Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Управління інцидентами інформаційної безпеки на основі використання DLP-систем
(тема)

Виконав: Ушатов В.В.

студент 2 курсу, групи БДІРм-18-1

Спеціальності 125 Кібербезпека
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Безпека державних інформаційних ресурсів
(повна назва освітньої програми)

Керівник доцент Сєвєрінов О.В.
(посада. прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри: _____ Халімов Г.З.
(підпис)
«____»_____ 2019 р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові Ушатову Владиславу Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Управління інцидентами інформаційної безпеки на основі використання DLP-систем
затверджена наказом по університету від 04.11. 2019 р. № 1648 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 24 грудня 2019 р.

3. Вихідні дані до роботи стандарт ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management», тип системи управління інцидентами інформаційної безпеки - DLP.

4. Перелік питань, що потрібно опрацювати в роботі
Розгляд систем управління інцидентами інформаційної безпеки.
Аналіз сучасних систем захисту від витоку конфіденційних даних.
Аналіз методів ідентифікації і аналізу конфіденційних даних в DLP-системах.
Розробка рекомендацій щодо вибору системи захисту від витоку конфіденційних даних.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5. включається до завдання за рішенням випускової кафедри)
презентаційний матеріал у вигляді слайдів

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	01.09.19	Виконано
2	Робота з джерелами за тематикою роботи	02.09.19-17.09.19	Виконано
3	Вивчення основних понять в сфері управління інцидентами інформаційної безпеки	18.09.19-29.09.19	Виконано
4	Розгляд систем управління інцидентами інформаційної безпеки	30.09.19-10.10.19	Виконано
5	Аналіз сучасних систем захисту від витоку конфіденційних даних	11.10.19-25.10.19	Виконано
6	Аналіз методів ідентифікації і аналізу конфіденційних даних в DLP-системах	26.10.19-15.11.19	Виконано
7	Розробка рекомендацій щодо вибору системи захисту від витоку конфіденційних даних	16.11.19-25.11.19	Виконано
8	Публікація тез конференцій за результатами досліджень	10.09.18-31.11.19	Виконано
9	Оформлення пояснювальної записки	26.11.19-31.11.19	Виконано

Дата видачі завдання _____ _____20__ р.

Студент _____
(підпис)

Керівник роботи _____ доцент Сєвєрінов О.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка включає в себе 70 сторінок, 13 рисунків, 1 таблицю, 22 джерела.

ІНЦИДЕНТ, УПРАВЛІННЯ ІНЦИДЕНТАМИ, ВИТІК ДАНИХ, DLP-СИСТЕМА, СТАТИСТИЧНИЙ АНАЛІЗ, ЛІНГВІСТИЧНИЙ АНАЛІЗ

Об’єктом дослідження є системи управління інцидентами інформаційної безпеки.

Предмет дослідження це процес захисту інформації від витоку конфіденційних даних.

Метою роботи є забезпечення управління інцидентами інформаційної безпеки на основі проведення аналізу існуючих систем захисту інформації від витоку конфіденційних даних та розробки рекомендацій щодо вибору DLP-систем.

В роботі проведений аналіз сучасних систем захисту від витоку конфіденційних даних. Розглянуті методи ідентифікації і аналізу конфіденційних даних в DLP-системах та розроблені рекомендації щодо вибору системи захисту від витоку конфіденційних даних.

РЕФЕРАТ

Пояснительная записка включает в себя 70 страниц, 13 рисунков, 1 таблицу, 22 источника.

ИНЦИДЕНТ, УПРАВЛЕНИЕ ИНЦИДЕНТАМИ, УТЕЧКА ДАННЫХ, DLP-СИСТЕМА, СТАТИСТИЧЕСКИЙ АНАЛИЗ, ЛИНГВИСТИЧЕСКИЙ АНАЛИЗ

Объектом исследования являются системы управления инцидентами информационной безопасности.

Предмет исследования - процесс защиты информации от утечки конфиденциальных данных.

Целью работы является обеспечение управления инцидентами информационной безопасности на основе проведения анализа существующих систем защиты информации от утечки конфиденциальных данных и разработке рекомендаций по выбору DLP-систем.

