ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія протидії несанкціонованому доступу до ресурсів інформаційної системи організації на базі DLP»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Нікита БОРИСЕНОК

Виконав: здобувач(ка) вищої освіти групи БСДМ-63
БОРИСЕНОК Нікита
(ПРІЗВИЩЕ, Ім'я)

Керівник: ГАЙДУР Галина
д.т.н, професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Борисенку Нікіті Дмитровичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія протидії несанкціонованому доступу до ресурсів інформаційної системи організації на базі DLP»
керівник кваліфікаційної роботи: ГАЙДУР Галина, д.т.н., професор,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
інформаційна система організації;
Технологія протидії несанкціонованому доступу до ресурсів інформаційної системи організації на базі DLP;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз необхідності контролю доступу до мережі на основі застосування політик пристроїв і користувачів корпоративних мереж.

2. Методи та засоби управління мережевим доступом організацій.

3. Технологія протидії несанкціонованому доступу до ресурсів інформаційної системи організації на базі DLP.

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми управління привілеями в інформаційній системі організації	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз необхідності контролю доступу до мережі на основі застосування політик пристроїв і користувачів корпоративних мереж	27.10. 2023р.	
4.	Методи та засоби управління мережевим доступом організацій	03.11.2023 р.	
5.	Розроблення варіанта технології управління доступом до мережі організації на базі рішення CISCO ISE	15.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач(ка) вищої освіти _____ Нікита БОРИСЕНОК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Галина ГАЙДУР

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи и на здобуття освітнього ступеня магістра: 76 сторінок, 20 рисунків, 4 таблиці, 21 джерел.

Об'єкт дослідження – процес контролю несанкціонованому доступу до мережі інформаційної системи організації.

Предмет дослідження – Технологія протидії несанкціонованому доступу до ресурсів інформаційної системи організації на базі DLP.

Мета роботи – Покращення інформаційної безпеки організації шляхом впровадження технології протидії несанкціонованому доступу до ресурсів інформаційної системи на базі системи захисту даних (DLP).

Методи дослідження - дослідження включають аналіз журналів подій системи DLP, проведення відновлення інцидентів, тестування вразливостей та аудит безпеки. Ці підходи дозволяють ефективно визначити ефективність заходів безпеки та виявити можливі ризики та вразливості в інформаційній системі організації.

В роботі проведено аналіз проблеми контролю доступу до мережі на основі застосування політик пристроїв і користувачів корпоративних мереж. Проаналізовано існуючі технології контролю доступу до мережі організації.

Досліджено ефективності впроваджених заходів DLP через систематичний аналіз інцидентів, виявлених та зареєстрованих системою.

Запропоновано варіант забезпечення ефективного контролю та моніторингу передачі та використання конфіденційної інформації, а також запобігання витокам даних шляхом виявлення, блокування та відстеження небажаної активності користувачів.

На основі проведених досліджень, в роботі розроблено варіант запобігання витокам даних шляхом виявлення, блокування та відстеження небажаної активності користувачів за допомогою DLP

Галузь використання – кібербезпека корпоративної мережі.

КОРПОРАТИВНА ІНФОРМАЦІЙНА МЕРЕЖА, КІБЕРБЕЗПЕКА, КОНТРОЛЬ ДОСТУПУ, МЕТОДИ ТА ЗАСОБИ, AAA, TACACS+, АРХІТЕКТУРА, МОДУЛІ, ФУНКЦІЇ

ABSTRACT

Text part of the master's qualification work:76 pages, 18 figures, 2 tables, 14 sources.

The purpose of the work is to develop options for network control management technology based on the Cisco Identity Services Engine solution for the organization's information system and recommendations for using the technology.

Object of research - is the process of managing control to the organization's information system network.

Subject of research - is the technology network control management technology based on the Cisco Identity Services Engine solution.

Research methods - study of the literature on this topic, analysis of operating documentation, international standards and their comparison, modeling of the network access control management process based on the Cisco Identity Services Engine solution.

The paper analyzes the problem of network access control based on the application of policies of devices and users of corporate networks. Existing access control technologies to the organization's network were analyzed.

The methods and means of managing network access of organizations have been studied.

A version of the access management technology to the organization's network based on the CISCO ISE solution is proposed. The purpose, main functions and composition of the modules of this technology are determined.

On the basis of the research carried out in the work, a version of the technology for managing access to the organization's network based on the CISCO ISE solution was developed.

The field of use is cyber security of the corporate network.

CORPORATE INFORMATION NETWORK, CYBER SECURITY, ACCESS CONTROL, METHODS AND TOOLS, AAA, TACACS+, ARCHITECTURE, MODULES, FUNCTIONS

ЗМІСТ

–

–

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NAC - контролю доступу до мережі

ISE - Identity Services Engine

NAC - network access control

BYOD - принесіть свій власний пристрій

PAN - Policy Administration Node

MnT node - Monitoring Node

PDP – Policy Decision Point

PEP – Policy Enforcement Point

M&T – моніторинг і усунення несправностей

TACACS+ - Terminal Access Controller Access-Control System Plus

VPN - Virtual Private Network

RADIUS - Remote Authentication Dial-In User Service

–

ВСТУП

У сучасному інформаційному суспільстві, де обсяги даних постійно зростають, їхня конфіденційність і цілісність стають ключовими пріоритетами для організацій. Загрози витоку даних становлять серйозний виклик, який може завдати значної шкоди як фінансовій стабільності, так і репутації компанії. У цьому контексті, тема Data Leak Prevention (DLP) стає актуальною і стратегічно важливою для забезпечення безпеки інформації.

Дипломна робота присвячена дослідженню та розробці методів і технологій DLP з метою запобігання витокам конфіденційних даних. Аналіз наявних методів та інструментів DLP, їхньої ефективності та застосовності в різних сценаріях, а також розробка нових підходів до забезпечення безпеки даних - усе це є основним фокусом дослідження.

У межах роботи буде розглянуто ключові проблеми, пов'язані з управлінням витоками даних, а також запропоновано інноваційні рішення для ефективного контролю та запобігання потенційним загрозам. Дослідження також приділятиме увагу практичним аспектам впровадження DLP-рішень у корпоративне середовище, їхньому налаштуванню та адаптації до специфіки різних галузей.

Мета цієї дипломної роботи - не тільки надати глибокий аналіз наявних рішень DLP, а й запропонувати конструктивні рекомендації для організацій, які прагнуть ефективно управляти ризиками витоків даних. Передбачається, що результати цього дослідження матимуть важливий вплив на розвиток сфери інформаційної безпеки і стануть основою для подальших інновацій у сфері DLP.

1. ВСТУП ДО ПРОБЛЕМАТИКИ НЕСАНКЦІОНОВАННОГО ДОСТУПУ

1.1. Актуальність цифрової безпеки та наслідки

У сучасному інформаційному суспільстві, де організації залежать від цифрових технологій для зберігання та обробки чутливої інформації, питання безпеки даних стають дедалі критичнішими. Одним з основних викликів, з яким стикаються організації, є несанкціонований доступ до їхніх інформаційних ресурсів. Цей вид загрози не тільки може призвести до витоків конфіденційних даних, а й залишити організацію вразливою перед різними видами кібератак.

Сформований ландшафт загроз в інформаційному середовищі ускладнюється динамічними та багатогранними природою кібератак. Атакуючі постійно вдосконалюють свої методи, використовуючи передові технології, а також звертаючись до соціальних та інженерних аспектів, щоб обійти традиційні системи захисту. Поява масштабних інцидентів, таких як витоки великих обсягів конфіденційної інформації, підкреслює актуальність проблеми несанкціонованого доступу та необхідність інтегрованих підходів до безпеки даних.

Усвідомлення важливості забезпечення конфіденційності, цілісності та доступності даних усередині організацій призводить до прагнення до розроблення та впровадження ефективних заходів із запобігання несанкціонованому доступу. У цьому контексті, технологія DLP (Data Loss Prevention) виокремлюється як ключовий інструмент в арсеналі засобів інформаційної безпеки, призначений для контролю і захисту конфіденційних даних організації.

1.2. Факти щодо витоку інформації за останні 5 років

Протягом 2014 року в світі було зафіксовано та оприлюднено у ЗМІ понад 1200 випадків витоку конфіденційної інформації, що на 19% перевищує

показники попередніх років. У пресі були оголошені збитки кредитно-фінансових організацій від витоків, які становили трохи більше 45,6 млн. доларів США за перше півріччя 2015 року. Кількість скомпрометованих записів перевищила 1,3 млрд., включаючи фінансову та особисту інформацію. Випадкові витоки стали менш поширеними, складаючи лише 39%. У державних компаніях та муніципальних установах збільшилася частка витоків, досягнувши 27% (зі зростанням на 9% порівняно з 2016 роком). Найбільш поширеним видом витоків залишаються персональні дані, що становлять 89,2%. Основним каналом витоків залишається паперова документація, яка відзначається на рівні 21,6%.

1.2.1. Статистика витоку інформації

У 2017 році Центром аналізу InfoWatch зафіксовано значну кількість випадків витоку інформації з компаній приватного та державного сектору. Серед жертв - понад 31 млн користувачів віртуальної клавіатури, де особиста інформація стала доступною через помилкові налаштування сервера розробників.

Дані, що просочилися, містили повне ім'я, місце розташування, адресу електронної пошти і час від встановлення програми. Користувачі безкоштовної версії клавіатури постраждали більше, адже їхні розширені дані також були зібрані.

В Індії виникла проблема з даними бенефіціарів, коли 210 веб-сайтів урядових установ розкрили особисті дані, такі як адреси та номери телефонів, у демонстрації переваг ідентифікаційного номера Aadhaar.

Уряд вживає заходів для запобігання подібних порушень. Фотосервіс Imgur також став жертвою порушення безпеки, коли понад 1,7 млн акаунтів було скомпрометовано у 2014 році. Хоча паролі були зашифровані, інформація про адреси електронної пошти вже раніше містилася в базі "Have I Been Pwned?".

–

Спроби атаки на інформаційні системи німецького Siemens та американських компаній Moody's і Trimble призвели до звинувачень на адресу трьох китайських громадян. Усі ці інциденти свідчать про постійну загрозу безпеці в інтернет-просторі та необхідність подальших заходів для захисту конфіденційної інформації.

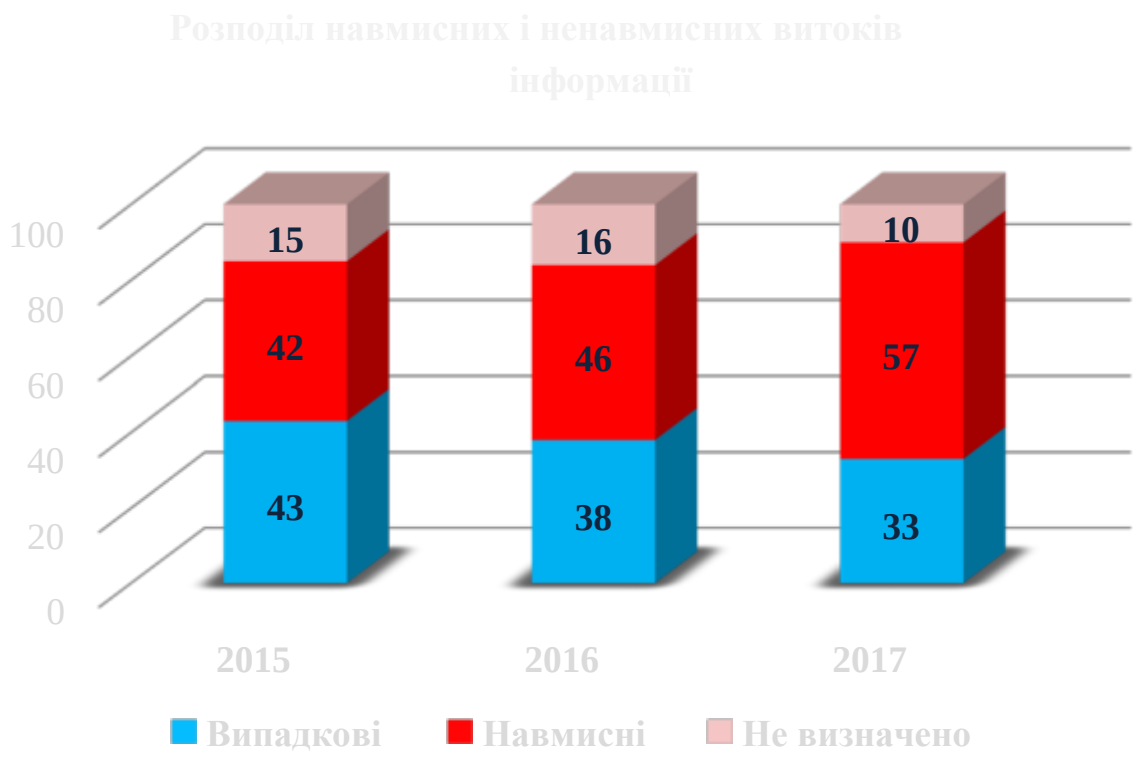

Рисунок 1.1 – Розподіл навмисних і ненавмисних витоків, 2015-2017рр.

