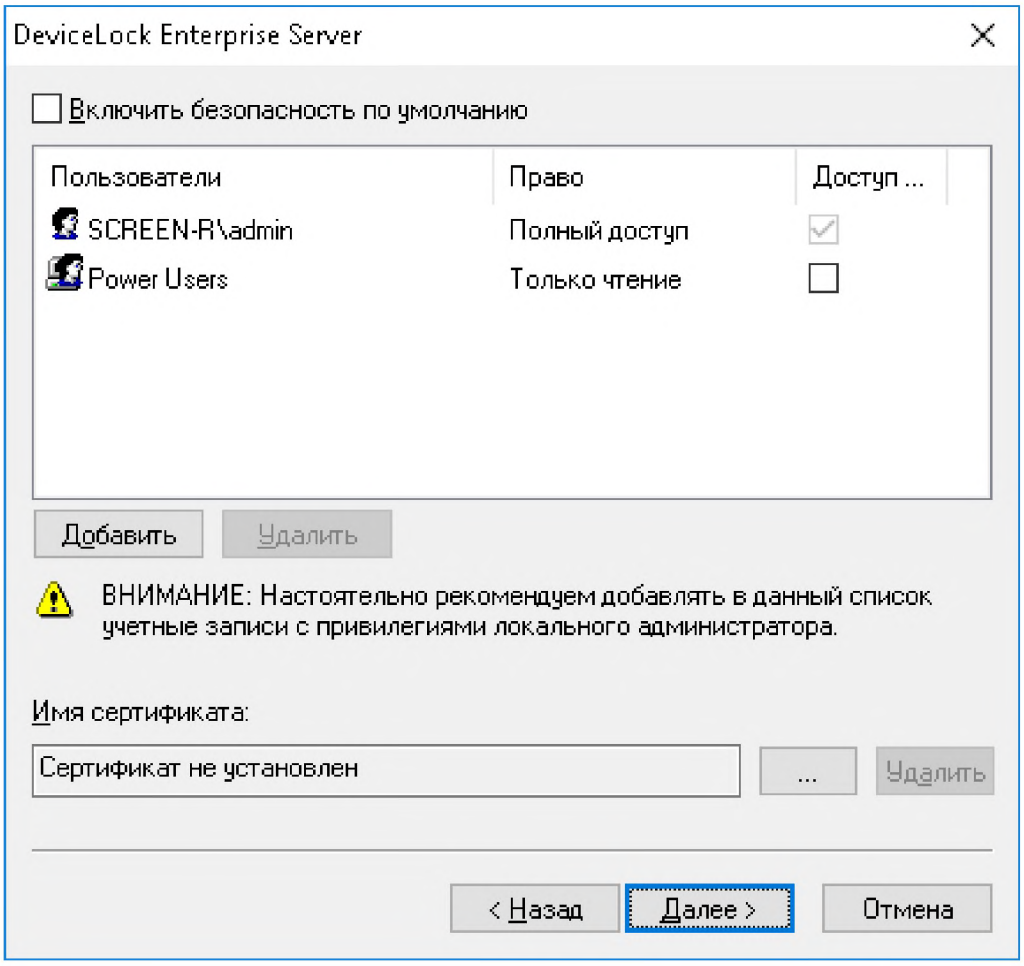

Рисунок 2.7 Налаштування DeviceLockEnterprise Server

До складу програмного комплексу DeviceLock DLP входять три основні частини: агент (сервіс DeviceLock), сервери (DeviceLock Enterprise Server і DeviceLock Content Security Server) і консолі управління (DeviceLock Management Console, DeviceLock Group Policy Manager, DeviceLock Enterprise Manager і DeviceLock WebConsole).

1. DeviceLock Enterprise Server (DLES) - це додатковий компонент, призначений для централізованого збору та зберігання даних тіньового копіювання і журналів аудиту. Для зберігання своїх даних DeviceLock Enterprise Server використовує сервер бази даних - SQL Server або PostgreSQL. Для рівномірного розподілу навантаження в локальній мережі кілька примірників DLES і серверів бази даних. Зображення компоненту схема на рисунку №2.8

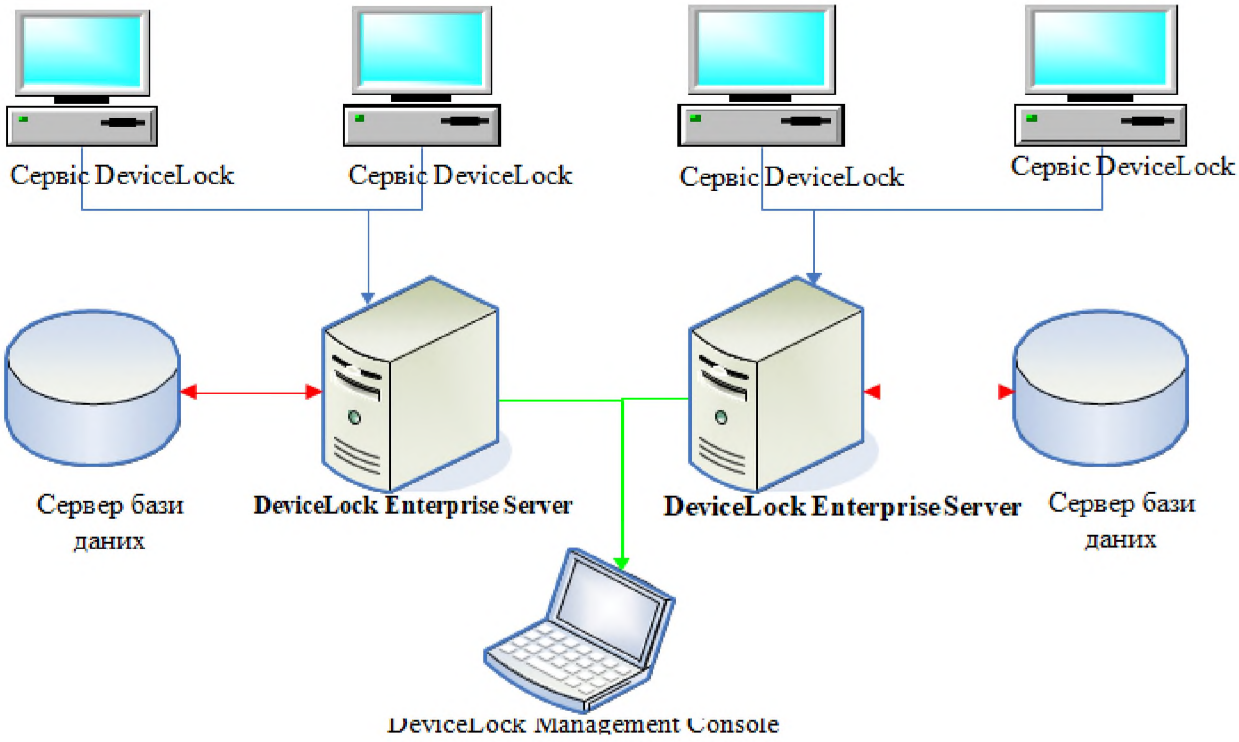

Рисунок 2.8 - схема DeviceLock Enterprise Server

DeviceLock Content Security Server - ще один додатковий компонент, що включає в себе компонент Search Server для швидкого пошуку тексту в файлах тіньового копіювання і журналах, які зберігаються на DeviceLock Enterprise Server.