В работе проведен анализ современных систем защиты от утечки конфиденциальных данных. Рассмотрены методы идентификации и анализа конфиденциальных данных в DLP-системах и разработаны рекомендации по выбору системы защиты от утечки конфиденциальных данных.

ABSTRACT

Explanatory note to the thesis contains 70 pages, 13 figures, 1 table, 22 references.

INCIDENT, INCIDENT MANAGEMENT, DATA LEAK, DLP SYSTEM, STATISTICAL ANALYSIS, LINGUISTIC ANALYSIS

The object of the study is information security incident management systems.

The subject of the study is the process of protecting information from leakage of sensitive data.

The purpose of the work is to ensure management of information security incidents on the basis of the analysis of existing systems of protection of information against leakage of confidential data and development of recommendations for the choice of DLP-systems.

The paper analyzes modern systems for protecting against confidential data leakage. Methods for identifying and analyzing confidential data in DLP systems are considered and recommendations are developed for choosing a system for protecting against confidential data leakage.

ЗМІСТ

с.

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

БКФ – база контентної фільтрації

ІБ – інформаційна безпека

ІНН – індивідуальний ідентифікаційний номер

ІТ – інформаційна технологія

ПІБ – подія інформаційної безпеки

ПЗ – програмне забезпечення

DLP – data leak prevention, система захисту від витоку конфіденційних даних

FTP – file transfer protocol, протокол передачі файлів

IMAP – Internet message access protocol, протокол доступу до Інтернет-повідомлень

OCR – optical character recognition, аналіз графічних файлів

POP3 – post office protocol version 3, протокол поштового відділення версії 3

SIEM – security information and event management, управління інформаційною безпекою та подіями безпеки

SMS – short message service, служба коротких повідомлень

SMTP – simple mail transfer protocol, простий протокол передачі пошти

UEBA – user and entity behavior analytics, аналіз поведінки користувачів та сутностей

USB – Universal Serial Bus, Універсальна послідовна шина

VML – vector machine learning, вектор машинного навчання

ВСТУП

Стрімкий процес інформатизації суспільства супроводжується посиленням небезпеки втручання в роботу інформаційних систем в формі несанкціонованого доступу до інформації.

В зв’язку з цим підвищується актуальність постійного вдосконалення систем захисту інформації, використання комплексного підходу, об’єднуючого законодавчі, організаційні і програмно-технічні заходи.

Розвиток ринкових відносин на Україні сприяв тому, що не тільки державні підприємства і установи, а і об’єкти господарювання інших форм стикаються з необхідністю збереження комерційних, технологічних і фінансових секретів фірм, персональних даних фізичних осіб.

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів.

В ринкових умовах основним рушієм прогресу є конкуренція, яка спрямована на створення умов для збільшення прибутку, тому інформація за певних обставин стає об'єктом дій конкурентів. Сьогодні існують досить потужні системи несанкціонованого збору інформації, високоефективні технічні засоби та досить якісно підготовлені фахівці. Діяльність, пов'язана з несанкціонованим збором інформації щодо промислових та комерційних таємниць, має назву промислового шпигунства.

При забезпеченні інформаційної безпеки організації одним з найважливіших видів діяльності є виявлення інцидентів інформаційної безпеки. Неможливо уникнути всіх інцидентів інформаційної безпеки, так як завжди можуть відбуватися події, що тягнуть за собою потенційну загрозу.

Інцидент інформаційної безпеки - одне або серія небажаних або несподіваних подій в системі інформаційної безпеки, які мають імовірність

скомпрометувати ділові операції і поставити під загрозу захист інформації [1, 2].

У великих організацій щодоби фіксується велика кількість подій, які не є інцидентами, але один пропущений інцидент може коштувати організації дуже великих збитків, аж до припинення її діяльності.

Існує безліч способів боротьби з інцидентами, як на рівні організаційних процедур, так і на рівні програмних рішень. Одним з найбільш ефективних методів є впровадження систем захисту від витоку конфіденційних даних (DLP, Data Leak Prevention).

Технологія DLP забезпечує можливість блокування передачі конфіденційної інформації по різним каналам, а також надає інструмент для спостереження за щоденною роботою співробітників, який дозволяє знайти слабкі місця в безпеці до настання інциденту.