–

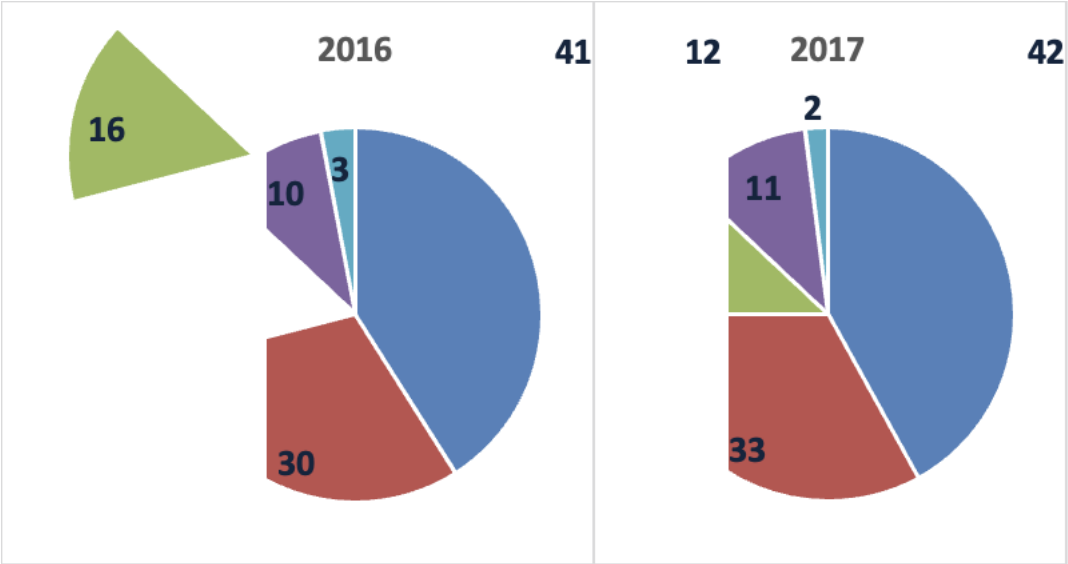

Рисунок 1.2 – Розподіл витоків інформації по організаціях, 2015-2017 рр.

Аналізуючи статистичні дані про розподіл витоків за період 2015-2017 років, можна відзначити, що рівень витоків в освітніх установах зменшився до 12%, порівняно з 19% у 2015 році. Збільшення частки витоків у комерційних та державних структурах можна пояснити проведенням інформаційної війни між державами.

1.3. Інформаційно-телекомунікаційна система підприємства

Інформаційно-телекомунікаційна система (ІТС) підприємства - це комплекс інтегрованих технологій, програмних засобів та апаратних засобів, спрямованих на забезпечення ефективного обміну, зберігання, обробки та передачі інформації всередині організації. Ця система включає в себе різноманітні компоненти, які спільно працюють для підтримки інформаційних потреб підприємства. Розглянемо деякі ключові складові ІТС підприємства:

Інформаційні системи (ІС): Вони включають в себе програмні продукти для автоматизації бізнес-процесів, такі як системи управління виробництвом, системи управління відносинами з клієнтами, бухгалтерські системи та інші.

ІС допомагають у зборі та обробці інформації для прийняття управлінських рішень.

_

1.3.1. Забезпечення безпеки інформації циркулюючої у ІТС підпріємства

Забезпечення безпеки інформації, яка циркулює у ІТС підприємства, представляє собою складне завдання управління, що вимагає координації різноманітних ресурсів. Серед цих ресурсів важливе місце займають інформаційні системи, які автоматизують бізнес-процеси підприємства, включаючи системи управління проектами, комунікацій, бази даних і комп'ютерні мережі.

Сучасні тенденції бізнесу зобов'язують підприємства зберігати та обробляти значні обсяги конфіденційної інформації, яка є доступною для численних працівників у ІТС.

1.4. Телекомунікаційні мережі

Телекомунікаційні мережі: Системи передачі даних і зв'язку, такі як локальні мережі (LAN), широкомасштабні мережі (WAN) і бездротові технології, що дозволяють ефективно обмінюватися інформацією між різними підрозділами та працівниками.

1.5. Системи зберігання даних

Системи зберігання даних: Вони включають в себе сервери та системи зберігання, які забезпечують надійне зберігання та доступ до великого обсягу даних.

1.5.1. Системи безпеки

–

Системи безпеки: Захисні заходи, такі як системи ідентифікації та аутентифікації, антивірусні програми, файрволи та системи моніторингу, щоб захистити інформацію від несанкціонованого доступу та атак.

Комп'ютерне обладнання: Сервери, комп'ютери, маршрутизатори, комутатори та інше обладнання, яке використовується для функціонування інформаційно-телекомунікаційної інфраструктури.

Програмне забезпечення: Операційні системи, бази даних, офісні програми та інші додатки, необхідні для виконання різних завдань та операцій.

IT-персонал: Кваліфіковані спеціалісти, які відповідають за розробку, впровадження та підтримку ІТС.

1.6. Роль DLP-технології в запобіганні несанкціонованому доступу

1.6.1. Основні принципи роботи DLP-технології

Для ефективної боротьби з несанкціонованим доступом і запобігання витокам конфіденційних даних, організації все частіше звертають увагу на технологію DLP (Data Loss Prevention). DLP являє собою комплексний підхід до забезпечення безпеки інформаційних систем, орієнтований на виявлення, контроль і запобігання витокам чутливих даних**.**

Data Leak/Loss/Leakage Prevention (DLP) – технології запобігання витоків конфіденційної інформації, що є власністю організації, за межі її інформаційної системи, а також комплекс технічних засобів (програмних або програмноапаратних) для запобігання витокам.

1.6.2. Моніторинг і контроль передачі даних:

DLP аналізує трафік даних у реальному часі, відстежуючи передачу інформації як усередині організації, так і за її межами. Дозволяє встановлювати політики, що визначають, які дані можуть бути передані, і хто має право здійснювати такі передачі.

–

1.6.3. Виявлення конфіденційної інформації:

Використовує механізми контенту і контекстного аналізу для ідентифікації чутливої інформації, такої як фінансові дані, персональні дані клієнтів або інтелектуальна власність. Розпізнає формати файлів, ключові слова, шаблони та інші ознаки, що вказують на конфіденційність даних.

1.6.4 Моніторинг та аналіз трендів безпеки:

Надає засоби моніторингу та аналізу, що допомагають виявляти тренди в безпеці та прогнозувати можливі загрози. Використовує дані про інциденти для постійного вдосконалення політик і заходів безпеки. Ці аспекти підкреслюють великий спектр функціональності DLP-технології та її значущість у запобіганні несанкціонованому доступу та витокам конфіденційної інформації в різноманітних сценаріях використання.

1.7 Висновок

Було проведено докладний аналіз ситуацій витоків інформації на підприємствах, що виникли внаслідок навмисних або недбалих дій працівників. Динаміка витоків за останні 5 років підкреслює актуальність впровадження систем запобігання витокам, оскільки спостерігається постійне зростання їх кількості.

Розглянуті актуальні проблеми безпеки підприємств із розвинутою IT-інфраструктурою та значним штатом співробітників виокремлюють особливості забезпечення безпеки інформаційних ресурсів і будови інформаційно-телекомунікаційної системи підприємства.

–

Зроблений аналіз технологій DLP, які відповідають за функціонал протидії витокам конфіденційної інформації та можуть бути впроваджені в склад КЗЗ, ставить за мету мінімізацію ризиків фінансових і репутаційних збитків

РОЗДІЛ 2. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТЕХНОЛОГІЇ DLP У ПРОТИДІЇ НЕСАНКЦІОНОВАНОМУ ДОСТУПУ, ТА МЕТОДИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЇ

2.1. Визначення та налаштування Data Loss Prevention (DLP)

2.1.1. Загальні видомості

Data Loss Prevention (DLP) — це стратегія та набір технологій, спрямованих на запобігання втрати конфіденційної чи важливої інформації з інформаційних систем. Ця стратегія включає в себе різні аспекти, такі як виявлення, моніторинг та захист даних від незаконного або ненавмисного витоку.

Бачення DLP в організації починається з ясного визначення її цілей. Це стратегія і технології, які спрямовані на запобігання витокам важливої інформації. Перш за все, слід провести аналіз видів даних, які потрібно захищати.

На цьому етапі також формулюються конкретні цілі використання DLP. Важливо провести інвентаризацію даних, класифікувати їх і визначити політики безпеки для різних типів інформації. Створення ефективних правил - ключовий момент.

Потім настає етап моніторингу та виявлення. Впроваджуються механізми для постійного контролю і виявлення незвичайних або потенційно небезпечних активностей з даними.

Для більш надійного захисту розробляються стратегії реагування на інциденти. Це включає в себе використання механізмів, таких як шифрування даних або обмеження доступу.

–

Важливою частиною процесу стає навчання та інформування персоналу. Усі співробітники мають бути в курсі правил і процедур використання та захисту даних.

Не менш значущим є етап регулярного оновлення політик безпеки і технічних засобів DLP. Це передбачає періодичний аналіз і оновлення, щоб враховувати нові загрози та вимоги.

Таким чином, визначення та налаштування DLP містять комплексний підхід, об'єднуючи організаційні аспекти та використання відповідної

2.1.2. Порівняння існуючих DLP рішень

Zecurion Zgate – програмне забезпечення для контролю мережевого трафіку для запобігання витоків (крадіжки, втрати, випадкової пересилання) конфіденційної інформації. Zgate відноситься до сімейства IPC / DLP-систем і дозволяє контролювати SMTP-, HTTP-, HTTPS-, FTP-і інший інтернет-трафік. Для пошуку і блокування передачі конфіденційних даних у Zgate використовуються різні технології детектування: сигнатури, лінгвістичний аналіз, регулярні вирази, метод Байєса, «цифрові відбитки» і власні.

Zecurion Zlock – програмне забезпечення для захисту від витоків конфіденційної інформації шляхом розмежування прав доступу користувачів до зовнішніх і внутрішніх пристроїв комп'ютера і до локальних і мережевих принтерів. Zecurion Zlock відноситься до сімейства IPC / DLP-систем і дозволяє архівувати роздруковуються на принтері документи і файли, що записуються на USB-, CD, DVD-носії та інші пристрої.

2.2. Symantec Data Loss Prevention

–

Symantec Data Loss Prevention (DLP): Високопродуктивне рішення, яке надає функції моніторингу, виявлення та захисту конфіденційної інформації в корпоративних мережах та системах.

McAfee Total Protection for Data Loss Prevention: Рішення від компанії McAfee, яке надає захист від витоків даних, аудит безпеки та контроль застосунків.

2.2.1. Symantec Data Loss Prevention Enforce Platform

Основним елементом продукту є платформа управління Symantec Data Loss Prevention Platform, яка забезпечує можливість визначення та розповсюдження політик запобігання втрати конфіденційної інформації на інші компоненти рішення. Цей компонент також постачає єдиний веб-інтерфейс для управління та взаємодії з продуктами лінійки SDLP.

2.2.2 Symantec Data Loss Prevention Network Discover

Компонент Symantec Data Loss Prevention Network Discover виявляє незахищені конфіденційні дані, проводячи сканування інформаційних ресурсів, таких як файлові сховища, бази даних, поштові сервери, веб-сервери і інші.

2.2.3 Symantec Data Loss Prevention Data Insight

Компонент Symantec Data Loss Prevention Data Insight дозволяє відстежувати доступ до конфіденційної інформації для автоматичного визначення власників цих даних, що сприяє підвищенню гнучкості в процесах виявлення та управління конфіденційними даними.

2.2.4 Symantec Data Loss Prevention Network Protect

–

Компонент Symantec Data Loss Prevention Network Protect розширює функціонал компонента Symantec Data Loss Prevention Network Discover, зменшуючи ризик втрати незахищених конфіденційних даних. Це досягається переміщенням цих даних з публічних сховищ на мережеві сервери в карантин або захищені сховища.

2.3. Критерії вибору DLP системи: обсяг і структура даних

Об'єм даних впливає на вибір типу DLP та сценарію роботи. Розділ про масштабованість ретельно розглядає відмінності між мережевим, змішаним і хостовим DLP. Особливу увагу приділено сценаріям роботи.

У зазвичайшій практиці при впровадженні DLP виникає питання вибору між активним та пасивним режимами роботи. У першому варіанті DLP "перерізає" всі дані, що проходять через кордони мережі, активно блокуючи неприпустимий обмін інформацією. У другому випадку система працює в повідомному режимі, не блокуючи передачу, а лише повідомляючи про підозрілі інциденти і заносячи усю інформацію в журнал подій.

Існує також змішаний режим, коли DLP "перерізає" дані, але політики налаштовуються так, що запобігають лише очевидним порушенням, дозволяючи іншому трафіку проходити без змін. Крім того, у більшості систем в активному режимі є можливість ручної перевірки, де підозрілі дані покладаються в "карантин" і чекають ручного огляду співробітником з безпеки.

Сценарій впровадження впливає на загальні витрати володіння: у довгостроковій перспективі пасивний режим вимагає значних зусиль для аналізу трафіку та розслідування, в той час як в активному режимі DLP автоматично блокує більшу частину витоків. При цьому вимоги до обладнання для всіх сценаріїв практично однакові — мінімум один потужний

сервер, хоча при невеликому навантаженні DLP можна встановити безпосередньо на проксі- поштовий або будь-який інший діючий сервер.