2. Консоль управління - це інтерфейс контролю, який системний адміністратор використовує для віддаленого управління будь-якою системою, на якій встановлено сервіс DeviceLock. DeviceLock поставляється з чотирма консолями управління: DeviceLock Management Console (оснащення для MMC), DeviceLock Enterprise Manager, DeviceLock WebConsole і DeviceLock Group Policy Manager (інтегрується в редактор групових політик Windows). DeviceLock Management Console також використовується для управління DeviceLock Enterprise Server і Content Security Server. Зображення консолі управління на схемі №2.9

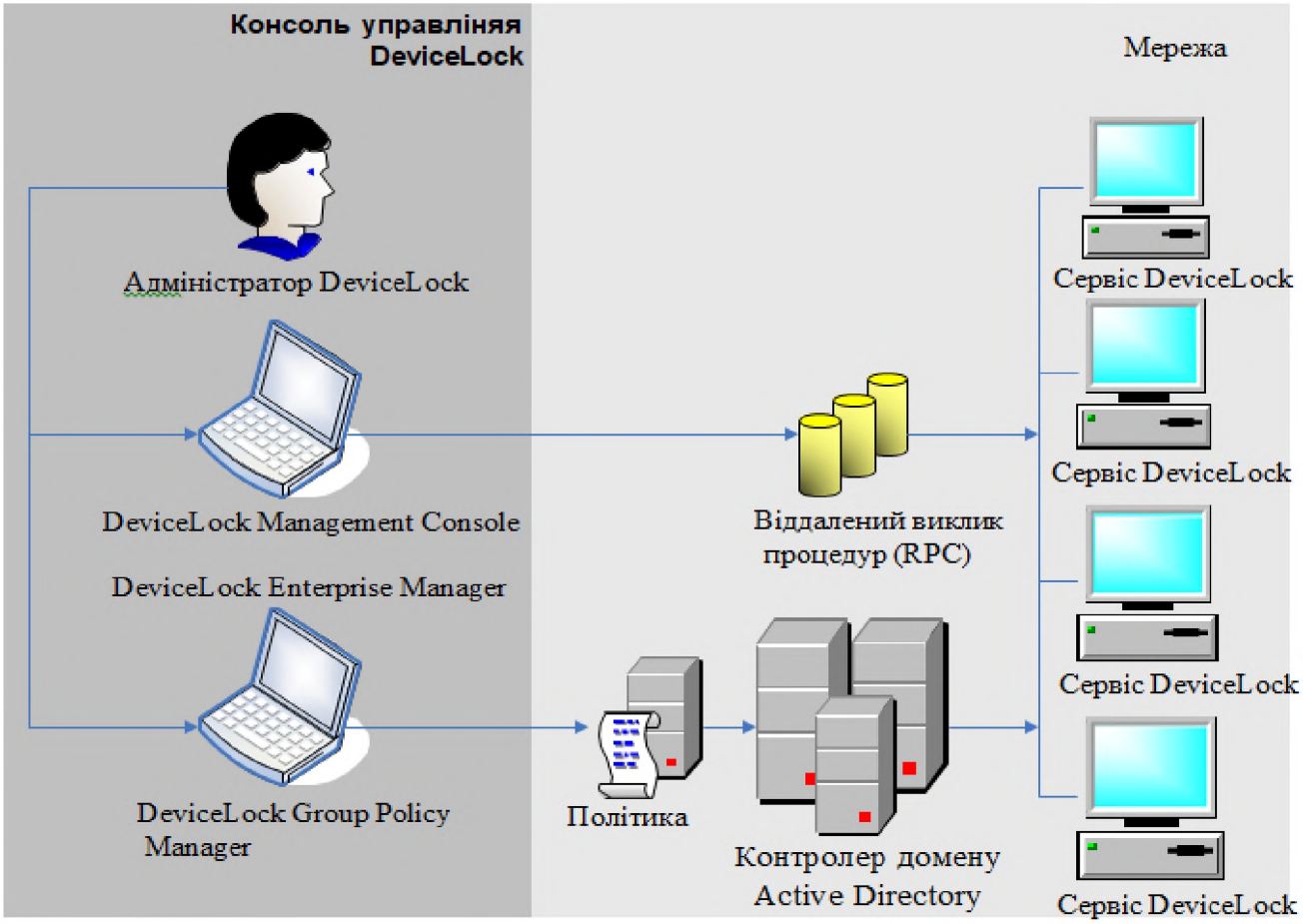

Рисунок 2.9 - схема консолі управління

3. Агент DeviceLock, або сервіс DeviceLock - це ядро системи DeviceLock. Агент встановлюється на кожен контрольований комп'ютер, автоматично запускається і забезпечує захист пристроїв і мережі на клієнті, залишаючись в той же час невидимим для локального користувача. Після інсталяції та ознайомлення з програмним комплексом DeviceLock, буде перевірена на основних поставлених для DLP задачах на різних рівнях. Зображення агента на схемі №2.10