Кількість інцидентів, пов’язаних з несанкціонованим витоком інформації, постійно зростає. Тому актуальним є проведення аналізу систем захисту від витоку конфіденційних даних, DLP-систем.

Об’єктом дослідження є системи управління інцидентами інформаційної безпеки.

Предмет дослідження це процес захисту інформації від витоку конфіденційних даних.

Метою роботи є забезпечення управління інцидентами інформаційної безпеки на основі проведення аналізу існуючих систем захисту інформації від витоку конфіденційних даних та розробки рекомендацій щодо вибору DLP-систем.

Для досягнення мети в роботі вирішуються наступні задачі:

1. Розгляд систем управління інцидентами інформаційної безпеки.
2. Аналіз сучасних систем захисту від витоку конфіденційних даних.
3. Аналіз методів ідентифікації і аналізу конфіденційних даних в DLP-системах.

4. Розробка рекомендацій щодо вибору системи захисту від витоку конфіденційних даних.

1 УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Інциденти інформаційної безпеки

Згідно прийнятому в ITIL (бібліотека інфраструктури інформаційних технологій) визначенню під «інцидентом» розуміється «будь-яка подія, що не є елементом нормального функціонування служби і при цьому надає або здатна зробити вплив на роботу служби шляхом її переривання або зниження якості» [1].

Під подією інформаційної безпеки (ПІБ) розуміється стан системи, сервісу або мережі, котрий свідчить про можливе порушення політики безпеки, або про невідому ситуацію, яка може мати відношення до безпеки, тоді як інцидент інформаційної безпеки (ІІБ) – це одна або серія подій інформаційної безпеки, які можуть призвести до збитків та втрат для організації. Втрати можуть бути, як матеріальними (вартість інформації, експлуатаційні витрати і т.д.) так і нематеріальними (репутація організації, зміна морально-психологічного клімату і т.д.) [1].

Інцидент інформаційної безпеки – це одинична подія або ряд небажаних та непередбачених подій інформаційної безпеки, через які існує ймовірність компрометації бізнес-інформації і загрози інформаційній безпеці [2].

В якості прикладу інцидентів можна привести такі події, як неавторизована зміна даних на сайті організації, залишення комп'ютера незаблокованим без нагляду, пересилка конфіденційно

Жоден найдосконаліший спосіб зниження ризиків інформаційної безпеки, будь це політика безпеки, що досконально опрацьована, або найсучасніший брандмауер, не може захистити від виникнення в інформаційному середовищі подій, що потенційно несуть загрозу діяльності організації. Статистика загроз безпеці інформації організації представлена на рис. 1.1.

Рисунок 1.1 – Статистика загроз безпеці інформації

Складність і різноманітність середовища діяльності сучасного підприємства зумовлюють наявність залишкових ризиків незалежно від якості підготовки і впровадження заходів протидії. Також завжди існує вірогідність реалізації нових, невідомих до теперішнього часу, загроз інформаційній безпеці. Неготовність організації до обробки подібного роду ситуацій може істотно ускладнити відновлення бізнес-процесів та потенційно збільшити завдані збитки.

1.2 Основи управління інцидентами інформаційної безпеки

Система управління інцидентами інформаційної безпеки є базовою частиною загальної системи управління інформаційною безпекою і дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти інформаційної безпеки. Без реалізації цих процесів неможливо забезпечити рівень захищеності, що адекватний сучасним стандартам і галузевим нормам.

Управління інцидентами, це важливий процес, який забезпечує організації можливість спочатку виявити інцидент, а потім за допомогою коректно обраних засобів підтримки якомога швидше його вирішити.

Основна задача управління інцидентами – якомога швидше відновити нормальну роботу служб і звести до мінімуму негативний вплив інциденту на роботу організації для підтримки якості і доступності служб на максимально можливому рівні. Нормальною вважається робота служб, що не виходить за рамки угоди про рівень обслуговування.

Цілі управління інцидентами:

– відновлення нормальної роботи служб в найкоротші терміни;

– зведення до мінімуму впливу інцидентів на роботу організації;

– забезпечення злагодженої обробки всіх інцидентів і запитів обслуговування;

– зосередження ресурсів підтримки на найбільш важливіших напрямах;

– надання відомостей, що дозволяють оптимізувати процеси підтримки, зменшити кількість інцидентів і запланувати управління.