Набір технологій виявлення витоків, якими повинна володіти DLP-система, значно залежить від структури та переліку даних, які перш за все підлягають захисту. Узагальнений спектр доступних технологій включає сигнатурний та лінгвістичний аналіз, пошук за базами регулярних виразів та "цифровими відбитками", OCR (виявлення тексту на передаваних зображеннях) і технології машинного навчання. На жаль, на даний момент не кожна система DLP пропонує хоча б половину від зазначених технологій.

Кожна з цих технологій оптимальна лише для конкретного типу даних. "Цифрові відбитки" визнані однією з популярних і легких у використанні технологій, ефективних у виявленні статичних документів, які рідко зазнають змін. "Регулярні вирази" ідеально підходять для виявлення передачі особистих даних та інформації із типовою структурою, такою як номери рахунків, телефони, адреси і т.д. Лінгвістичні технології (морфологія) ефективно працюють із більшістю типів даних, але їхню ефективність визначає тщательність налаштувань, яку, як правило, можуть забезпечити лише фахівці-лінгвісти.

2.3.1. Критерії оцінки DLP системи: необхідність розслідування інцидентів

Дійсно, критерії оцінки DLP-системи, зокрема аспект, пов'язаний із необхідністю розслідування інцидентів, є важливим елементом визначення ефективності та функціональності цього типу захисних систем. Розслідування інцидентів в контексті DLP передбачає виявлення, аналіз та реагування на можливі витоки конфіденційної інформації.

Для оцінки DLP-системи з точки зору необхідності розслідування інцидентів важливо враховувати кілька ключових аспектів. По-перше, ефективність системи виявлення та сповіщення про потенційні порушення

–

безпеки. Це включає в себе здатність реєструвати та ідентифікувати ненормативний обіг конфіденційної інформації в режимі реального часу.

Крім того, важливим критерієм є точність розпізнавання ризикованих сценаріїв. DLP-система повинна бути здатна вчасно і точно класифікувати інциденти, враховуючи специфіку конкретного бізнес-контексту.

Також слід враховувати можливості системи автоматизованого реагування та контролю за розгортанням заходів безпеки під час розслідування інцидентів. Це включає в себе блокування небезпечних дій, ізоляцію порушників, а також автоматичне відновлення нормального режиму роботи після припинення загрози.

Оцінюючи DLP-систему з точки зору необхідності розслідування інцидентів, важливо враховувати інтеграцію з іншими компонентами безпеки та можливість взаємодії з персоналом, який відповідає за вирішення інцидентів безпеки в організації.

2.3.2. Критерії оцінки DLP системи: захист даних при зберіганні

Останнім часом дедалі частіше обговорюється проблема втрати конфіденційних даних, яку вже почали включати до комплексу рішень DLP (захист від втрат даних). Багато провідних продуктів вже оснащені системами криптографічного захисту. На перший погляд може здатися, що ймовірність втрати важливих даних менша, ніж, наприклад, можливість копіювання конфіденційних файлів на USB-накопичувачі. Проте насправді все більше витоків інформації відбувається саме через втрату магнітних стрічок, флеш-накопичувачів і ноутбуків.

Певні DLP-рішення вже вбудовують функціонал для ефективного захисту даних при їх зберіганні за допомогою сучасних алгоритмів шифрування, таких як AES (Advanced Encryption Standard), або AES-XTS.

–

2.3.3. Критерії оцінки DLP системи: масштабованість

Оцінка DLP-системи за критерієм масштабованості визначається її здатністю ефективно функціонувати та витримувати навантаження в умовах різноманітних обсягів даних та розмірів мережі. Масштабованість виявляється ключовим аспектом при впровадженні DLP, оскільки обсяг інформації, що обробляється, може значно зростати відповідно до потреб організації.

Ефективна масштабованість DLP передбачає здатність системи обробляти велику кількість даних, що транслюються через мережу, в умовах високих швидкостей передачі інформації. Це особливо важливо для компаній з великим обсягом інформації, таких як корпоративні гіганти, фінансові установи або провідні технологічні компанії.

Додатковою складовою масштабованості є здатність системи пристосовуватися до збільшення числа користувачів та пристроїв, які підключаються до мережі. Забезпечення стабільної та надійної роботи DLP в умовах ростучого числа працівників та пристроїв є критичним аспектом забезпечення інформаційної безпеки організації.

Окрім того, масштабованість DLP-системи включає в себе легкість і ефективність інтеграції з існуючими технологічними стеками та апаратурою компанії. Забезпечення сумісності та безперебійної роботи системи в різних середовищах із різними конфігураціями є важливим аспектом успішного впровадження DLP-рішення в організації різних масштабів.

2.4. Аналіз інформаційної безпеки ІТС

Аналіз інформаційної безпеки ІТС (Інформаційно-технічні системи) - це процес визначення потенційних загроз, оцінки ризиків та визначення ефективних заходів для захисту інформації та технічних ресурсів. Включає в себе перевірку

–
вразливостей, моніторинг заходів безпеки, аналіз подій та реагування на інциденти для забезпечення стійкості та конфіденційності даних в інформаційних системах.

2.4.1. Інформаційна безпека ІТС

Інформаційний захист передбачає гарантування недоступності втручань, будь то випадкових чи зловмисних, які можуть стати причиною втрати інформації або завдати збитків її власникам та зберігаючій інфраструктурі.

Система інформаційного захисту включає в себе наступні завдання:

- Класифікація інформації з обмеженим доступом.
- Запобігання витоку такої інформації.
- Прогнозування, виявлення та усунення загроз інформаційній безпеці підприємства.
- Створення механізму оперативного реагування на загрози інформаційній безпеці.
- Ефективна зупинка посягань на інформаційні ресурси підприємства за допомогою правових, організаційних і інженерно-технічних засобів.

Об'єктами безпеки є:

- Інформація про персонал (керівництво, співробітники).
- Інформація щодо використовуваних технологій.
- Інформація про клієнтів.
- Інформація про проекти.
- Інформаційні ресурси (інформація з обмеженим доступом, комерційна таємниця, конфіденційна інформація).

Структурна інформаційна безпека підприємства – це комплексна система заходів та організаційних елементів, спрямованих на забезпечення надійності та стійкості інформаційної інфраструктури. Цей підхід передбачає

–
взаємодію різноманітних компонентів для створення цілісної системи, яка має захищати інформацію від можливих загроз та небезпек.

На перший погляд, структурна інформаційна безпека охоплює велику кількість аспектів та елементів, зокрема:

Організаційна Структура: Забезпечення інформаційної безпеки починається з правильної організації внутрішньої структури підприємства, визначенням відповідальності та розподілом повноважень.

Політики та Процедури: Розробка та впровадження чітких політик та процедур, спрямованих на захист конфіденційної інформації та попередження можливих загроз.

Технічні Засоби Захисту: Використання спеціалізованих технічних рішень, таких як антивіруси, системи виявлення вторгнень, файрволи, що забезпечують ефективний захист мережі та інфраструктури.

Освіта та Навчання: Забезпечення свідомості персоналу щодо інформаційної безпеки, навчання співробітників правилам та процедурам безпеки.

Аудит та Моніторинг: Постійне відстеження та аналіз подій в мережі для своєчасного виявлення аномалій та потенційних загроз.

Ці компоненти взаємодіють і взаємодіють, утворюючи інтегровану систему інформаційної безпеки, яка працює як єдина сутність для захисту цінної інформації підприємства від різних ризиків та загроз.

Основу інформаційної системи складає база даних первинних документів, також до неї входять сервери обробки та зберігання даних із серверами додатків які реалізують таки компоненти ІТС як системи електронної пошти, системи керування та ведення проектів, системи контролю версій, бази знань.

Загальна схема ІТС типового підприємства зображена на рисунку 2.1

–

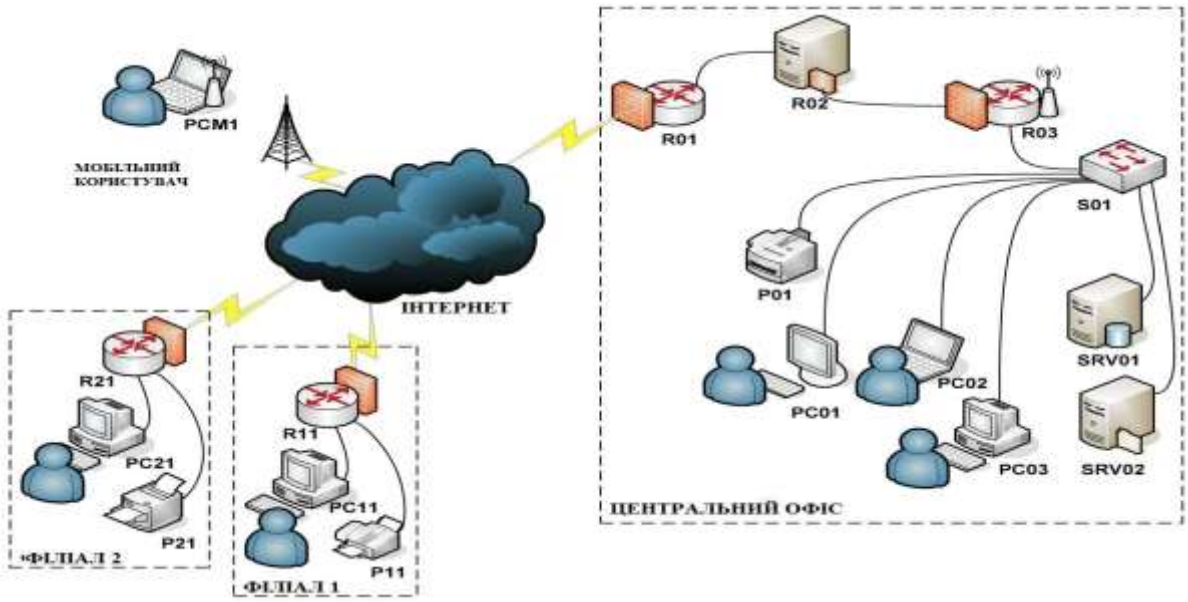

Рисунок 2.1 - Загальна схема ІТС типового підприємства

2.4.2 Аналіз інформації циркулюючої на типовому підприємстві

Вся інформація, яка обертається на підприємстві, тісно пов'язана з клієнтами, бізнес-процесами та особистими даними і має конфіденційний характер. Працівники отримують доступ до цієї інформації відповідно до своєї посади та виробничих обов'язків.

Таблиця 2.1 – Інформація циркулююча на підприємстві

Інформація	**Режим доступу**	**Правовий режим**	**Співробітник, маючий доступ**
Проектна документація	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту працюючого із клієнтом, співробітники безпосередня працюючі над проектом
Інформація о клієнтах	Обмежений	Конфіденційна інформація	Бізнес аналітики, менеджери департаменту працюючого із клієнтом, топ менеджери

–

Щоденні звіти	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту працюючого із клієнтом, співробітник відповідальний за звіт
Місячні звіти	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту працюючого із клієнтом, співробітник відповідальний за звіт
Бухгалтерська документація	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери, бухгалтери, працівники яких стосується документа-ція
Інформація о працівниках	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаментів, працівники відділу кадрів.
Внутрішні розпорядження	Обмежений	Конфіденційна інформація	Всі працівники підприємства, для яких призначене розпорядження
Ділова переписка із клієнтами	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту відповідального за працівників, бізнес аналітики працюючи з даним клієнтом, працівники що ведуть переписку
Внутрішня ділова переписка	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту відповідального за працівників, працівники що ведуть переписку

–

Продовження таблиці 2.1

Інформація	Режим доступу	Правовий режим	Співробітник, маючий доступ
Результаті бізнес аналізу проектів	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту відповідального за працівників, бізнес аналітики працюючи з даним клієнтом
Інформаційні ресурси проектів	Обмежений	Конфіденційна інформація	Персонал що безпосередньо працює з проектом, топ менеджери
Загальна інформація о підприємстві, статут підприємства	Не обмеже-ний	Відкрита інформація	

Інформаційні потоки в межах ІТС підприємства відбуваються між працівниками та клієнтами, та дійсно із доступом до ресурсів та виробничим потребам.

Таблиця 2.2 – Аналіз інформаційних потоків типового підприємства

Інформація	Режим доступу	Правовий режим	Співробітник, маючий доступ
Внутрішня ді-лова переписка	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту відповідального за працівників, працівники що ведуть переписку

–

Ділова перепи-ска із клієнтами	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту відповідального за працівників, бізнес аналітики працюючи з даним клієнтом, працівники що ведуть переписку
Звітування місячних та денних звітів	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту працюючого із клієнтом, співробітник відповідальний за звіт
Звітування аналітичних звітів	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери, менеджери, працівники які складають звіт

Продовження таблиці 2.3

Інформація	**Режим доступу**	**Правовий режим**	**Співробітник, маючий доступ**
Розробка та поширення інформаційних ресурсів проекту	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери, менеджери, працівники що розроблюють інформаційні ресу-рсі
Узгодження проектної документації	Обмежений	Конфіденційна інформація	Клієнти, менеджери, співпрацівники що розроблюють проектні плани та документацію

–

Узгодження бухгалтерської документації	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери, менеджери, бухгалтери, працівники яких стосуються документація
Презентації проектів	Обмежений	Конфіденційна інформація	Персонал що безпосередньо працює з проектом, топ менеджери
Командний аналіз проектних планів	Обмежений	Конфіденційна інформація	Персонал що безпосередньо працює з проектом, топ менеджери

2.5. Аналіз загроз безпеці ІТС підприємства

На тлі сучасного інформаційного прогресу, виробничих технологій та зростаючої важливості інформаційних технологій для підприємств, аналіз загроз безпеці інформаційно-телекомунікаційних систем (ІТС) стає необхідністю для забезпечення надійного функціонування підприємства та захисту конфіденційної інформації.