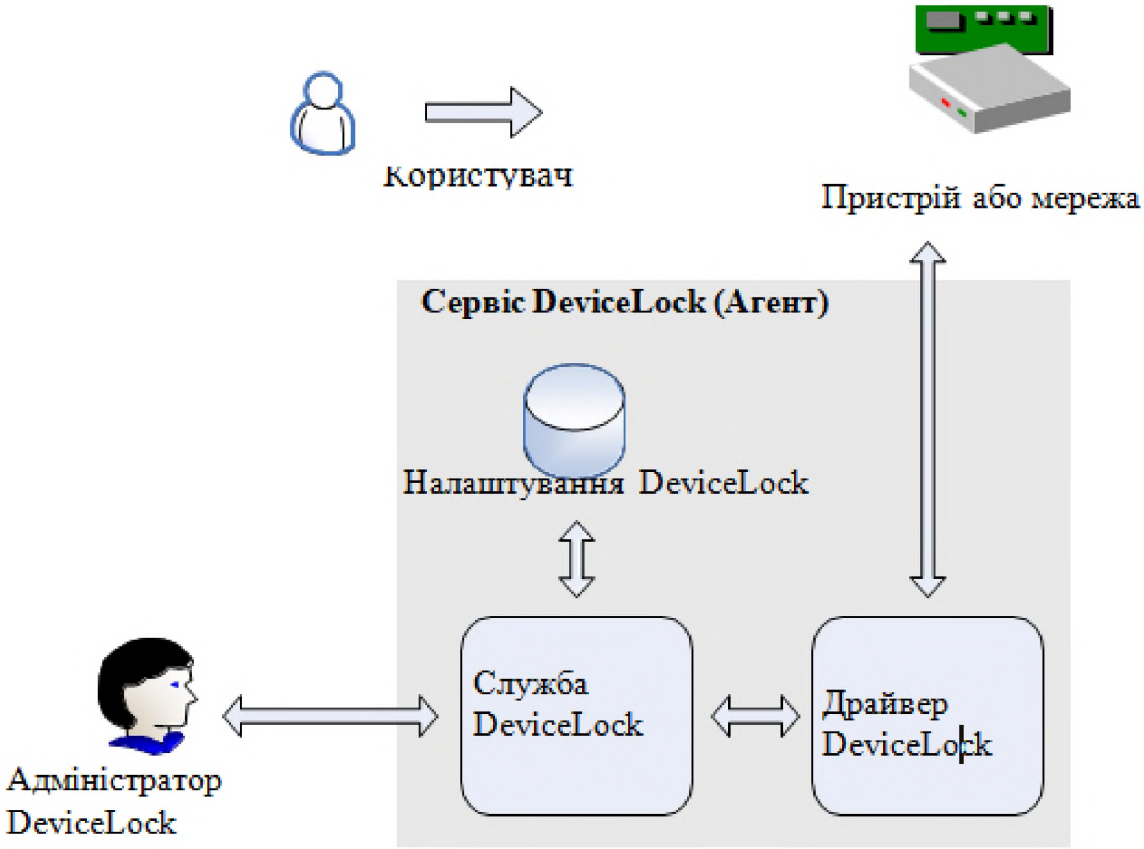

Рисунок 2.10 - схема Агент DeviceLock.

Контроль доступу для пристроїв працює наступним чином: кожен раз, коли користувач намагається отримати доступ до пристрою, DeviceLock перехоплює запит на рівні ядра ОС. Залежно від типу пристрою і інтерфейсу підключення (наприклад, USB), DeviceLock перевіряє права користувача у відповідному списку управління доступом (ACL). Якщо у користувача відсутні права доступу до цього пристрою, буде повернуто повідомлення про помилку "доступ заборонено".

Перевірка дозволів на доступ виконується на трьох рівнях: інтерфейс (порт), тип і зміст файлу. Деякі пристрої перевіряються на всіх трьох рівнях, в той час як інші - лише на одному: або на рівні інтерфейсу (порту), або на рівні типу. Схематично зображено на рисунку №2.11

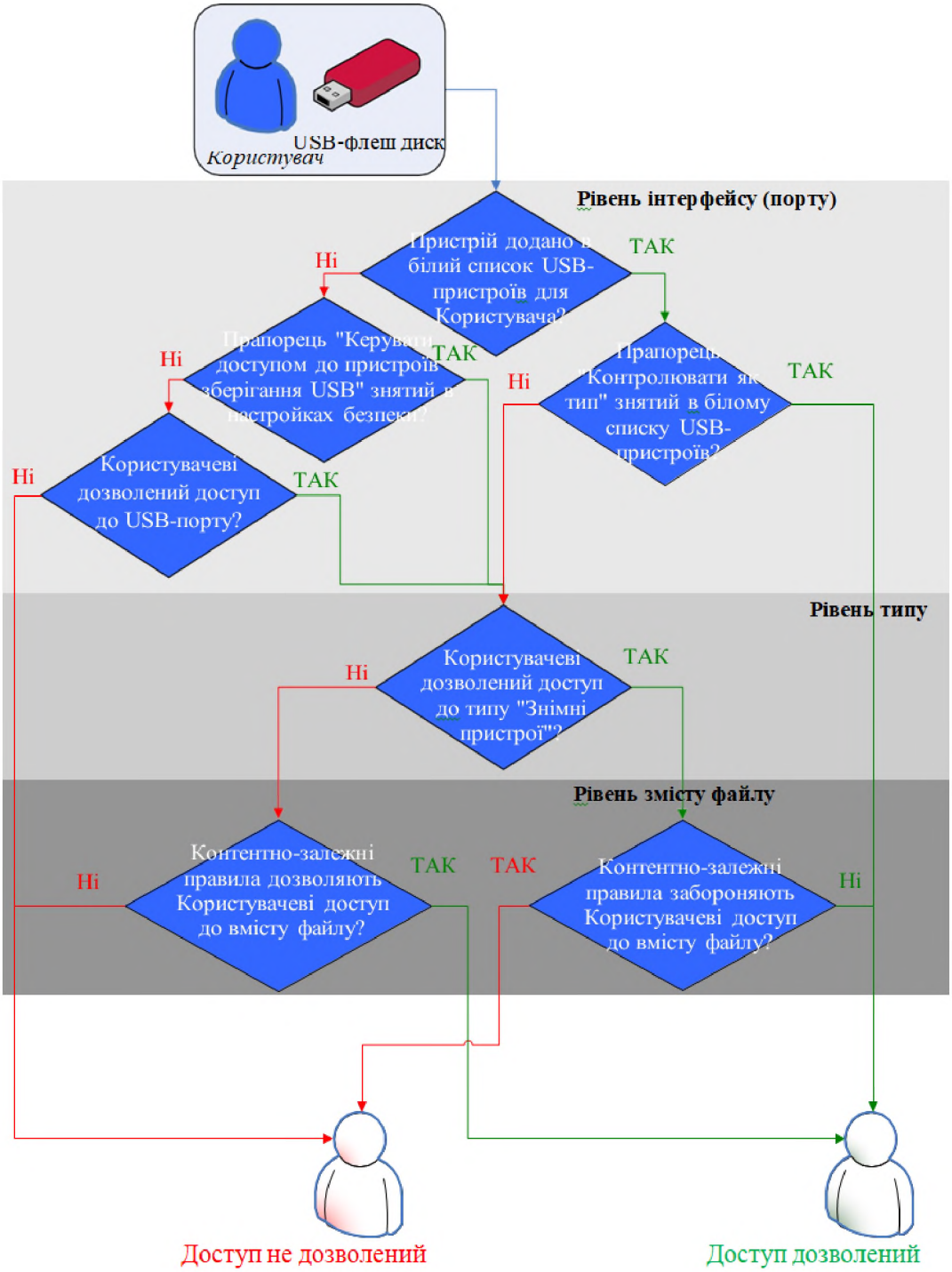

Рисунок 2.11 - Контроль доступу

Розглянемо випадок доступу користувача до USB-флеш через USB-порт (рисунок №2.12). В даному випадку DeviceLock в першу чергу перевірить на рівні інтерфейсу (USB-порту), відкритий чи ні доступ до USB-порту. Потім, оскільки Windows визначає USB-флеш як знімний носій, DeviceLock також перевірить обмеження на рівні типу пристрою (знімне). І на завершення перевірки DeviceLock також перевірить обмеження на рівні вмісту файлу, певні контентно-залежними правилами. У разі ж використання USB-сканера доступ буде перевірятися тільки на рівні інтерфейсу (USB-порту), оскільки DeviceLock не має окремого типу пристроїв для сканерів.