Для реалізації системи управління інцидентами інформаційної безпеки необхідно провести наступні роботи:

– виділити ресурси для розробки та впровадження системи управління інцидентами;

– визначити область функціонування системи управління інцидентами;

– розробити комплекс процесів системи управління;

– навчити персонал;

– впровадити процеси управління інцидентами та інтегрувати їх зі вже функціонуючими процесами управління інформаційної безпекою, такими як, інвентаризація активів, аналіз ризиків та оцінка ефективності;

– розробити архітектуру і комплекс технічних засобів з автоматизації процесів управління інцидентами і моніторингу подій інформаційної безпеки;

– впровадити комплекс програмно-технічних засобів автоматизації управління інцидентами.

В результаті проведених робіт буде впроваджена система управління інцидентами інформаційної безпеки, яка буде вирішувати наступні задачі:

– оперативний моніторинг стану інформаційної безпеки в рамках обраної галузі діяльності системи;

– виявлення, облік, реагування, розслідування та аналіз інцидентів інформаційної безпеки;

– інформування вищого керівництва і зацікавлених осіб про поточний стан інформаційної безпеки.

Для забезпечення інформаційної безпеки необхідно реалізувати комплексний підхід щодо вирішення наступних задач:

– виявлення, інформування та облік інцидентів інформаційної безпеки;

– реакція на інциденти інформаційної безпеки, включаючи застосування необхідних засобів для запобігання, зменшення і відновлення завданого збитку;

– аналіз відбувшихся інцидентів, з метою планування превентивних заходів захисту і поліпшення процесу забезпечення інформаційної безпеки в цілому.

Також слід зазначити, що при експлуатації різного роду систем менеджменту інформаційної безпеки процес управління інцидентами є одним з найважливіших постачальників даних для аналізу функціонування подібних систем, оцінки ефективності використовуваних заходів зниження ризиків і планування поліпшень в роботі системи.

Для подолання реальної або потенційної шкоди працездатності системи, яку завдають інциденти, необхідно організувати процес управління ними. Він включає в себе (рис. 1.2):

– визначення переліку подій, які є інцидентами;

– визначення факту вчинення інциденту інформаційної безпеки;

– оповіщення відповідальної особи про виникнення інциденту;

– порядок усунення наслідків і причин інциденту;

– порядок розслідування інциденту;

– винесення дисциплінарних стягнень;

– реалізація необхідних коригувальних і превентивних заходів.