Починаючи аналіз, слід зазначити, що в сучасному світі підприємства стають об'єктами різноманітних загроз інформаційної безпеки. Однією з ключових загроз є кібератаки, спрямовані на порушення цілісності, конфіденційності та доступності даних. Кіберзлочинці намагаються використовувати різноманітні методи, такі як віруси, троянські програми та фішингові атаки, щоб незаконно отримати доступ до інформації та завдати шкоду підприємству.

Іншим значущим аспектом є внутрішні загрози, пов'язані з недбалістю або навмисними діями власних співробітників. Зловмисники, які мають доступ до внутрішніх ресурсів підприємства, можуть використовувати свої

привілеї для незаконного доступу або розголошення конфіденційної інформації.

Крім того, існує загроза фізичних втручань, таких як крадіжка обладнання або документів, що може призвести до втрати важливих даних та порушення роботи ІТС підприємства.

У світлі цих реальних загроз, аналіз безпеки ІТС стає важливою частиною стратегії підприємства. Виявлення потенційних вразливостей, розробка ефективних заходів захисту та постійний моніторинг безпекових процесів є ключовими етапами у забезпеченні стійкості підприємства до сучасних викликів і загроз інформаційної безпеки.

2.5.1. Загрози порушення конфіденційності

Конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом. Конфіденційність передбачає забезпечення захисту даних, що передаються, від пасивних атак, тобто захист потоку даних від можливості його аналітичного дослідження.

–

Рисунок 2.2 – Базові загрози безпеці інформаційних ресурсів

Загрози порушення конфіденційності інформації включають в себе різноманітні аспекти, такі як розкрадання (копіювання) та витоки інформації. В основі атак, спрямованих на порушення конфіденційності, лежать такі види, як пасивне підслуховування та перехоплення в каналах зв'язку, незаконне використання прав і викрадання ключової інформації.

Витоки або втрати інформації мають потенціал підірвати авторитет компаній і завдати значних фінансових збитків. За даними аналітиків, прогнозується, що світовий корпоративний сектор в найближчі роки може зазнати втрат приблизно на рівні $1 трлн. щорічно внаслідок витоків конфіденційних даних.

2.5.2. Загрози порушення цілісності

Цілісність інформації - це властивість, яка забезпечує, що інформацію не можна модифікувати несанкціонованим чином, ні користувачем, ні

–

процесом.Загрози цілісності можуть виникнути щодо даних, програм та апаратури. Цілісність даних та програм може бути порушена при несанкціонованому знищенні, додаванні непотрібних елементів і модифікації записів про стан рахунків. Також може бути порушена шляхом зміни порядку розташування даних, формування фальсифікованих платіжних документів у відповідь на законні запити та активної ретрансляції повідомлень з затримкою.

Несанкціонована модифікація інформації про безпеку системи може викликати несанкціоновані дії, такі як невірна маршрутизація або втрата передаваних даних, або спотворення сенсу переданих повідомлень. Цілісність апаратури може бути порушена її пошкодженням, викраданням або незаконною зміною алгоритмів роботи.

2.5.3. Загрози порушення доступності

В першу чергу, слід врахувати можливість фізичних атак або негараздів, таких як природні катастрофи, пожежі або поводження з обладнанням. Ці події можуть призвести до непередбачуваного відмови у доступі до інформації та послуг.

Кіберзагрози, такі як хакерські атаки або зловмисні програми, також є серйозною загрозою для доступності. Зловмисники можуть зблокувати доступ до важливих систем, вимагати викуп або завдати інших шкідливих наслідків.

Крім того, технічні проблеми, такі як недоліки в мережевому обладнанні, можуть також вплинути на доступність інформації. Відсутність необхідної бекап-системи або неефективна стратегія відновлення може призвести до втрати доступу до даних.

Загрози DPL вимагають комплексного підходу до забезпечення надійності і доступності інформаційних ресурсів. Спроби попередження,

–
виявлення та відновлення після інцидентів є важливими етапами у забезпеченні неперервного доступу до інформації.

Доступність, одна з ключових властивостей інформаційної системи, визначає можливість користувача або процесу, обладнаного необхідними правами, використовувати ресурси системи відповідно до встановлених правил політики безпеки. Це означає, що доступ до інформації повинен бути наданий оперативно та відповідно до установлених вимог.

Загрози, які можуть вплинути на доступність даних, походять від можливого відмову об'єкта (користувача або процесу) у доступі до законно виділених служб чи ресурсів. Такі загрози можуть виявитися в захопленні ресурсів, блокуванні ліній зв'язку несанкціонованими об'єктами та внаслідок передачі по ним інформації. Це може призвести до ненадійності обслуговування в системі та впливу на достовірність і своєчасність доставки платіжних документів.

Згідно з вимогами стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010, інформаційна безпека повинна забезпечувати збереження конфіденційності, цілісності та доступності інформації, а також може враховувати інші властивості, такі як автентичність, спостережність, неспростовність та надійність.

Автентичність, наприклад, гарантує, що суб'єкт або ресурс ідентичні їхнім заявленням. Спостережність дозволяє фіксувати дії користувачів та процесів для уникнення порушення політики безпеки, або для встановлення відповідальності за певні дії. Неспростовність забезпечує засвідчення дій або подій так, що їхнє спростування стає неможливим.

–

Рисунок 2.3 – Модель реалізації загроз

Шляхом хакерського перехоплення інформації, що рухається в системах зв'язку та комп'ютерній техніці, використовуючи розвідувальні технічні засоби та програми для несанкціонованого доступу та програмно-математичних втручань в процес обробки та зберігання інформації:

Шляхом підслуховування конфіденційних переговорів у службових приміщеннях, службовому та особистому автотранспорті тощо.

Шляхом використання слабкої охорони інформації під час переговорних процесів між підприємствами та іноземними чи вітчизняними фірмами.

Шляхом використання окремих працівників підприємства, які можуть допустити недозволений доступ або розголошення конфіденційної інформації з особистих мотивів.

За ознакою джерела загрози безпеки комерційної установи вирізняються:

–

Загрози від конкурентів, які можуть використовувати недобросовісні методи, такі як економічний шпигунаж, переманювання персоналу та інші, для зміцнення своїх позицій на ринку.

Загрози від кримінальних структур і окремих зловмисників, які можуть шукати власну користь за рахунок захоплення контролю над підприємством, розкрадання власності тощо.

Загрози від нелояльних співробітників, які свідомо можуть завдати шкоду підприємству з особистих мотивів.

За видами можливих джерел загроз інформаційній безпеці виділяються наступні класи загроз:

Загрози внутрішніх порушників, які здійснюють погрози безпосередньо в інформаційній системі, включаючи користувачів й інші особи з доступом.

Загрози зовнішніх порушників, які реалізують погрози зовнішніми мережами зв'язку загального користування та мережами міжнародного інформаційного обміну.

2.6. Розгляд моделей загроз та порушників інформаційної безпеки

Розгляд моделей загроз та порушників інформаційної безпеки виявляється критично важливим у контексті сучасного цифрового світу, де зростаюча кількість технологічних засобів і зв'язків створює ситуацію, де безпека інформації стає пріоритетним завданням для організацій та індивідів.

Однією з основних моделей загроз є внутрішній порушник. Це може бути співробітник організації, який має доступ до конфіденційної інформації і вирішує використовувати цю інформацію для особистої вигоди або навіть зловживати нею. Такі порушники можуть викликати серйозні загрози безпеці, оскільки вони оперують всередині самої системи.

–

Ще однією моделлю є зовнішні загрози, такі як хакери, кіберзлочинці та інші агенти, які намагаються незаконно отримати доступ до інформації або завдати шкоду системі. Ці загрози можуть включати різні форми атак, від вірусів та троянських коней до фішингу та атак на вибуховість.

Додатковою моделлю є загрози в результаті технічних неполадок або природних катастроф. Відмови обладнання, системні помилки або природні події, такі як повені чи землетруси, можуть призвести до втрати даних та порушення інформаційної безпеки.

Необхідно також враховувати загрози, пов'язані з людським фактором. Соціальний інжиніринг, який включає в себе обман або маніпуляцію людей з метою отримання доступу до системи або конфіденційної інформації, стає все більш поширеним.

Загалом розгляд моделей загроз та порушників інформаційної безпеки є необхідним етапом для створення ефективних стратегій захисту. У світі, де обсяги даних і їхнє значення непередбачувано зростають, розуміння загроз і розробка відповідних заходів безпеки стають вирішальним завданням для забезпечення інформаційної безпеки на всіх рівнях.

2.6.1. Модель загроз

Згідно з вимогами до забезпечення безпеки інформаційної системи, визначені наступні сценарії можливих втручань:

Використання спеціально створених програмних або технічних засобів для цілеспрямованого порушення цілісності інформації під час її обробки, передачі та зберігання в межах системи.

Порушення санкціонованої доступності інформації в системі шляхом впливу на працездатність програмного забезпечення, засобів зв'язку, маршрутизаторів або їх перепрограмування, включаючи дефекти, збої, аварії та відмови апаратно-програмних комплексів.

–

Несанкціонований доступ до конфіденційної інформації через технічні засоби системи, що може викликати витік та спотворення конфіденційних даних через технічні канали.

Розголошення конфіденційної інформації та недозволені дії від осіб, які мають право доступу до конфіденційних даних, реалізуючи загрози як в межах своїх повноважень, так і поза ними.

Таблиця 2.5 – Загальна модель загроз безпеці інформаційних ресурсів

Джерело загрози безпеці КІ	**Рівень реалізації загрози безпеці КІ**	**Типи об'єктів середовища**	**Загроза безпеці ІзОД**
Комп'ютерні зловмисники, що здійснюють цілеспрямовану деструктивну дію	ОС	Файли даних з ІзОД	К, Ц, Д
	ПЗ	Бази даних з ІзОД, прикладні програми доступу і обробки ІзОД, ПК	К, Ц, Д
Постачальники програмно-технічних засобів, витратних матеріалів, послуг і т.п., підрядчики, що здійснюють монтаж, усконалагоджувальні роботи устаткування і його ремонт	ОС	Файли даних з ІзОД	К, Ц
	ПЗ	Бази даних з ІзОД, прикладні програми доступу і обробки ІзОД, ПК	К, Ц

Продовження таблиці 2.5

Джерело загрози безпеці КІ	**Рівень реалізації загрози безпеці КІ**	**Типи об'єктів середовища**	**Загроза безпеці ІзОД**

–

Співробітники, що діють в рамках наданих повноважень	Фізичний рівень	Лінії зв'язку, апаратні і технічні засоби, сервера, фізичні носії інформації, маршрутизатори, комутатори, концентратори, програмні компоненти передачі даних по комп'ютерних мережах (мережеві сервіси)	К, Ц, Д
	ОС	Файли даних з ІзОД	К, Ц, Д
	ПЗ	Бази даних з ІзОД, прикладні програми доступу і обробки ІзОД, програмні компоненти передачі даних по комп'ютерних мережах	К, Ц, Д
Співробітники, що діють поза рамками наданих повноважень	ОС	Файли даних з ІзОД	К, Ц
	ПЗ	Бази даних з ІзОД Прикладні програми доступу і обробки ІзОД	К,Ц

Ключовими елементами засобів автоматизації інформаційних систем, розташованими в порядку їхньої важливості, є:

Серверні компоненти, такі як бази даних та додаткові програми. Елементи комунікаційного устаткування, включаючи компоненти систем передачі даних, такі як маршрутизатори, концентратори та модеми.

Спеціалізовані робочі місця (АРМ) з встановленими системами криптографічного захисту інформації (СКЗІ).

Об'єктами захисту в межах засобів автоматизації є:

Програмно-технічний комплекс автоматизованої системи в цілому, який обробляє конфіденційну інформацію.

–

Сервери баз даних та додаткові програми.

Спеціалізовані робочі місця з встановленими системами криптографічного захисту інформації.

Робочі станції кінцевих користувачів інформаційної системи.

Канали зв'язку, які використовуються для обміну інформацією в межах інформаційної системи.

Приміщення, де розташовуються серверні компоненти програмно-технічних комплексів і робочі станції кінцевих користувачів, в залежності від характеру оброблюваної інформації.

Система інформаційної безпеки інформаційної системи будується враховуючи конкретні загрози та основні компоненти системи, на які ці загрози можуть впливати.