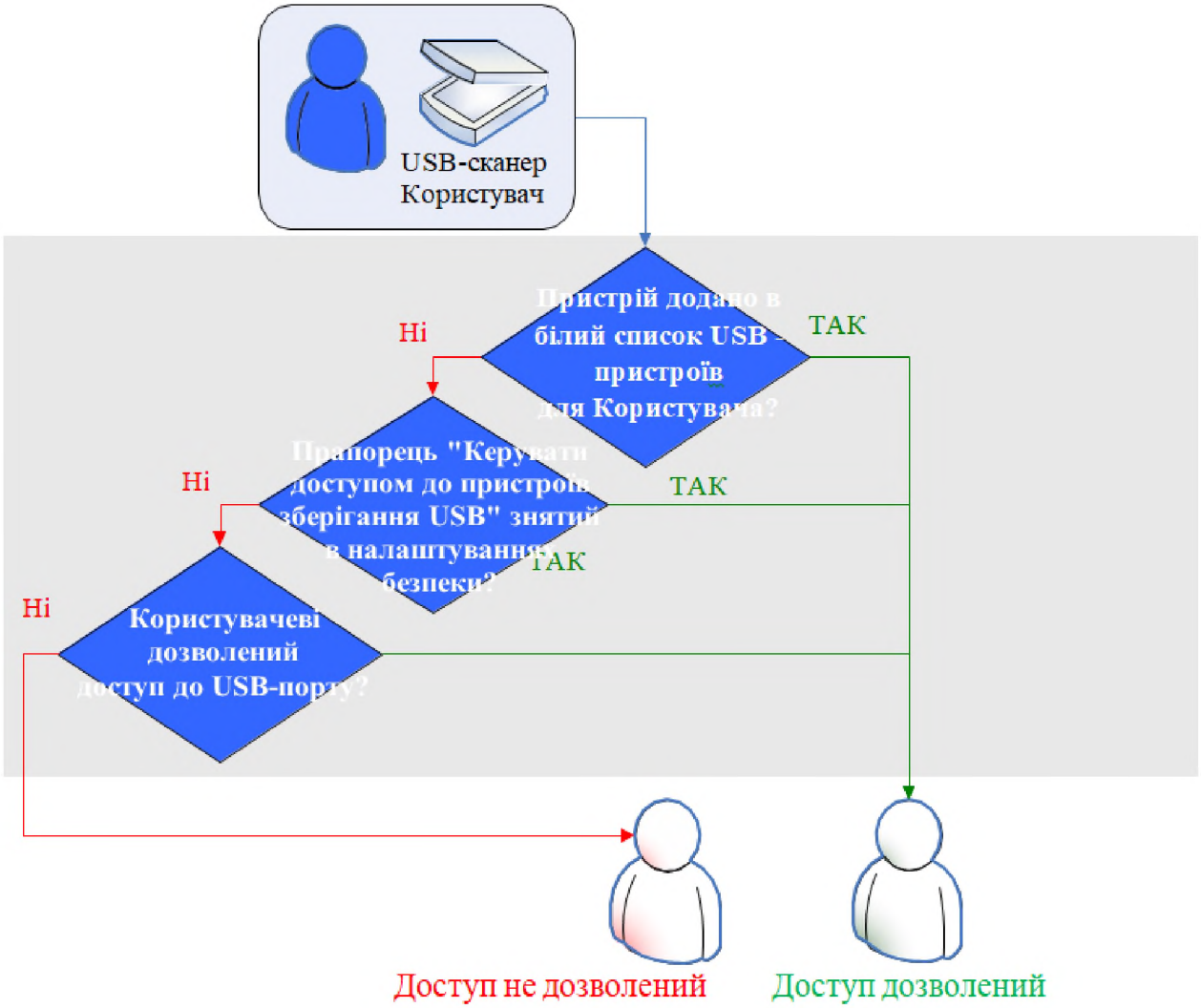

Рисунок 2.12 - випадок доступу користувача до USB-флеш через USB-порт

Існують додаткові налаштування безпеки, які можуть вимикати контроль доступу для класів пристроїв (наприклад для всіх USB-клавіатур і мишей), в той час як інші пристрої залишаються під контролем. В цьому випадку, якщо пристрій належить до класу, для якого контроль відключений, DeviceLock пропускає всі запити на з'єднання з цим пристроєм на рівні інтерфейсу (порту).

Контроль доступу для протоколів працює наступним чином: кожен раз, коли користувач намагається отримати доступ до віддаленого мережевого ресурсу, DeviceLock перехоплює запит на з'єднання на рівні ядра ОС і перевіряє права користувача у відповідному списку управління доступом (ACL). Якщо у користувача відсутні права доступу до даного протоколу, буде повернуто повідомлення про помилку "доступ заборонено". Зображено схематично на рисунку №2.13

Перевірка дозволів на доступ виконується на двох рівнях: протокол і зміст. Усі мережеві підключення перевіряються на обох рівнях, за винятком підключень по протоколам Торрент, Telnet , Telegram і WhatsApp, які перевіряються тільки на рівні протоколу. Наприклад, при спробі користувача підключитися до віддаленого вузла, DeviceLock перевірить, чи дозволено підключення на рівні протоколу, а потім будуть перевірені дозволу на рівні вмісту переданих даних, певні контентно -залежними правилами.