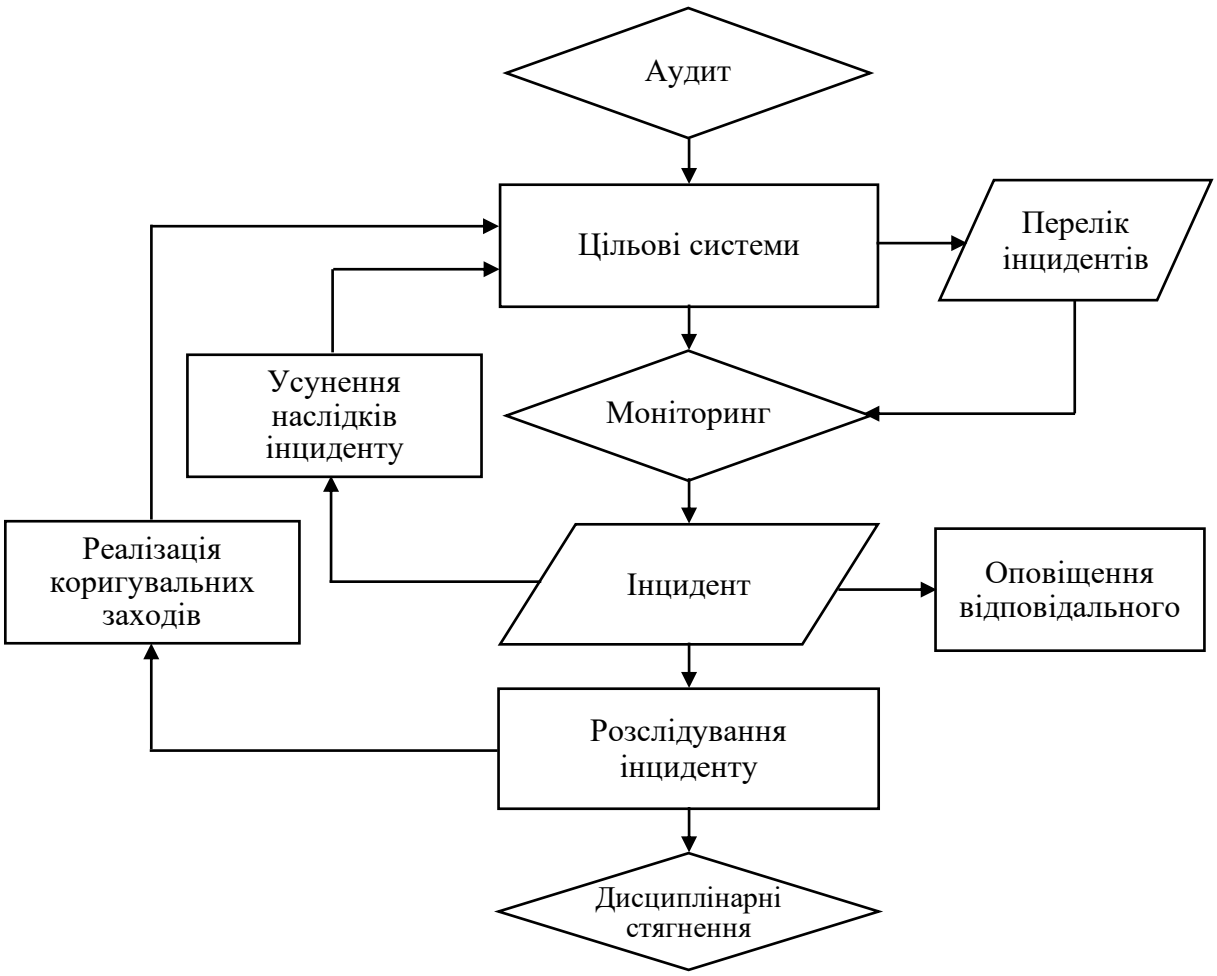

Рисунок 1.2 – Процес управління інцидентами

До теперішнього часу в міжнародній практиці розроблено достатню кількість нормативних документів, що регламентують питання управління інцидентами інформаційної безпеки. Для найбільш ефективної реалізації системи управління інцидентами інформаційної безпеки необхідно спиратись на вимоги міжнародних і галузевих стандартів, таких як ISO\IEC 27001-2013 "Information security management systems. Requirements" та ITU-T X-1051 "Information security management systems. Requirements for telecommunications".

В рамках даних стандартів висуваються загальні вимоги до побудови системи управління інформаційною безпеки, що відносяться у тому числі и до

процесів управління інцидентами, даються практичні підходи з виявлення, реєстрації та оцінці випадків порушення інформаційної безпеки та вразливостей.

Специфічні питання управління інцидентами інформаційної безпеки розглядаються в наступних документах:

- ISO/IEC 27035:2011 "Information technology. Security techniques. Information security incident management" (ISO/IEC TR 18044 "Information security incident management") описує інфраструктуру управління інцидентами в рамках циклічної моделі PDCA. Розглядаються питання забезпечення нормативно-розпорядчою документацією, ресурсами, приводяться докладні рекомендації щодо необхідних процедур [4].

- CMU/SEI-2004-TR-015 Defining incident management processes for CISRT (Software Engineering Institute/Carnegie Mellon University) описує методологію планування, впровадження, оцінки і поліпшення процесів управління інцидентами. Основний наголос робиться на організації роботи CISRT (Critical Incident Stress Response Team) – групи або підрозділів, які забезпечують сервіс і підтримку запобігання, обробки і реакції на інциденти інформаційної безпеки. Вводиться ряд критеріїв, на підставі яких можна оцінювати ефективність даних сервісів, приводяться докладні процесні карти [5].

- NIST SP 800-61 Computer security incident handling guide - збірка "кращих практик" щодо побудови процесів управління інцидентами і реакції на них. Детально розбираються питання реакції на різні типи загроз, такі як розповсюдження шкідливого програмного забезпечення, несанкціонований доступ та ін. [6].