2.6.2. Модель порушника

Джерелами загроз непоширення секретної інформації в інформаційних системах можуть бути:

Зовнішні порушники: розвідувальні служби держав, кримінальні структури, конкуренти, недобросовісні партнери, зовнішні суб'єкти (фізичні особи). Зовнішні порушники можуть:

Здійснювати несанкціонований доступ до каналів зв'язку поза межами службових приміщень.

Проникати через автоматизовані робочі місця, підключені до мереж зв'язку загального користування та/або мереж міжнародного інформаційного обміну.

–

Використовувати спеціальні програмні дії для несанкціонованого доступу до інформації, такі як віруси, шкідливі програми та алгоритмічні або програмні закладки.

Здійснювати несанкціонований доступ через елементи інформаційної інфраструктури, які опиняються за межами контрольованої зони під час життєвого циклу (модернізація, супровід, ремонт, утилізація).

Здійснювати несанкціонований доступ через інформаційні системи взаємодіючих відомств, організацій і установ при їхньому підключенні до інформаційних систем.

Внутрішні порушники можуть бути:

Особи з санкціонованим доступом до контрольованої зони, але без доступу до конфіденційної інформації.

Зареєстровані користувачі інформаційних ресурсів з обмеженими правами доступу до інформаційних систем з робочих місць.

Користувачі, що здійснюють віддалений доступ до інформаційних ресурсів.

Користувачі з повноваженнями системного адміністратора або адміністратора безпеки інформаційних систем.

Програмісти-розробники та особи, що забезпечують супровід прикладного програмного забезпечення.

Розробники та особи, що забезпечують постачання і супровід в інформаційних системах.

Можливості внутрішніх порушників значно залежать від ефективності режимних та організаційно-технічних заходів в межах контрольованої зони.

–

Залежно від потенційних можливостей внутрішніх порушників можна представити у вигляді наступної ієрархії рівнів (кожний наступний рівень включає в себе функціональні можливості попереднього):

Перший рівень – визначається можливістю запуску фіксованого набору завдань (програм), які реалізують передбачені функції обробки інформації.

Другий рівень – визначається можливістю створення і запуску власних програм з новими функціями обробки інформації.

Третій рівень – визначається можливістю управління функціонуванням ІС, тобто впливом на базове програмне забезпечення системи і конфігурацію її устаткування.

Четвертий рівень – визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супровід програмно-апаратного забезпечення ІС, включаючи власні засоби з новими функціями обробки інформації.

За рівнем знань про ІС всіх порушників можна класифікувати як таких, що:

Володіють інформацією про функціональні особливості ІС, основні закономірності формування масивів даних та потоків запитів до них, вміють користуватися штатними засобами.

Володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їх обслуговування.

Володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації ІС.

Володіють інформацією про функції та механізм дії засобів захисту.

–

Класифікація порушників за рівнем можливостей та рівнем знань наведена згідно НД ТЗІ 1.4-001-2000 Типового положення про службу захисту інформації.

2.6.3. Аналіз загроз витоків інформаційних ресурсів ІТ підприємства

У дипломній роботі модель загроз витокам інформаційних ресурсів в ІТ підприємстві розглядатиметься, враховуючи найзначущу загрозу внутрішніх порушників - навмисних або ненавмисних дій персоналу.

У таблиці 2.6 представлена модель загроз безпеці інформаційних ресурсів, джерелом яких є навмисні та ненавмисні дії персоналу.

Таблиця 2.6 – Модель загроз безпеці інформаційним ресурсам

Перелік загроз	**Імовірність реалізації загрози**	**Небезпека загрози**
Загрози несанкціонованого доступу до інформації		
Загрози знищення, розкрадання носіїв інформації шляхом фізичного доступу до елементів ІС		
Крадіжка носіїв інформації	Середня	Висока
Крадіжка ключів доступу	Висока	Висока
Крадіжки, модифікації, знищення інформації.	Висока	Висока
Несанкціонований доступ до інформації при технічному обслуговуванні (ремонті, знищення) вузлів ПЕОМ	Низька	Середня
Несанкціоноване відключення засобів захисту	Висока	Висока
Загрози навмисних дій внутрішніх порушників		
Витік даних від порушення експлуатації програмного забезпечення	Висока	Висока
Компрометація інформації за допомогою відновлення середовища, що повторно використовується або викинуто	Висока	Висока
Передача конфіденційної інформації, з використанням електронної пошти	Висока	Висока

–

Витік даних від неавторизованого використання обладнання/програмного забезпечення	Середня	Висока
Передача нешифрованої інформації, що захищається, в зовнішню мережу	Середня	Висока
Передача зашифрованої інформації, що захищається, в зовнішню мережу	Середня	Середня
Витік інформації за рахунок запису інформації, що захищається на знімні носії (USB накопичувачі і т. д.)	Середня	Висока
Витік інформації за рахунок друку документів, які містять конфіденційну інформацію	Висока	Висока
Компрометація інформації за допомогою шахрайського копіювання даних	Висока	Висока
Компрометація інформації за допомогою нелегального оброблення даних	Висока	Висока
Компрометація інформації за рахунок зловживання працівником правами доступу до інформації	Середня	Висока
Компрометація інформації за рахунок підробки прав доступу до інформації	Середня	Середня
Доступ, модифікація, знищення інформації особами, не допущеними до її обробки	Висока	Висока
Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки	Висока	Висока

Продовження таблиці 2.6

Перелік загроз	Імовірність реалізації загрози	Небезпека загрози
Загрози ненавмисних дій користувачів і порушень безпеки функціонування		
Витік даних від недбалості персоналу	Висока	Висока
Витік даних від порушення експлуатації обладнання/ програмного забезпечення	Середня	Висока
Витік даних від неавторизованого використання обладнання/програмного забезпечення	Середня	Висока
Компрометація інформації за рахунок помилки/недбалості персоналу під час оброблення даних	Середня	Висока
Втрата ключів доступу	Висока	Висока
Ненавмисна модифікація (знищення) інформації співробітниками	Висока	Висока
Ненавмисне відключення засобів захисту	Низька	Середня

Під небезпекою загрози розуміється її можливий вплив на безпеку інформаційних ресурсів підприємства, який може привести до негативних наслідків.

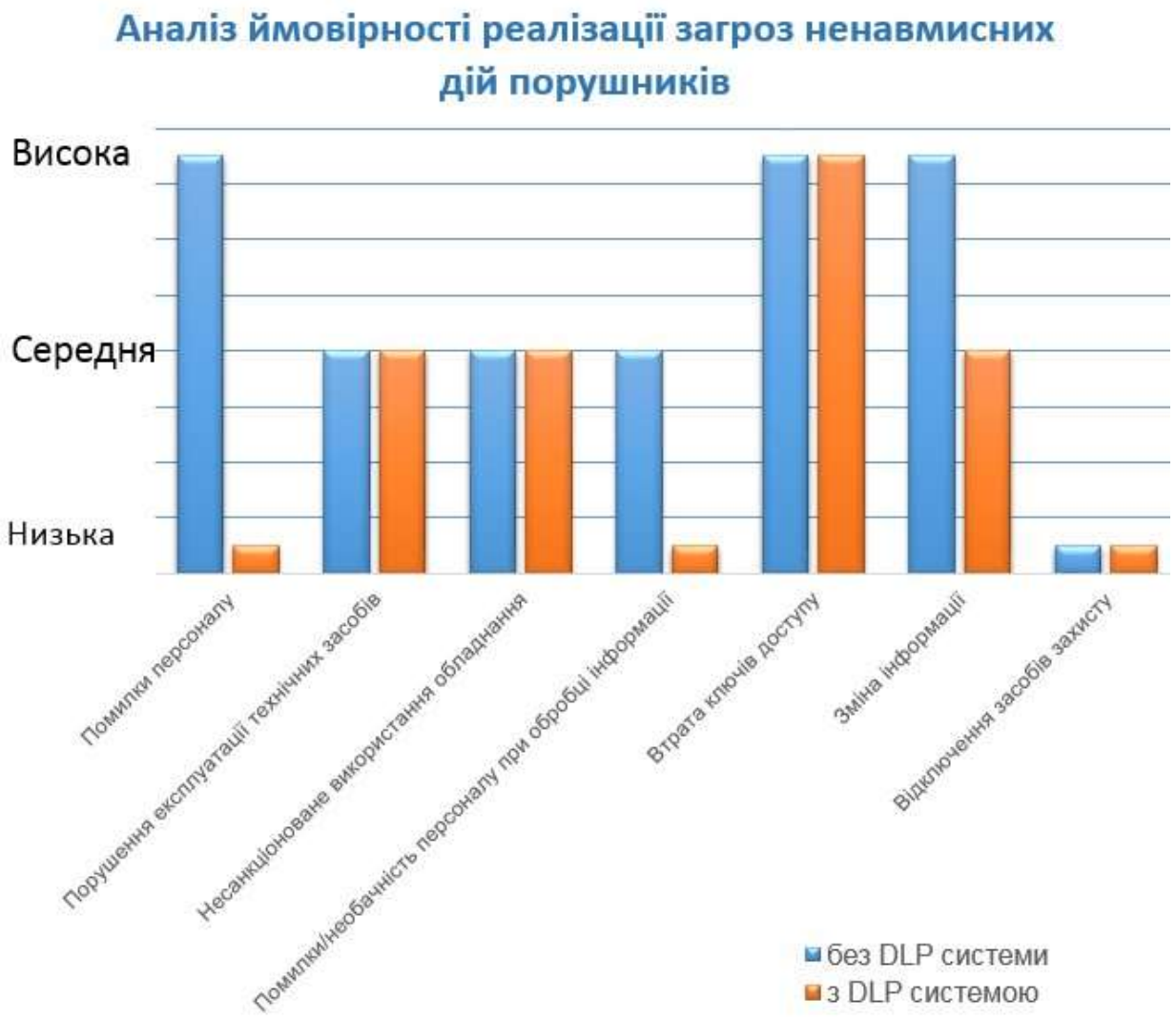

Рисунок 2.4 – Порівняльний аналіз ймовірностей реалізації загроз від ненавмисних дій внутрішніх порушників

На рисунку 2.4 наведена порівняльна характеристика ймовірностей реалізації загроз безпеці інформаційних ресурсів від навмисних дій внутрішніх порушників, До та Після впровадження DLP-системи, яка відображає ефективність використання системи протидії витокам конфіденційної інформації на основі DLP.

2.7. Висновок

У другому відділі досліджено структуру існуючих рішень для запобігання витоку конфіденційної інформації (DLP), методи забезпечення інформаційної безпеки, що базуються на використанні цих рішень, та їх вплив на моделі інформаційної безпеки в інформаційно-технічній системі (ІТС) підприємства. Були ретельно розглянуті та проаналізовані загрози безпеки в типовій ІТС підприємства, проведений аналіз впливу використання моделей інформаційної безпеки, заснованих на використанні DLP-систем, на загальний стан інформаційної безпеки.

Виявлено, що розглянуті моделі забезпечення інформаційної безпеки мають позитивний вплив на загальний стан інформаційної безпеки в межах ІТС підприємства. Ураховуючи швидкий розвиток ІТС на сучасних підприємствах та зростання інформаційно-телекомунікаційних потреб сучасного бізнесу, а також обсяг великої кількості даних, що перебувають в обігу, використання засобів захисту інформації стає необхідною умовою для життєздатності підприємства.

У контексті динаміки сучасного ІТС та зростання обсягу інформації, яка обробляється, використання традиційних рішень інформаційної безпеки не забезпечує достатнього рівня захисту від існуючих та нових загроз, зокрема від внутрішніх порушників. Використання моделей інформаційної безпеки, що ґрунтуються на DLP-системах, є ефективним заходом для запобігання витоку конфіденційної інформації.

DLP-система розглядається як необхідна складова частина комплексної системи захисту, метою якої є мінімізація ризиків прямих і непрямих фінансових наслідків витоку конфіденційної інформації.

РОЗДІЛ 3. ТЕХНОЛОГІЯ ПРОТИДІЇ НЕСАНКЦІОНОВАНОМУ ДОСТУПУ НА БАЗІ DLP

Безпека конфіденційної інформації в інформаційних системах здійснюється через використання системи захисту, що включає організаційні заходи та технічні засоби захисту. Ці заходи охоплюють широкий спектр заходів, таких як шифрування, інструменти для запобігання несанкціонованого доступу, запобігання витокам через технічні канали, і програмні/технічні засоби впливу на технічні засоби обробки конфіденційної інформації, а також використання інформаційних технологій в межах інформаційної системи.

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

До технічних засобів, які дозволяють обробку конфіденційної інформації, входять засоби вичислювальної техніки, інформаційно-вимірювальні комплекси, мережі передачі, приймання та обробки інформації, а також програмні засоби захисту інформації, що використовуються в інформаційній системі.

Для забезпечення безпеки конфіденційної інформації під час її обробки в інформаційних системах підприємства необхідно захищати всі можливі канали витоку та втрати інформації.

Для створення ідеальної системи захисту від витоків інформації та організації робіт по захисту конфіденційної інформації, портібно виконати наступні кроки:

Визначити загрози безпеці інформації під час її обробки та транспортування, формуючи на їх основі моделі загроз.

Розробити систему захисту інформації, спрямовану на нейтралізацію визначених у моделі загроз.