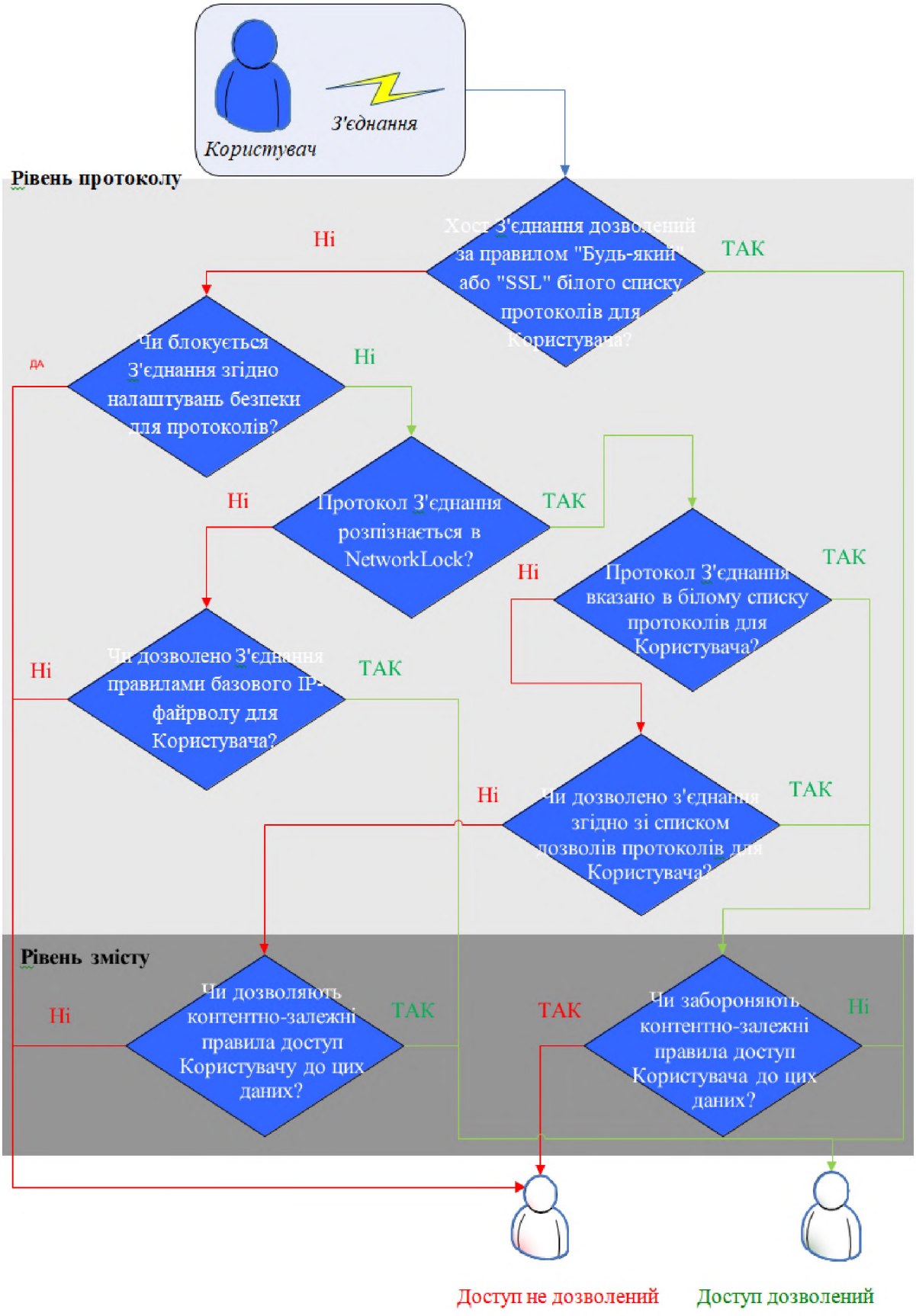

Рисунок 2.13 – Доступ до соціальної мережі

Розглянемо випадок доступу користувача до сайту соціальної мережі (рисунок №2.14). В даному випадку DeviceLock в першу чергу перевірить на рівні протоколу, відкритий чи ні доступ до соціальних мереж. Потім DeviceLock перевірить дозволу на рівні вмісту даних, певні контентно-залежними правилами.

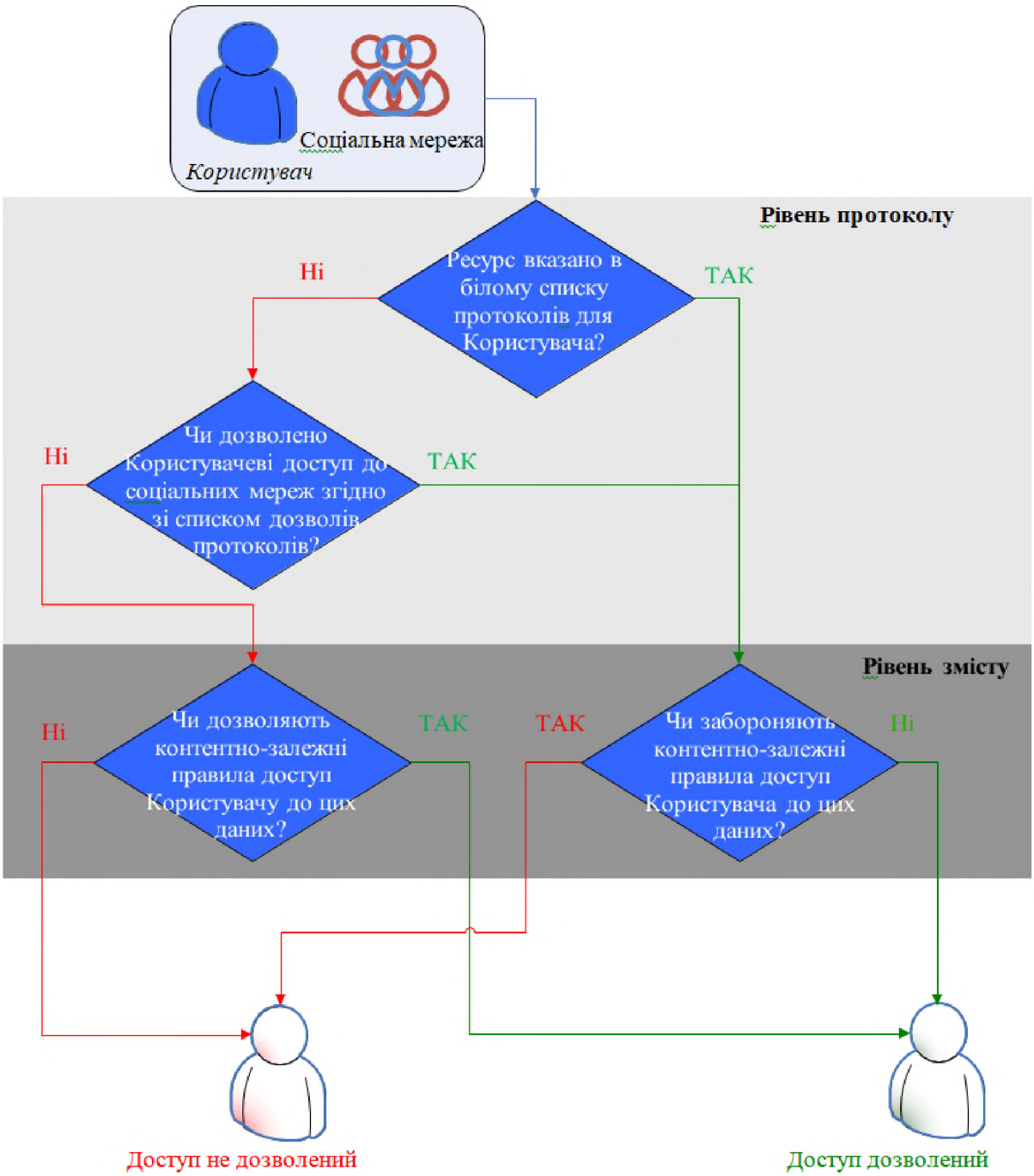

Рисунок 2.14 – Доступ до соціальної мережі

Найбільш ефективний підхід до захисту від витоків інформації з комп'ютерів починається з використання, перш за все, механізмів контекстного контролю - показувати чи даних для конкретних користувачів в залежності від форматів даних, типів інтерфейсів і пристроїв, мережевих протоколів, напрямки передачі, дня тижня і часу доби і т.д.