Документ ISO/IEC 27035:2011 (ISO/IEC TR 18044 Information security incident management) визначає формальну модель процесу реакції на інциденти [4]. Цілями проходження цієї моделі є впевненість в тому, що:

– події та інциденти інформаційної безпеки виявляються і обробляються ефективним чином, особливо в частині класифікації подій;

– виявлені інциденти інформаційної безпеки враховуються і обробляються найбільш відповідним і ефективним чином;

– наслідки інцидентів інформаційної безпеки можуть бути мінімізовані в процесі реакції на інциденти, можливо із залученням процесів відновлення після збоїв та аварій (DRP/BCP);

– за рахунок аналізу інцидентів та подій ІБ підвищується ймовірність запобігання майбутніх інцидентів, поліпшуються механізми і процеси забезпечення ІБ.

Стандарт ISO/IEC 27001 накладає ряд загальних вимог з побудови процесів управління інформаційною безпекою, до складу яких входить і процес управління інцидентами. До числа таких вимог відноситься:

– використання моделі PDCA для забезпечення планування процесів, впровадження процесів, контролю й аналізу процесів, поліпшення процесів.

– належне документування процесів і процедур;

– своєчасне виявлення невдалих і успішних спроб порушення безпеки та інцидентів інформаційної безпеки;

– своєчасне повідомлення про інциденти ІБ за належними управлінськими каналами;

– встановлення відповідальності керівництва і процедур для забезпечення швидкої і ефективної реакції на інциденти ІБ;

– повинні бути реалізовані механізми, які дозволяють вимірювати і відстежувати типи, обсяги і вартість інцидентів ІБ;

– необхідно зібрати, зберегти і надати докази відповідно до вимог локального законодавства;

– повинна бути забезпечена підтримка керівництвом процесів управління інцидентами;

– процеси управління інцидентами повинні безперервно аналізуватися і поліпшуватися.

Основні вимоги до процесу управління інцидентами в стандартах ISO/IEC 27001 та ISO/IEC 27002 полягають в наступному [2, 7]:

- розподіл відповідальності та розробка процедур. Це ключовий момент в будь-якому процесі. Якщо персонал не знатиме, кому і яким чином реагувати на інцидент, то про управління даним процесом не може бути й мови;

- інформування про інциденти. Стандарт визначає, що всі (не тільки штатні співробітники компанії, але і підрядники, які залучаються для виконання будь-яких робіт) повинні в обов'язковому порядку своєчасно інформувати відповідальних осіб про відповідні події ІБ;

- інформування про уразливість ІБ. Дана міра призначена для запобігання можливим інцидентам ІБ;

- оцінка і прийняття рішень по інцидентах. Не всяке подія ІБ є інцидентом - все залежить від прийнятої класифікації та проведеної оцінки;

- реагування на інциденти. Рекомендується, щоб процедура дій у відповідь на інциденти була документально підтверджена, включала такі дії, як збір свідчень, проведення експертного аналізу, ескалація (при необхідності), ведення необхідних записів, оповіщення зацікавлених сторін, усунення виявлених вразливостей, закриття інциденту і оформлення необхідної документації;

- витяг уроків з інцидентів. Якщо інцидент стався, слід досконально вивчити його причини і вжити необхідних заходів, щоб по можливості запобігти його повторному виникненню;

- збір свідчень. Даний процес повинен забезпечити наявність доказової бази як для внутрішніх дисциплінарних процесів, так і при необхідності для судового розгляду.

Стандарт ISO/IEC 27035: 2011 «Information technology. Security techniques. Information security incident management» («Інформаційна технологія. Методи і засоби забезпечення безпеки. Управління інцидентами ІБ») містить структурований і планомірний підхід [4]:

– до виявлення, складання звітів і оцінці інцидентів ІБ;

– здійснення відповідної реакції і управління інцидентами ІБ;

– виявлення, оцінки та усунення вразливостей;

– постійного поліпшення управління ІБ і інцидентами ІБ.

ISO/IEC 27035: 2011 є досить ємним і всебічно розглядає управління як вразливостями (vulnerability management), так і інцидентами ІБ.