Перевірити готовність для встановлення нових правил та програм на пристроях обробки інформації.

Забезпечити співробітників служби безпеки підприємства правилами роботи.

Створити систему слідкування за співробітниками, які мають доступ до конфіденційної інформації.

Створити систему захисту апаратно-програмного забезпечення.

Створити систему фізичної безпеки співробітників.

3.1. Опис існуючого підпріємства

Для аналізу було взято імовірне підприємство під назвою "Intelin (Інтелектуальні іновації)", топологічна структура якого подана на рисунку 3.1. Усі пристрої, включаючи мережеві, необхідні для операцій локальної та глобальної мереж, виглядають наступним чином:

Cisco switch 2960 – 2;

Cisco router 2911 – 2;

Sico Server-PT – 2;

PC – 10.

Система організована за топологічною структурою "Зірка". Топологія "Зірка" характеризується наявністю чітко виділеного центрального вузла, до якого з'єднуються всі інші абоненти. Вся взаємодія інформацією здійснюється виключно через центральний комп'ютер, на який покладається значно більше обчислювального навантаження. Отже, центральний комп'ютер здатний виконувати тільки мережеві функції, і йому не призначено виконувати інші завдання. Зрозуміло, що обладнання мережі центрального вузла має бути значно більш складним порівняно з обладнанням периферійних вузлів. В даному випадку не існує рівноправності між абонентами, оскільки центральний комп'ютер є потужнішим і відповідає за всі функції управління обміном інформації.

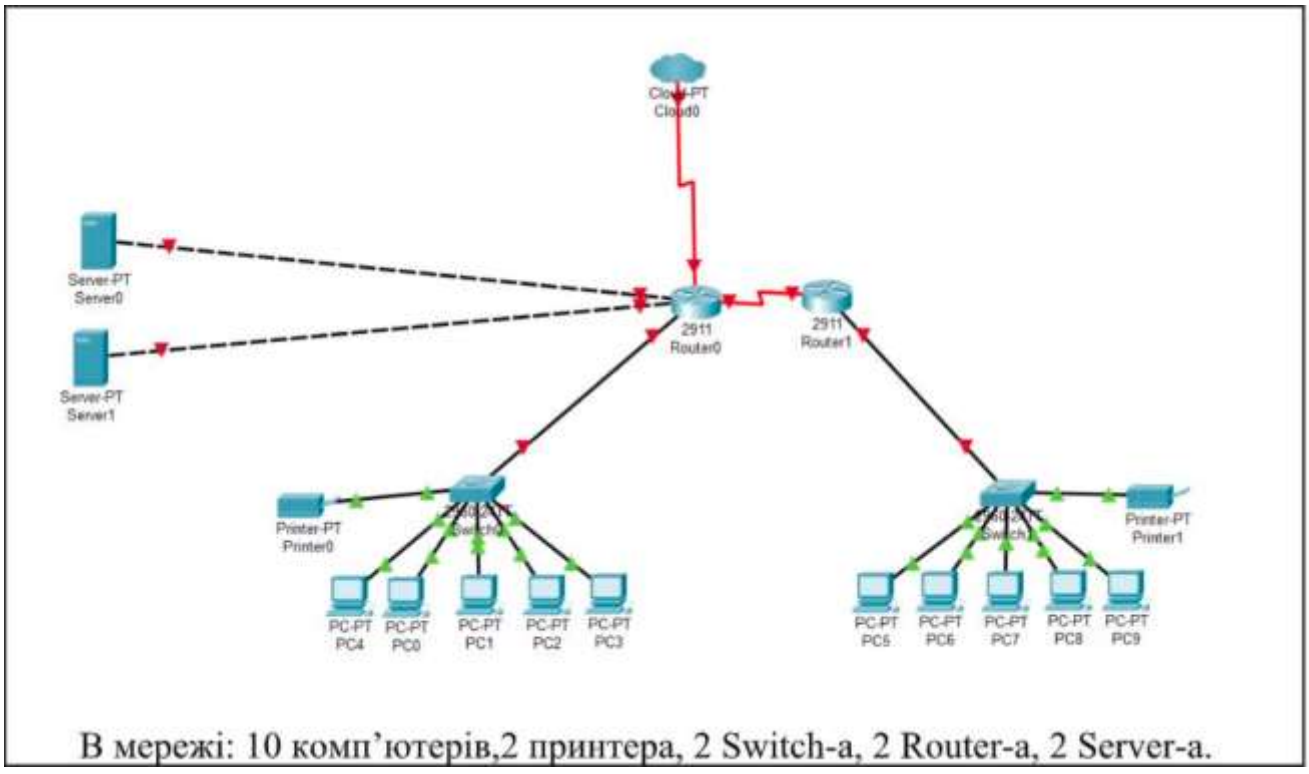

Рисунок. 3.1 Топологія локальної мережі фірми 'Intelin'

Фізичний дизайн можна знайти на малюнку 3.2. У приміщенні офісу підприємства розташовані чотири кімнати, призначених для різних потреб. Дві

з них відведені для персоналу, ще одна служить серверною, а в четвертій розташовано офіс керівника відділу, обладнаний роутерами. Усі кімнати мають скляні розсувні двері, а в кожній з них розміщено по дві розетки. Вікон немає, оскільки приміщення знаходиться в підвалі.

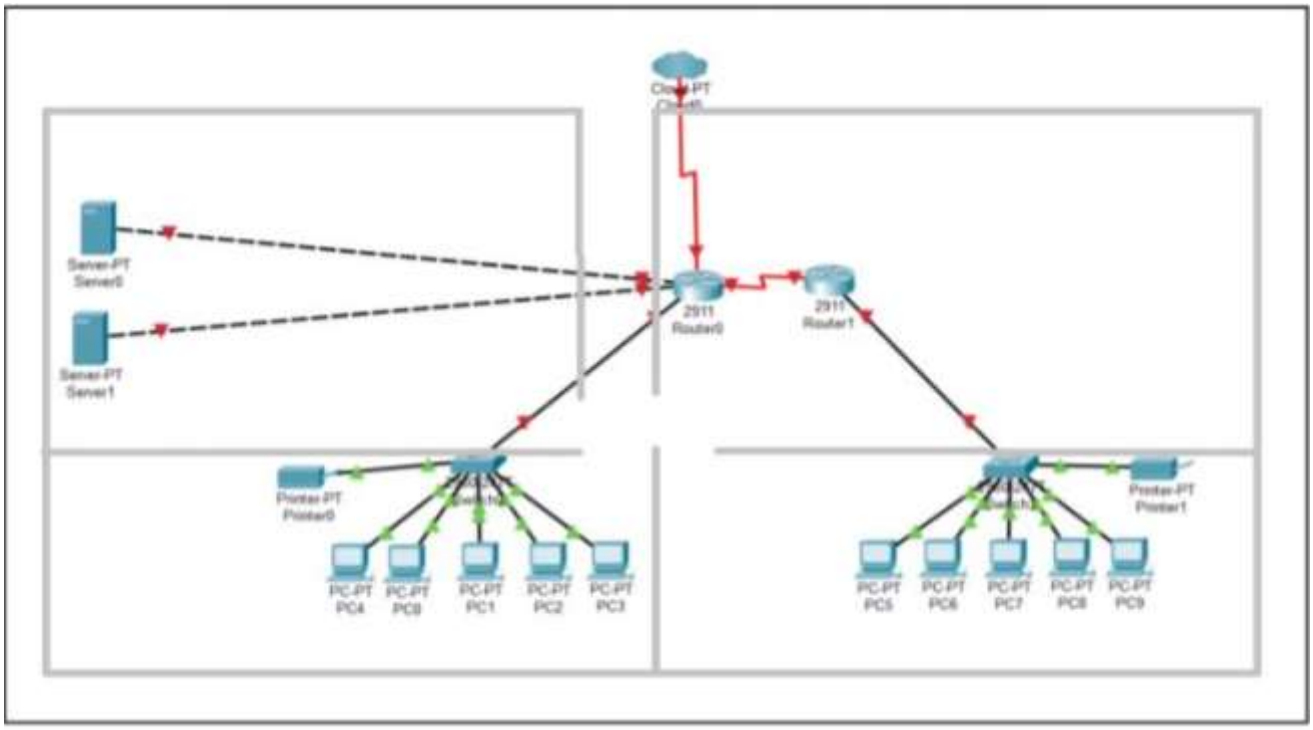

Рисунок.3.2 Імітація фізичної моделі кімнати.

На роутерах встановлено системи IDS та Firewall. На кожному комп'ютері встановлено антивірус. У випадку взлому серверів передбачено можливість виконання резервного копіювання.

Вид діяльності - збереження та обробка даних ФОП та бізнесів.

Зберігаються та оброблюються такі дані: повні імена, електронні адреси, фізичні адреси, кошти, історія покупок та номери телефонів клієнтів. Обробка відбувається у формі таблиць Oracle,Firebird

Приблизний обсяг обробки даних на місяць становить 100 Гб.

У фірмі працює 12 співробітників, які відносяться до різних відділів. Технічне відділення налічує 4 особи (повний доступ), відділ управління - 4 особи (повний доступ), відділ офісних працівників - 4 особи (обмежений доступ).

Характеристики використованої техніки:

Роутер: Cisco 2911 router

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

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

-Стандарти Wi-Fi : 802.11b/g/n

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

-Додаткові інтерфейси :

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

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

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

2 порти USB 4-пін USB тип A.

-Пам'ять:

Стандартна пам'ять:512 МБ

Максимум пам'яті: 2 Гб

Технологія пам'яті: DRAM

Флеш-пам'ять: 256 МБ

Switch: Cisco switch 2960

Сервер: Cisco UCS C240 M5

-Процесор Intel Xeon Scalable

-Кількість ядер до 28 ядер

Форм-фактор 2U

-Максимально процесорів 2

-Тип памяти DDR4

-Максимально слотів пам’яті 24

-Формат дисків SFF 2,5, LFF 3,5

-Максимальна кількість дисків 26

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

-RAID-контроллер 12 Гбит/с SAS.

Характеристики ПК:

-Модель: Logicpower 2013-400 Tower new

-Процесор: Intel Core i3-6100 (2 ядра по 3.7GHz), 8 MB cache

-Материнська плата: ASUS H110 M-K

-Оперативна пам’ять: 12 GB DDR3

-Постійна пам’ять: 120 GB SSD + 500 GB HDD

-Графіка: інтегрована Intel HD Graphics 530

-Блок живлення: SeaSonic S12III-500

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

-Оптичний привід: нема.

Система захисту від витоків інформації використовує Outpost Firewall Pro, вбудований антивірус Windows Defender у Windows 10 та функції роутерів Cisco, таких як Cisco Security Manager, VPN encryption, Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, Cisco IOS Content Filtering, AAA, DES, 3DES, AES.

Існують обмеження доступу для звичайних співробітників до серверної кімнати та адміністративних функцій управління інформацією в базах даних. Однак комплексна система DLP не впроваджена.

Всі дії співробітників фірми здійснюються відповідно до Закону України "Про захист персональних даних". Цей закон регулює правові відносини, пов'язані з захистом та обробкою персональних даних, і спрямований на захист основних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя у зв'язку з обробкою персональних даних.

Зазначений закон поширюється на діяльність, пов'язану з обробкою персональних даних, що здійснюється повністю або частково за допомогою автоматизованих засобів, а також на обробку персональних даних, які містяться у картотеці чи призначені для внесення до картотеки, за допомогою неавтоматизованих засобів.

3.2. Розгортання комплексоної DLP-системи і перевірка працеспроможності

Важним кроком для оптимізації ефективності DLP є розгортання комплексної системи запобігання витоків інформації на підприємстві. З урахуванням того, що для такої системи необхіден адміністратор, виникає необхідність вирішення юридичних питань, оскільки в його владі опиниться вся інформація, перехоплена системою, а також всі дані серверів. В зв'язку з цим буде необхідно виконати такі юридичні дії:

Внесення додаткових пунктів до трудових договорів.

Зміни у робочому розпорядку працівників.

Розробка додаткових політик щодо використання систем обробки інформації.

Наступним етапом буде вибір комплексної DLP-системи. Облік даних ведеться за допомогою Oracle, Firebird, оптимальним варіантом вважається рішення від McAfee, тому будемо розгортати саме її.

Починаючи з конфігурації місця системного адміністратора, який буде відповідальний за управління політиками безпеки та обробку даних щодо інцидентів, на його робочій станції встановлюється компонент ePolicy Orchestrator (ePO).

Далі, на робочих місцях співробітників фірми встановлюється DLP Endpoint - сервіс, який відповідає за основний контроль даних на їхніх пристроях. Цей сервіс відстежує трафік на каналах витоків інформації через різні канали, такі як електронна пошта, файлообмінники, хмарні сервіси, сервіси миттєвого обміну повідомленнями і т. д.

Потім встановлюється DLP Prevent, який контролює HTTP/HTTPs/SMTP, охоплюючи різні варіанти пошти, месенджери, блоги. При виявленні порушень політик безпеки програма дозволяє зашифрувати дані, заблокувати їх передачу і перемістити документ в карантин. McAfee DLP Prevent інтегрується з сервером MTA або веб-проксі-сервером для моніторингу трафіку електронної пошти та веб-трафіку з метою запобігання інцидентам потенційного витоку даних.