Однак, у багатьох випадках потрібно більш глибокий рівень контролю - наприклад, перевірка змісту переданих даних на наявність персональної або конфіденційної інформації в умовах, коли порти введення-виведення не повинні блокуватися, щоб не порушувати виробничі процеси, але окремі користувачі входять до «групи ризику», оскільки підозрюються в причетності до порушень корпоративної політики інформаційної безпеки. У подібних ситуаціях додатково до контекстного контролю необхідно застосування технологій контентного аналізу і фільтрації, що дозволяють виявити і запобігти передачі неавторизованих даних, не перешкоджаючи при цьому інформаційному обміну в рамках службових обов'язків співробітників.

Програмний комплекс DeviceLock DLP використовує як контекстні, так і засновані на аналізі контенту методи контролю даних, забезпечуючи надійний захист від інформаційних витоків з призначених для користувача комп'ютерів і серверів корпоративних ІС при мінімальних витратах на придбання та обслуговування комплексу. Контекстні механізми DeviceLock реалізують гранульований контроль доступу користувачів до широкого спектру периферійних пристроїв і каналів введення-виведення, включаючи мережеві комунікації.

Подальше підвищення рівня захисту досягається за рахунок застосування методів контентного аналізу і фільтрації даних, що дозволяє запобігти їх несанкціоноване копіювання на зовнішні накопичувачі і Plug-and-Play пристрої, а також передачу з мережних протоколах за межі корпоративної мережі. Поряд з методами активного контролю ефективність застосування DeviceLock забезпечується за рахунок детального протоколювання дій користувачів і адміністративного персоналу, а також селективного тіньового копіювання даних,

що передаються для їх подальшого аналізу, в тому числі з використанням методів повнотекстового пошуку.

Програмний комплекс DeviceLock DLP складається з взаємодоповнюючих функціональних модулів - DeviceLock, NetworkLock, ContentLock, DeviceLock Search Server (DLSS) і DeviceLock Discovery, що ліцензуються опціонально в будь-яких комбінаціях для задоволення завдань служб інформаційної безпеки.

2.5 Аналіз змін у мережі

Після інсталяції системи в мережу з правильним налаштуванням , офіцер безпеки (або супервайзер , який виконує обов'язки за додаткову оплату) може отримувати звіти на основі журналів сервера DeviceLock Enterprise Server. Звіти надають статистично оброблені дані про те, як співробітники використовують ті чи інші пристрої або мережеві протоколи. На етапі створення звіту визначаються його параметри, що дозволяють вибирати дані для побудови звіту. Наприклад, можна вказати звітний період, за який будуть відбиратися дані для звіту. Також DeviceLock дозволяє створювати дуже інтерактивні звіти (графи зв'язків) для відображення та аналізу комунікацій співробітників організації, засновані на даних про канали комунікації і частоті їх використання. За допомогою графа зв'язків можна візуально проаналізувати хто, з ким, як часто і яким способом здійснював комунікації. Звіти можна створювати, надсилати електронною поштою і зберігати в різних форматах. Звіти створюються в консолі DeviceLock Management Console.

Таким чином на основі звітів , можна зробити висновок а також зробити аналіз загроз з урахуванням DLP DeviceLock системи.

Проведемо аналіз загроз з урахуванням 3-х рівнів ризиків і збитків за 5-ти бальною шкалою після інсталяції DLP системи DeviceLock та внесемо у таблицю №2.9

- Великий – якщо реалізація загрози надає великих збитків (5 бали);
- Середній – якщо реалізація загрози надає помірних збитків (3 бали);
- Низький – якщо реалізація загрози надає незначних збитків (1 бал).

Таблиця 2.9 - Модель загроз з визначенням рівня ризиків і збитків після інсталяції DLP системи

	Механізм реалізації	Рівень		Сума загроз
		ризиків	збитків	
Загроза конфіденційності				
К.1	Викрадення носіїв з метою несанкціоновагого ознайомлення сторонніх осіб	1	3	4
К.1	Передавання співробітниками конфіденційної інформації стороннім особам	1	1	2
К.3	Агенти конкуруючих компаній	1	1	2
Загроза цілісності				
Ц.1	Навмисна модифікація або створення інформації персоналом ІТС на жорсткому диску або зовнішніх носіях	3	3	6
Ц.2	Прояви помилок системного ПЗ, в наслідок яких стала можливою модифікація ІзОД(інформація з обмеженим доступом)	3	3	6
Ц.3	Безпосередній доступ до інформації сторонніми особами	1	1	2
Загроза доступності				
Д.1	Помилки співробітників ІТС, які призвели до знищення інформації або доступу до неї	1	1	2
Д.2	Помилки системного ПЗ ІТС, які призвели до знищення інформації або доступу до неї	3	5	8
Д.3	Некоректне налагодження засобів захисту, яке призвело до втрати доступу до інформації	1	3	4

Таблиця 2.10 – Загальний рівень ризиків після інсталяції DLP системи DeviceLock

№	Види загроз	1	2	3	Сума загроз
1	Конфіденційності	4	2	2	8
2	Цілісності	6	6	2	14
3	Доступності	2	8	4	14

Отже с фінальної Таблиці №2.10 бачимо , що після впровадження DLP DeviceLock покращили показники КД , КВ , ЦО, ЦВ, ДР, НР, НК, НО, НЦ згідно з НД ТЗІ-2.5-005—99 та знизили рівень загроз для конфіденційності, цілісності та доступності.

КД - встановили обмеження на використання ПЗ, що не зазначене адміністратором, закрили доступ на передачу конфіденційних даних через сервіси в мережі інтернет, що не належать до корпоративних.

КВ – реалізовано і система дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією.

ЦО – система дає можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану.

ЦВ - Цілісність забезпечується за допомогою алгоритмів DLP системи , що дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації.

ДР - Користувачі мають обмеження до використання ресурсів.

НР - система дозволяє контролювати небезпечні для КС дії. DeviceLock Management Console дає можливість аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

НК – система може відслідковувати та взаємодіяти з апаратурою робочих станцій.

НЦ – система дає змогу ПК захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

НО – система дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Супервазеру (або найнятого нового співробітника на посаду офіцера безпеки) надали доступ до системи DLP та розподілили обов’язки між системними адміністраторами для того щоб була змога стежити та відслідковувати дії співробітників. Також встановлено обмеження прав користувачів і заборонена можливість до скачування та запуску будь-яких програм, що не будуть дозволені адміністратором або будуть знаходитись поза кореневою директорією Windows.