У стандарті після освітлення основ управління інцидентами ІБ, його переваг і ключових питань, деяких прикладів інцидентів ІБ і причин їх виникнення процес управління інцидентами ІБ розглядається як включає кілька підпроцесів:

– планування та підготовка до обробки інцидентів ІБ, включаючи складання документів, що підтримують управління інцидентами;

– виявлення/ідентифікація і підготовка звіту щодо інциденту ІБ;

– оцінка інциденту і прийняття рішень щодо інциденту ІБ;

– відповідна реакція на інцидент ІБ;

– витяг уроків з інциденту ІБ.

Даються рекомендації щодо необхідних ресурсів і процедур.

Таким чином, для управління інцидентами інформаційної безпеки необхідно організувати комплекс процесів управління інцидентами, забезпечити його належними ресурсами, відповідною нормативно-розпорядчою і робочою документацією, технічними засобами забезпечення механізмів контролю.

Основною метою забезпечення інформаційної безпеки організації є зниження ризиків, діючих відносно інформаційних ресурсів, і як наслідок запобігання або мінімізація збитку від можливих інцидентів.

За останні кілька років кількість витоків конфіденційної інформації та персональних даних виросло більш ніж в 5 разів. Для забезпечення захисту конфіденційних даних організації використовують DLP системи (Data Leak Prevention), які створюють захищений цифровий «периметр» навколо організації, аналізуючи всю інформацію, що витікає, а в ряді випадків і входить в захищену зону. Контрольованої інформацією повинен бути не тільки інтернет-трафік, але і ряд інших інформаційних потоків: документи, які виносяться за межі контуру безпеки на зовнішніх носіях, роздруковуються на принтері, що відправляються на мобільні носії через Bluetooth і т.п.

Впровадження системи для захисту даних завжди пов'язане з ризиком створення зайвого навантаження на локальну мережу компанії. Особливо це

стосується організацій, які в силу специфіки своєї діяльності працюють зі значними обсягами даних. Тому часто DLP-системи мають клієнт-серверну архітектуру і складаються з декількох компонентів, кожен з яких відповідає за виконання певних завдань. Завдяки чому DLP-системи легко масштабуються, тим самим забезпечуючи надійну роботу навіть в умовах високих навантажень на мережу.

2 АНАЛІЗ СУЧАСНИХ СИСТЕМ ЗАХИСТУ ВІД ВИТОКУ КОНФІДЕНЦІЙНИХ ДАНИХ

2.1 Система захисту від витоку конфіденційних даних

Витік інформації - це неконтрольоване поширення інформації, що захищається, за межі організації або кола осіб, котрим ці відомості були довірені, в результаті її розголошення або несанкціонованого доступу до неї [8]. Витік інформації можна розділити на два типи: навмисні і ненавмисні.

Навмисний витік характеризуються тим, що зловмисник, маючи доступ до інформації, що захищається, розуміє протиправність своїх дій і усвідомлює їх можливі негативні наслідки. Причому основними мотивами для здійснення подібного роду злочинів є в більшості випадків матеріальна нажива або отримання іншої вигоди. Крім того, крадіжка критичних даних хакерами, які обманним або іншим шляхом отримали прямий доступ до них за допомогою співробітника організації, теж відноситься до навмисних витоків, навіть якщо протиправних намірів у співробітника не було.

Ненавмисний витік пов'язаний з халатністю або недостатньою обізнаністю користувачів в своїх функціональних обов’язках. Найбільш поширені помилки працівників організації, що ведуть до витоків, представлені на рисунку 2.1 [9].

В даний час однією з найбільш актуальних загроз у сфері інформаційної безпеки є витік конфіденційних даних від несанкціонованих дій користувачів. Це пов’язано з тим, що більша частина традиційних засобів захисту, таких як антивіруси, міжмережні екрани, системи автентифікації та контролю доступу не здатні забезпечити ефективний захист від внутрішніх порушників.

Тому першочерговим завданням для сучасних підприємств є оптимізація робочих процесів і захист від витоків інформації.

Рисунок 2.1 – Поширені помилки користувачів, що ведуть до ненавмисних витоків даних

Здійснити запобігання витоку конфіденційної інформації дозволяють системи DLP.