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

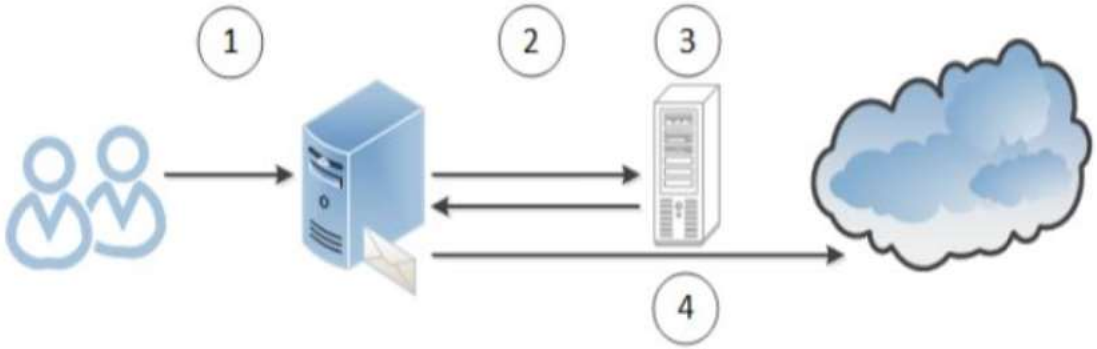

Рисунок. 3.3 Принцип дії захисту трафіку електронної пошти за допомогою DLP Prevent.

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

Сервер MTA - передає електронну пошту до McAfee DLP Prevent.

McAfee DLP Prevent - отримує з'єднання SMTP від сервера MTA і: Аналізує компоненти повідомлення електронної пошти.

Виділяє текст для ідентифікації вмісту за його відбитками та проводить аналіз за встановленими правилами.

Перевіряє повідомлення електронної пошти на предмет відповідності політикам безпеки.

Додає заголовок X-RCIS-Action.

Надсилає повідомлення на попередньо налаштований проміжний вузол. У даному випадку в якості проміжного вузла використовується вихідний сервер MTA.

Сервер MTA - засновуючись на інформації, отриманій з заголовка X-RCIS-Action, виконує відповідні дії щодо обробки електронної пошти.

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

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

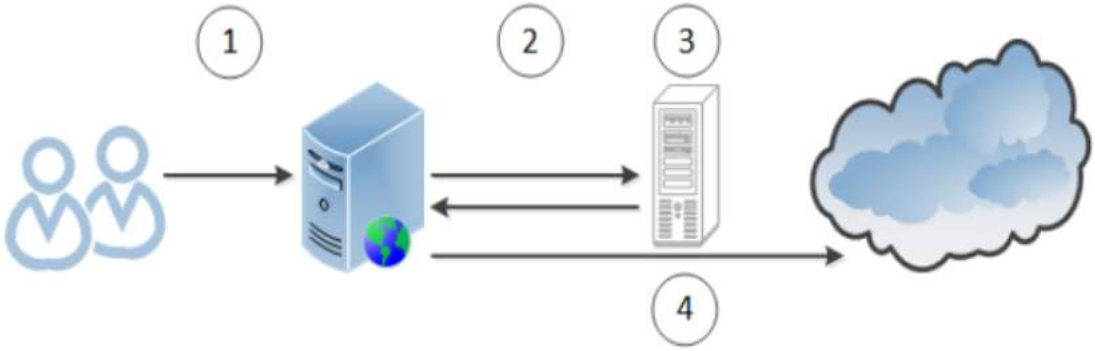

Рисунок. 3.4 Принцип дії захисту web-трафіку за допомогою DLP Prevent.

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

Веб-проксі-сервер направляє веб-трафік до McAfee DLP Prevent.

McAfee DLP Prevent перевіряє веб-трафік і повертає його на веб-проксі-сервер для дозволу або блокування передачі через сервер призначення.

Веб-проксі-сервер надсилає перевірений веб-трафік на відповідний адресу призначення.

Після цього встановлюється DLP Monitor, який в реальному часі відслідковує корпоративну мережу, проводить розслідування інцидентів та аналізує трафік через протоколи FTP, HTTP, IMAP, IRC, LDAP, POP3, SMB, SMTP. Також він проводить аналіз даних в усій базі даних на сервері.

McAfee DLP Monitor використовується для вивчення обсягу та типів даних, що пересуваються через мережу. Він не блокує або не змінює мережевий трафік, що дозволяє інтегрувати його в корпоративне мережеве середовище без впливу на реальний трафік.

Останнім етапом є встановлення DLP Discoverer, програмного забезпечення для серверів, призначеного для пошуку критичних даних та співпраці з платформами SharePoint, Microsoft SQL, MySQL, Oracle.

Після встановлення цих рішень систему вважають розгорнутою, і наступним етапом є налаштування. Спочатку потрібно класифікувати файли на кожній робочій станції і створити політику правил.

На малюнку 3.3 зображено меню програми DLP Endpoint, де можна обрати вкладку 'Classification'.

Класифікація даних - це процес, що оптимізує програми, процедури та процеси захисту даних. Дані класифікуються в залежності від їх чутливості та впливу на організацію в разі втрати, зміни або розкриття.

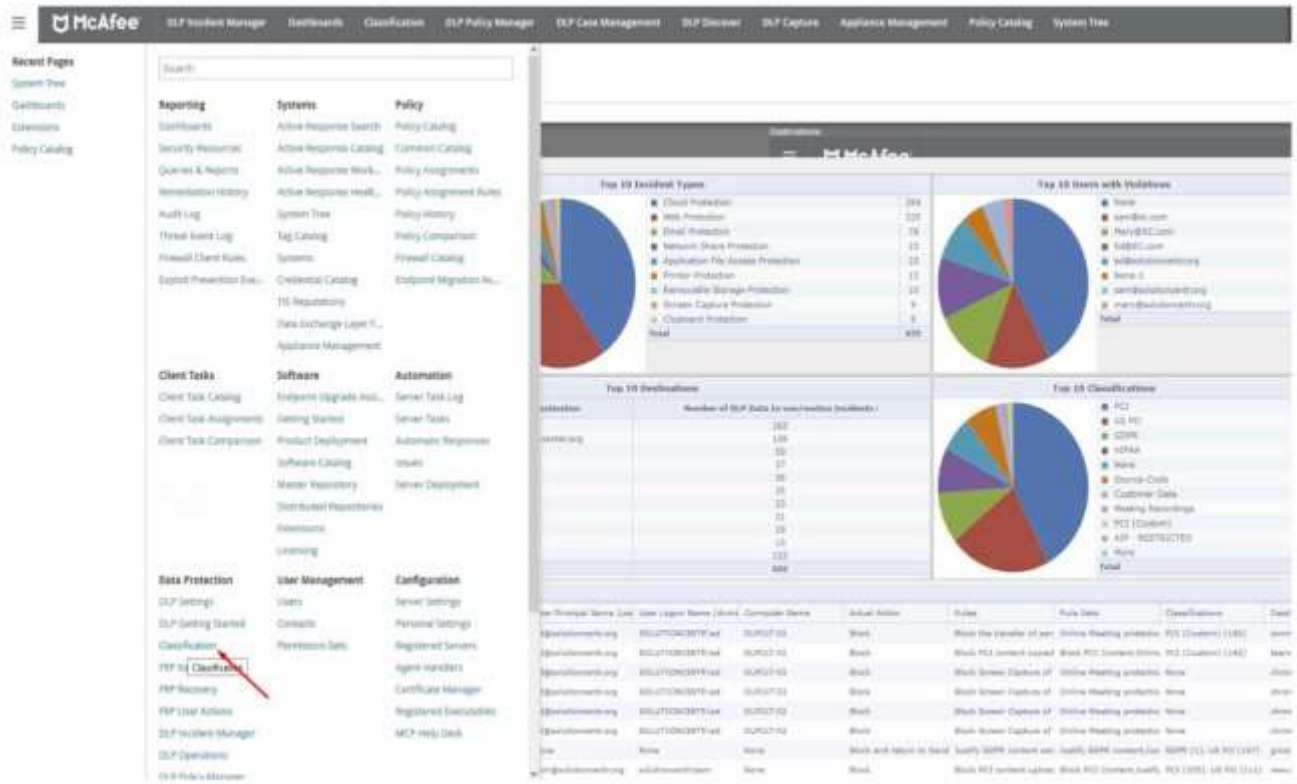

Рисунок. 3.5 Головне меню

Далі вводимо характеристику даних для розпізнавання, наприклад, ідентифікатори телефонів чи домени електронних адрес. Це можна зробити через меню Actions → New Classification Criteria → Advanced Pattern, як показано на рисунках 3.5 та 3.6.

Є різноманітні варіанти встановлення точного відповідності інформації, порівняння з бібліотеками, пошук за основними словами та за схожістю.

Зберігаємо обрані параметри і переходимо до створення політики правил.

Будь-яка розроблена політика безпеки в системі DLP є набором конкретних правил, які беззаперечно виконуються програмою.

На етапі проектування та виконання розглядаються всі набори правил, що застосовуються до середовища, в якому функціонує програма або цикл. Це робиться для оцінки відповідності ресурсу політиці DLP та визначення можливих порушень цієї політики.

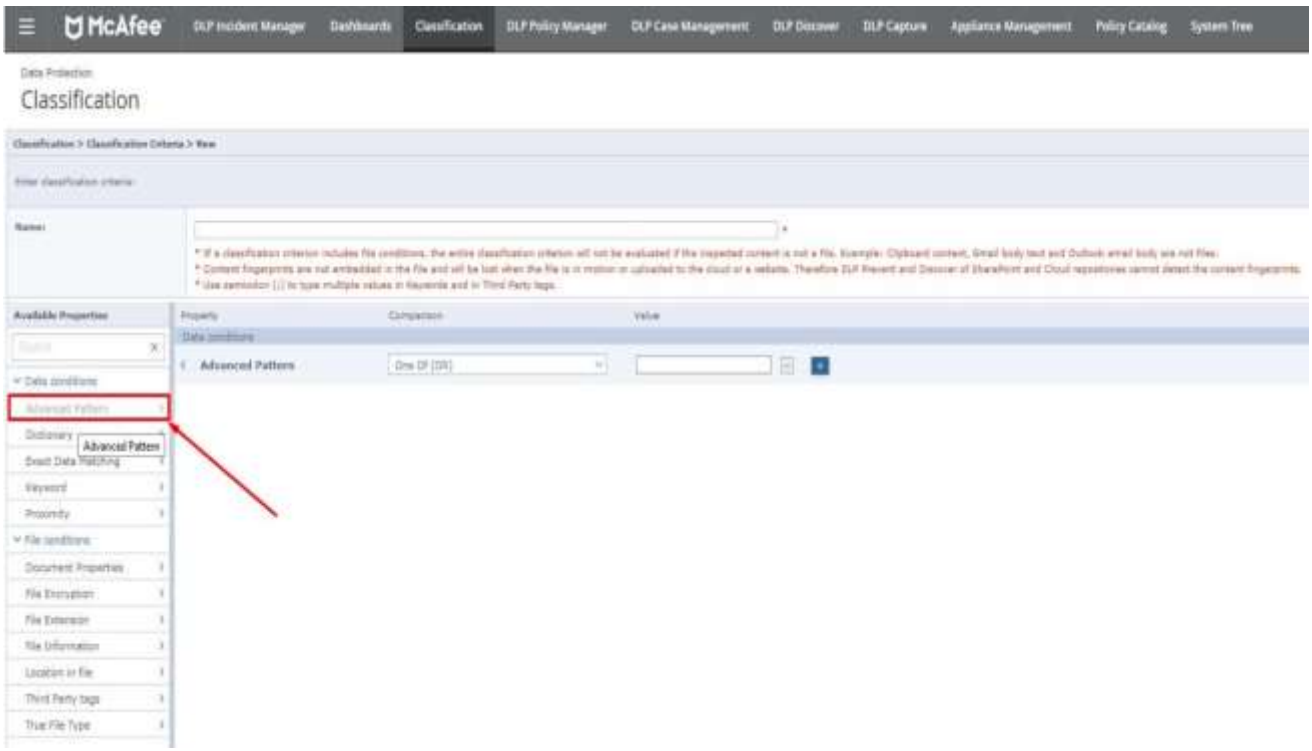

Рисунок 3.6 Меню підбору класифікації

Зберігаємо наш вибір і переходимо до створення політики правил.

Для створення нової політики слід перейти в менеджер політик, потім

Actions → New Rule Set і створити набір правил, як показано на рисунку 3.7.