Ключові функції , які тепер викнуються через систему DeviceLock DLP в компанії:

- Контроль доступу до пристроїв і інтерфейсів.
- Контроль мережевих комунікацій.
- Тематична фільтрація.
- Виявлення несанкціонованого вмісту в сховищах даних.
- Сервер повнотекстового пошуку.
- Захист від локального адміністратора.
- Централізоване управління.
- Керуючий сервер.
- Контроль за типом файлів.
- Контроль буфера обміну.
- Білий список USB-пристроїв.
- Білий список носіїв.
- Тимчасовий білий список.
- Білий список мережевих протоколів.
- Аудит.
- Тіньове копіювання.
- Тривожні оповіщення (алертінг).
- Централізоване зберігання журналів аудиту та тіньового копіювання.
- Запобігання витоку даних через мобільні пристрої.
- Політики автономного та оперативного режиму.
- Оптичне розпізнавання символів (OCR).
- Інтеграція з зовнішніми засобами шифрування.
- Контроль для віртуальних і термінальних середовищ.

2.6 Висновки

Для вирішення проблеми інсайдерських витоків даних інсталювали програмний комплекс DeviceLock DLP . Багаторівневі контекстні механізми перевірки та перехоплення операцій забезпечують контроль доступу користувачів для широкого спектра потенційних каналів витоку даних. Подальше підвищення рівня захисту від витоків інформації досягається за рахунок застосування агентом DeviceLock аналізу і фільтрації контенту, що дозволяє запобігти їх несанкціоноване копіювання на знімні накопичувачі і Plug-and-Play пристрої, друк і передачу через мережеві додатки і інтернет-сервіси. Завдяки ефективному запобіганню витоків даних з корпоративних комп'ютерів DeviceLock DLP дозволяє організаціям звести до мінімуму відповідні ризики інформаційної безпеки, а також забезпечити відповідність корпоративним політикам захисту даних, стандартам безпеки в IT і вимогам регуляторів.

РОЗДІЛ 3 ЕКОНОМІЧНИЙ РОЗДІЛ

Успішність, як і ефективність будь-кого бізнесу, безпосередньо залежить від збереження і цілісності конфіденційних даних. У сучасних реаліях найбільш актуальною проблемою в сфері інформаційної безпеки, є захист особистих даних і запобігання несанкціонованого доступу до них простих користувачів.

Так виходить, що стандартні методи захисту даних, такі як Firewall, антивіруси, IPS (система запобігання вторгнень) до сьогодні не можуть забезпечити збереження даних від внутрішніх проблем - інсайдерів. Це користувачі, які ставлять перед собою мету крадіжку конфіденційної корпоративної інформації для подальшої її перепродажі конкурентам, передачі третім особам, публікації у відкриті джерела і т.д. Для запобігання навмисних або випадкових витоків конфіденційної інформації створюються спеціальні DLP системи. Тому метою економічного розділу є здійснення відповідних розрахунків, які дозволять встановити економічного ефекту від впровадження та налагодження комплексів засобів захисту інформації комп'ютерної мережі через DLP системи.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

До капітальних витрат належать витрати на розробку політики безпеки інформації, які визначаються виходячи з трудомісткості розробки політики безпеки інформації.

Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{mз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин,} \qquad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_в$ – тривалість розробки концепції безпеки інформації у організації;

$t_а$ – тривалість процесу аналізу ризиків;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_д$ – тривалість документального оформлення політики безпеки.

Визначено, що відповідно до етапів розробки політики безпеки інформації, тривалість операцій склала наступні величини:

$t_{тз}$=24 годин, $t_в$=20 годин, $t_{тз}$=40 годин, $t_{вз}$=54 годин, $t_{озб}$=6 годин, $t_{овр}$=6 годин, $t_д$=6 годин.

Отже, t=24+20+40+54+6+6+36= 186 годин,

Розрахунок витрат на створення політики безпеки інформації Витрати на розробку політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч.

$$К_{рп} = З_{зп} + З_{мч} . \qquad (3.2)$$

$$К_{рп} = З_{зп} + З_{мч} = 24000 + 1110,42 = 25110,42 \text{грн.}$$

$$З_{зп} = t\, З_{пр} = 186 * 129 = 24000 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t*С_{мч} = 186*5,97 = 1110,42 грн.$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = 0,9 \cdot 3 \cdot 1,64 + \frac{3800 \cdot 0,4}{1920} + \frac{7200 \cdot 0,2}{1920} = 5,97 \text{ грн.}$$

Відповідно до розроблених рекомендації щодо удосконалення існуючої системи інформаційної безпеки мережі «TravelTeam», а також рекомендацій та інструкції по безпосередній роботі з системою планується використання антивірусу NOD32, який вже встановлений на комп'ютерах підприємства та потребує лише подовження ліцензії.

Для впровадження DLP системи обрано DeviceLock програмний комплекс, вартість якого складає 40 000грн. Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають 20% відсотків від первісної вартості програмного забезпечення, тобто 8000 грн. Також планується придбання додаткових модулей для DLP системи , вартість яких складає 1500грн.

Таким чином, капітальні (фіксовані) витрати на створення політики інформаційної безпеки підприємства складають:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$
$$= 25110,42 + 40000 + 1500 + 8000 = 74\,610,42 \text{ грн.}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн.} \qquad (3.3)$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.} \qquad (3.4)$$

Витрати на навчання адміністративного персоналу (супервайзерів та адміністраторів) визначаються ($С_{н} = 7000$ грн.).

Річні амортизаційні відрахування за обслуговування та додаткову підтримку збоку розробників складає 5000 грн із корисним строком використання 2 роки, за прямолінійним методом нарахування амортизації складуть:

$С_{а} = 5000 / 2 = 2500$ грн.

Вартість подовження ліцензії наступних програмних комплексів:
- антивірусу NOD32, який вже встановлений на всіх комп'ютерах підприємства, складає 579грн на рік.
- Nmap, яка вже встановлена на 2 комп'ютерах підприємства, складає 309грн на рік.
- cisco Jabber та Sender , яка вже встановлена на 28 комп'ютерах підприємства, складає 2500грн загально за комплекс сервісу на рік.
- Columbis CRM, яка вже встановлена на 30 комп'ютерах підприємства, складає 699грн на рік.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.5)$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 8000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Отже,

$$С_з = 8000*12 + 8000*12*0,1= 105600\text{грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 8000*0,22 = 1760 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.6)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=2,3 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$С_{ел}$ = 2,3*1920*1,68 = 7418,88 грн.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% (Стос =74 610,42 *0,01=746,10 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$С_к$ = 7000+2500+579+309+2500+699+105600грн +1760 +7418,88 + 746,10 = 129 111,98грн.