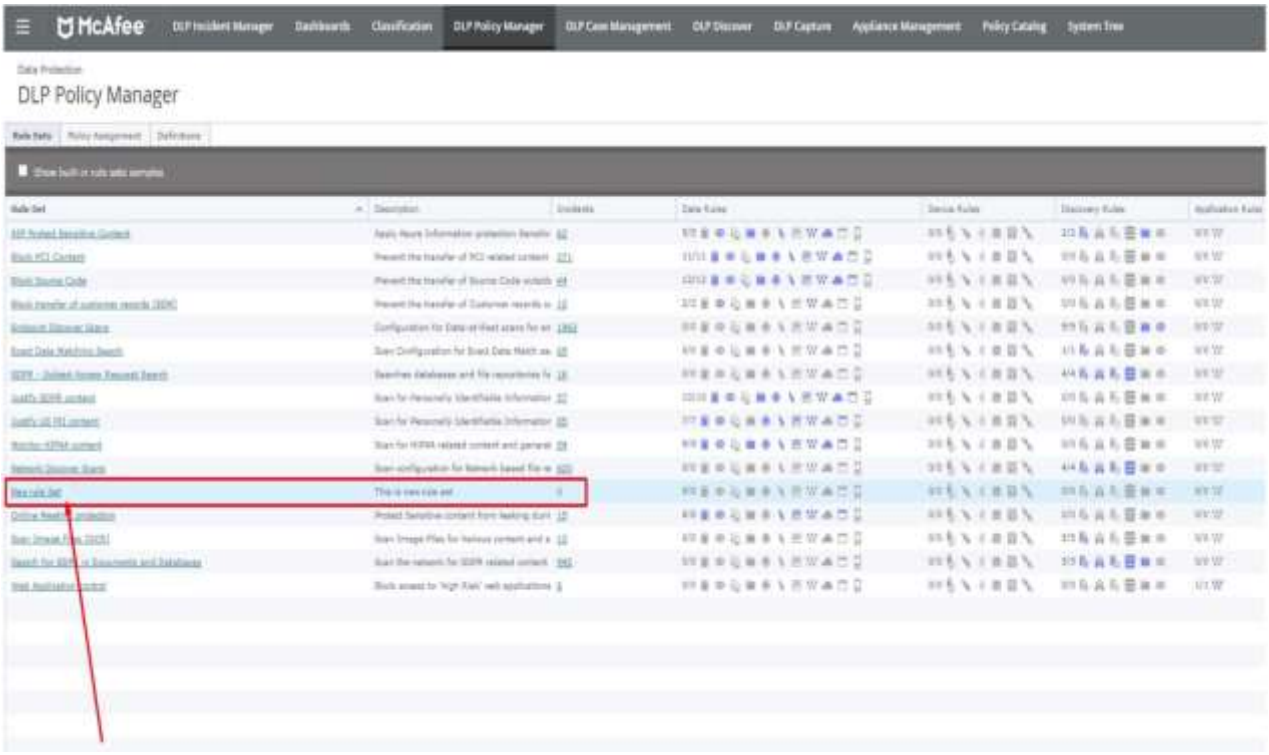

Рисунок 3.7 Створення набору правил

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

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

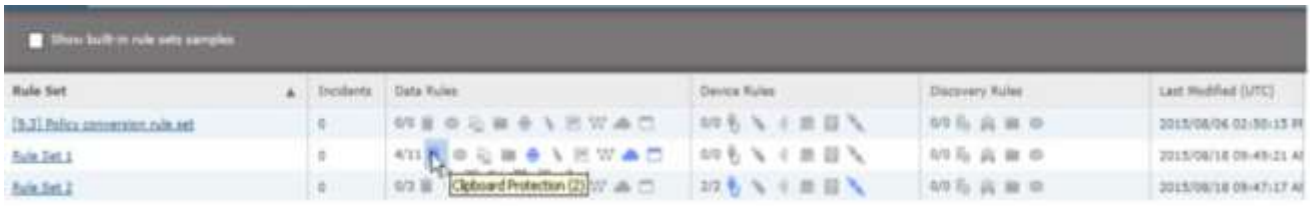

Рисунок. 3.8 Список створених правил.

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

На рис 3.9 зображений приклад повідомлення при спробі ввести захищаєму інформацію на веб-сторінці.

Рисунок 3.9 Блокування спроби вивести дані на веб-ресурс.

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

На жаль, в месенджері Telegram використовується криптографічний протокол MTProto, що на даний момент не підтримується моніторингом у використовуваному рішенні для запобігання витокам інформації.

Рисунок 3.10 Спроба відправити файл через сервіс моментальних

Рисунок 3.11 Блокування спроби вивести дані через пошту.

Також не треба забувати про спроби скопіювати інформацію на фізичний носій. З цим система впоралась теж без проблем, що показано на рисунку 3.12.

Рис 3.12 Блокування спрби копіювання інформації на фізичний носій.

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

Інтерфейс показано на рисунку 3.13.

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

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

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

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

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

Рисунок 3.13 Інтерфейс даних про інцеденти.

Крім того, у інтерфейсі демонструються актуальні дані щодо навантаження на мережу, використання потужностей кожної системи в корпоративній мережі та інші функції, які полегшують відстеження трафіку. Значущим є екран продуктивності системи. Приклад наведено на зображенні 3.14.

Інформація, представлена на даному екрані:

Evidence Queue (Черга підтверджень) - кількість файлів, які очікують копіювання в сховище підтверджень. Розмір черги відображається в режимі реального часу.

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

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

CPU usage (Використання ЦП) - рівень використання ресурсів центрального процесора.

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

-Disk (Диск) - використання диска в процентах.

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

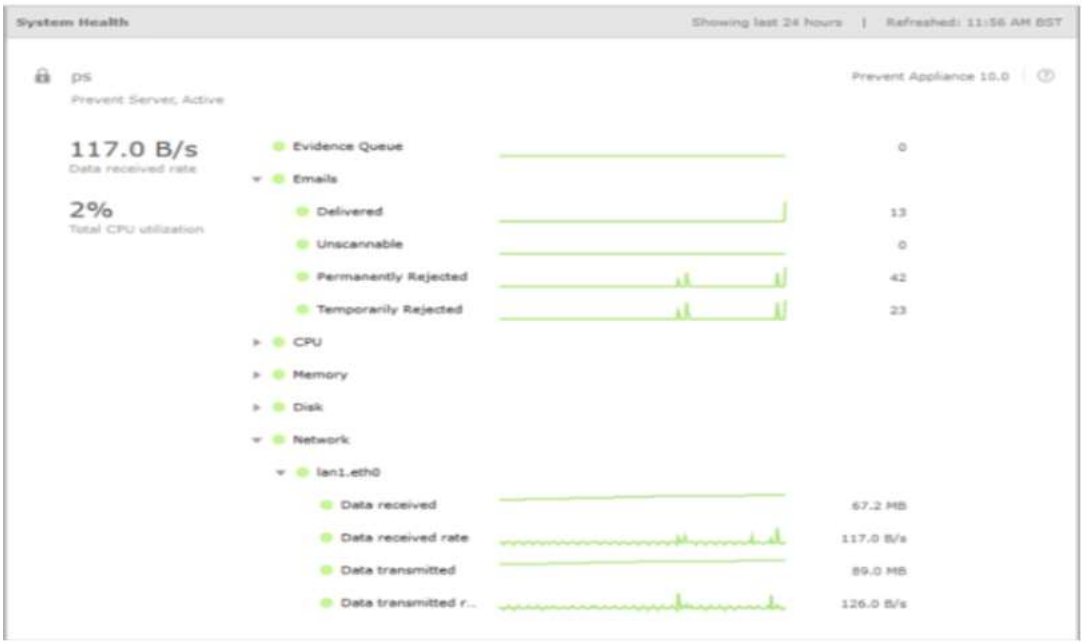

Рисунок 3.14 Екран працеспроможності системи.

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

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

Значно знилися ризики:

-витоку через веб-додатки

-витоку через пошту

-витоку через моментальні повідомлення

-витоку через копіювання на фізичні носії

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

Порівняння ризиків витоків інформації основними каналами.

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

3.3. Додаткові рекомендації для підвищення рівня захисту

Захист від витоків інформації не завершується на встановленні серверних та агентських рішень. Завжди існує можливість проникнення сторонніх осіб на територію підприємства, а також можливість співробітників зняти дані з моніторів на свої пристрої, такі як камера мобільного телефону. Для унеможливлення цих дій потрібно вжити наступні заходи.

Провести адміністративно-організаційні заходи.

Це включає в себе розробку політики безпеки, яка представляє собою набір документальних рішень, ухвалених директором фірми та начальником служби безпеки підприємства. Ця політика повинна ґрунтуватися на аналізі ризиків інформаційної системи підприємства.

Розробити документацію.

Вся документація, що стосується захисту конфіденційності оброблюваної інформації, повинна строго відповідати державним нормативно-правовим актам щодо захисту інформації. Крім того, необхідно отримати державну ліцензію, що спростить вирішення судових питань у разі витоку інформації.

Провести роботу з персоналом.

Витоки через персонал є найпоширенішими, тому особливу увагу слід приділяти роботі з персоналом. При роботі з базами даних обов'язково потрібно розробити політику допусків до інформації та чітко визначити ролі працівників.

Створити пропускний режим на підприємстві.

Контроль території підприємства від сторонніх осіб є необхідним на всіх підприємствах. Це забезпечується через створення контрольно-пропускного пункту.

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

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

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

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

Пункт безпеки оснащується системою захисту, яка має бути з'єднана з централізованим пультом контролю служби охорони. Для живлення системи захисту в аварійних ситуаціях повинен бути передбачений автономний джерело живлення. Перемикання на автономне джерело живлення повинно відбуватися автоматично.

Типи та характеристики системи захисту повинні відповідати встановленим вимогам та мати відповідні сертифікати.

Вимоги, спрямовані на запобігання витоку інформації каналом паразитних електромагнітних випромінювань і наведень:

Телекомунікаційні та електропостачальні мережі мають бути прокладені в металевих рукавах з обов'язковим заземленням.

Транзитні трубопроводи, повітроводи та інші металеві конструкції інженерних комунікацій не повинні проходити через об'єкт захисту. Якщо цього уникнути неможливо, то вони повинні бути обладнані вставками із ізоляційного матеріалу.

Виключити транзитне проходження будь-яких кабелів (мережі, сигналізації, оповіщення, електромережі тощо) через об'єкт захисту. Також слід уникати спільного прокладання кабельних ліній різного призначення (силових та сигнальних) в одному каналі з відстанню не менше 0,8 м.

Вимоги, спрямовані на забезпечення протипожежної безпеки на об'єкті захисту:

Внутрішні стіни, матеріали підвісних стель, розсіювачі освітлення повинні бути виготовлені з негорючих матеріалів.

Як засоби зменшення шуму слід використовувати негорючі (НГ) або матеріали з низькою горючістю (Г1), такі як перфоровані плити, панелі, мінеральна вата з максимальним коефіцієнтом звукопоглинання у межах частот 31,5 - 8000 Гц або інші матеріали, затверджені органами санітарно-епідеміологічного нагляду, для оздоблення приміщень.

Об'єкт оснащується автоматичною системою пожежного сигналізації. Тип та конфігурація системи пожежного сигналізації повинні відповідати встановленим вимогам та мати відповідний сертифікат.

3.4. Висновок

Після проведення аналізу ринку DLP-систем та ретельної роботи вибір був здійснений на користь комплексної системи запобігання витокам інформації, яка ідеально відповідає потребам даного підприємства. Після успішного розгортання обраної DLP-системи ризики витоку інформації значно зменшилися, що свідчить про ефективність її інтеграції в мережу підприємства. Проте, незважаючи на це, існує постійний ризик витоку через недбалість працівників, оскільки вони можуть ненавмисно розголошувати важливу інформацію під час звичайних розмов чи спілкування з колегами.

ВИСНОВКИ

Унаслідок розгляду ринку послуг DLP-систем та пильної роботи вибір був здійснений на користь комплексної системи запобігання витокам інформації, яка ідеально відповідає потребам даного підприємства. Завдяки успішному розгортанню обраної DLP-системи ризики витоку інформації в мережу підприємства були мінімізовані до критично низького рівня. Невдовзі після впровадження системи виявилися значущі зменшення загроз та збільшення ефективності контролю над інформаційною безпекою.

Згідно аналізу, найбільше витоків інформації відбувається через внутрішніх акторів, як то інсайдери або внаслідок необережності співробітників. Системи захисту від витоків інформації не лише взаємодіють з корпоративною мережею, а й відстежують дії працівників у цій мережі, що підсилює загальний рівень безпеки.

Під час дослідження загроз витоку інформації на підприємстві, було враховано різні класифікації та запропоновано шляхи мінімізації цих ризиків. Здійснено порівняльний аналіз різних комплексних систем запобігання витокам інформації, результатом якого став вибір оптимального варіанту для найбільш ефективного захисту від загроз. Реальні тестування та аналіз функціоналу системи McAfee підтвердили її високий рівень ефективності у запобіганні витокам через різноманітні канали.

Хоча впроваджена система значно знизила можливість витоків через основні канали, слід враховувати появу нових технологій, що можуть послабити захист. Тим не менш, системи DLP продовжують розвиватися, стаючи все більш

комплексними та ефективними рішеннями для забезпечення конфіденційності корпоративної інформації. Нинішні вимоги до їх функціональних можливостей швидко зростають, що дозволяє їм залишатися ключовим інструментом в області інформаційної безпеки. Розглянуті в роботі DLP-системи визначаються як одні з найбільш ефективних та системних рішень для захисту конфіденційної корпоративної інформації. Аналізовані функції та характеристики цих систем свідчать про їх високий потенціал в різних областях бізнесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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