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 249 891,98грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 6000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 8000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 2 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 15 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 1млн. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 50.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить, а також наслідки від втраченої інформації:

$$U = П_п + П_в + V, \qquad (3.7)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зо}{F} \cdot t_n = \frac{6000 \cdot 9}{165} \cdot 4 = 1309{,}09 \quad \text{грн},$$

де F – місячний фонд робочого часу.

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \qquad (3.8)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum Зо}{F} \cdot t_{ви} = \frac{6000 \cdot 9}{165} \cdot 6 = 1963{,}63 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{8000 \cdot 1}{165} \cdot 2 = 96{,}96 \text{ грн.}$$

$П_в$ = 1963,63 + 96,96 = 2060,60 грн.

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або втраченої інформації із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{1000000}{2080} \cdot (4 + 2 + 6) = 5769{,}23 \text{грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

U =1309,09+ 2060,60 + 5769,23 = 9138,92 грн.

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_1 \sum_{50} 9138{,}92 = 456946 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.,} \qquad (3.9)$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (35%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

Е = 456 946*0,35 – 129 111,98= 30 819,12 грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \qquad (3.10)$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{30819,12}{74\,610,42} = 0.41,$$ частки одиниці,

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (18 %);

$N_{інф}$ – річний рівень інфляції, (11%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,41 > (18 - 11)/100 = 0,41 > 0,07.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0,41} = 2.4,$$ років.

3.4 Висновок

Розробка системи захисту від витоку конфіденційної інформації в комп'ютерній мережі «TravelTeam» є економічно доцільним, оскільки капітальні та експлуатаційні витрати будуть меншими за можливий відвернений збиток. Капітальні витрати складають 74 610,42 грн., експлуатаційні – 129 111,98грн. Величина річного економічного ефекту складає 30 819,12 грн. Коефіцієнт повернення інвестицій ROSI складає 0,41 грн./грн.

З розрахунків , видно , що впровадження DLP DeviceLock системи та його експлуатація , є коштовним в матеріальному плані ресурсі , але необхідним.

ВИСНОВОК

У сучасному інформаційному світі завдання захисту цінної інформації стає не просто примхою, а нагальною необхідністю. Корпоративне шпигунство і отримання несанкціонованого доступу до даних стає буденним явищем, а цінність інформації зростає з кожним роком.

У цій роботі було ознайомлення с DLP системами, розібрано основні функції DLP систем , а також проаналізовано методи аналізу потоків даних. Було обрано та описано 3 найбільш актуальні системи протидії витоку інформації для малого та середнього бізнесу , а остаточний вибір був зроблений на користь DeviceLock DLP. Система була обрана , тому що виконує всі основні функції захисту інформації , які були поставлені в кваліфікаційній роботі та є доцільною з економічної точки зору.

Основною метою було поставлено встановлення моделі загроз та опис потенційного порушника в мережі компанії для аналізу можливих витоків інформації. На основі аналізу інстальована DeviceLock DLP система з основними налаштування для корпоративної мережі. Програмний комплекс DeviceLock DLP ефективно запобігає витоку інформації з корпоративних комп'ютерів, використовуючи повний набір механізмів контекстного контролю операцій з даними, а також технології їх контентної фільтрації.

З економічної точки зору , система є дуже вигідною , за підрахунками може окупити себе майже за 2 роки. Оскільки компанія буде активно розвиватись , питання безпеки при роботі з даними є дуже актуальним. Все більше компаній розуміють, що захищатися від витоків важливо. І краще робити це за допомогою спеціалізованих рішень, які відмінно справляються з таким завданням, запобігаючи фінансові, репутаційні та інші види втрат.

ПЕРЕЛІК ПОСИЛАНЬ

1. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5—004—99 [Електронний ресурс]. – 1999р. — Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.5—004—99.pdf.

2. Порядок проведення робіт по створенню комплексної системи захисту інформації в інформаційно—телекомунікаційній системі НД ТЗІ 3.7—003 —2005 [Електронний ресурс]. — 2005. — Режим доступу до ресурсу: https://tzi.com.ua/downloads/3.7—003—2005.pdf.

3. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5—005—1999 – Київ 1999 р.

4. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу НД ТЗІ 2.5—005 —99 [Електронний ресурс]. — 1999. — Режим доступу до ресурсу: https://tzi.ua/assets/files/%D0%9D%D0%94—%D0%A2%D0%97%D0%86—2.5—005——99. pdf.

5. Налаштування захисту кінцевих точок [Электронный ресурс] — Режим доступу к ресурсу:https://docs.mcafee.com/ru—RU/bundle/endpoint—security—10.7.x—common—product—guide—windows/page/GUID— E3F80434—FD29—4D5C—A150—7BD6DC88BC21.html.

6. Закон України про інформацію: [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

7. Закон України про телекомунікації: [Електронний ресурс] – Режим до—ступу: https://zakon.rada.gov.ua/laws/show/1280-15#Text

8. Вибір DLP системи [Електронний ресурс] — Режим доступу до ресурсу: https://q.center/kak—vybrat—dlp—i—ne—oshibitsya—funktsionalnost—stoimost—vladeniya—i—doverie—k—vendoru/.

9. Компьютерные сети [Электронный ресурс]. — 2012. — Режим доступа к ресурсу: https://www.litmir.me/br/?b=639789.

10. Вимоги до системи захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: https://studfiles.net/preview/6012701/page:6

11. DeviceLock DLP: https://www.devicelock.com/ru/

12. Системы предотвращения утечек данных — Режим доступу до ресурсу:http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/dlp-systems

13. Системы защиты от утечек конфиденциальной информации (DLP)— Режим доступа к ресурсу: https://www.anti-malware.ru/security/data-loss-prevention

14. Інформаційний ресурс Хабр: https://habr.com/ru/post/440838/

15. Предотвращение утечки данных: http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/dlp-systems

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	1	
5	А4	1 Розділ	21	
6	А4	2 Розділ	37	
7	А4	3 Розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г ВІДГУК

На кваліфікаційну роботу студента групи 125-17-1

Пащенко Тимофія Валерійовича

на тему

«Розробка засобів захисту інформації інформаційно-телекомунікаційної системи підприємства «TravelTeam» на основі DLP технології»

Пояснювальна записка складається зі вступу, трьох розділів і висновків викладених на 85 стор.

Метою роботи є розробка системи захисту інформації від антропогенних загроз підприємства «TravelTeam».

Тема кваліфікаційної роботи тісно пов'язана з об'єктом діяльності бакалвара спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: проведення аналізу найпопулярніших DLP систем, їх оцінка та обрання більш актуальної для конкретного підприємтва. Впровадили систему в мережу та побачили покращення безпеки інформації для підприємства.

На основі моделі загроз було розроблено елементи комлексної системи захисту інформації і обраний профіль захищеності, відштовхуючись від якого були виконані всі вимоги захищеності інформації.

За час дипломування Пащенко Т.В проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека»

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

Кваліфікаційна робота заслуговує оцінки _____.

Керівник