DLP-системи забезпечують блокування загроз, дбають про безпеку інформації, контролюють роботу персоналу. Це комплекс програмного забезпечення, що запобігає несанкціонованому доступу і втраті важливої інформації. Завдяки глибокій аналітиці вхідних і вихідних даних DLP-система розпізнає загрози та сповіщає про це її власника. Також система визначає рівень конфіденційності документів, аналізуючи відповідні маркери або їх вміст.

DLP-системи не тільки захищають від витоку інформацію, а й дозволяють виконувати широкий спектр інших не менш важливих завдань захисту даних. Вони можуть забезпечувати контроль роботи співробітників, перевірку їх комунікацій, правомірність дій, стеження за раціональним використанням

робочого часу. Також система дозволяє прогнозувати звільнення працівників, виявляючи тих, хто відправляє своє резюме в інші організації. Це дозволяє керівництву володіти обстановкою і вживати відповідних заходів.

Основні функції DLP-систем [10, 11]:

– контроль передачі інформації через Інтернет з використанням e-mail, http, https, ftp і інших додатків і протоколів;

– контроль збереження інформації на зовнішні носії та мобільні пристрої;

– захист інформації від витоку шляхом контролю друк даних;

– блокування спроб пересилання або збереження конфіденційних даних, інформування адміністраторів ІБ про інциденти, спроби створення копій;

– пошук конфіденційної інформації на робочих станціях і файлових серверах за ключовими словами, мітками документів, атрибутами файлів і цифровими відбитками;

– запобігання витоку інформації шляхом контролю життєвого циклу і руху конфіденційних відомостей.

В результаті використання DLP-систем можуть бути вирішені питання:

– запобігання витокам і несанкціонованої передачі конфіденційної інформації;

– мінімізації ризиків фінансового і репутаційного збитку;

– підвищення дисципліни користувачів;

– розслідування інцидентів та їх наслідків;

– ліквідації загроз безпеки персональних даних, відповідності вимогам щодо захисту персональних даних.

Останнім часом вимоги до функціональних можливостей DLP-систем постійно зростають, що призводить до перетворення їх в один з найефективніших, комплексних і системних рішень в сфері захисту конфіденційної корпоративної інформації.

Сучасна DLP-система, як правило, являє собою розподілений програмно-апаратний комплекс, що складається з декількох модулів, які функціонують на

виділених серверах, на робочих місцях співробітників компанії (персональних комп'ютерах, робочих станціях, інших пристроях) і на рівні внутрішньої служби безпеки:

– модулі бази даних, систематизації, аналізу та іншої обробки інформації, що стосується всіх інцидентів, виявлених системою, а також інших даних, відстеження і контроль яких закладені в систему;

– модулі пасивного і (або) активного спостереження, контролю за діями співробітників компанії (користувачів). Перелік дій, що відслідковуються і контролюються системою, встановлюється заздалегідь і як правило носить обмежений характер. Стандартний перелік зазвичай включає контроль входу і виходу з системи, безпроводової передачі даних, підключення зовнішніх пристроїв, на які може бути скопійована інформація, друку документів та інших процесів.

– модулі управління, моніторингу, налаштування системи, аналітичної роботи для потреб служби безпеки.

Кожен з модулів DLP-системи вирішує своє коло завдань. Розглянемо основні функціональні модулі DLP-систем.

1. Контроль корпоративної пошти. В базах даних DLP можуть зберігатися все поштові повідомлення контрольованого користувача, незважаючи на те, що користувач може видалити отримане або відправлене повідомлення, а відновлення з резервної копії може займати значний час або ж резервування пошти може не бути зовсім. За адресатам листів може бути побудований відповідний звіт, який дасть розуміння, з ким і в якому обсязі взаємодіє користувач (рисунок 2.2). Також здійснюється аналіз тексту листів на збіг з певними словоформами.

2. Контроль програм обміну повідомленнями. Всі повідомлення месенджерів контрольованого користувача можуть зберігатися в базах даних DLP. Згідно з політиками і правилами, що налаштовані в DLP, відбувається спрацьовування на певний контент, оператор DLP оповіщається про відповідні повідомленнях. Незважаючи на те, що обмін між клієнтом і сервером

месенджера може відбуватися за допомогою засобів шифрування месенджера, DLP-система отримує незашифровані дані, якщо вона підтримує відповідний месенджер.

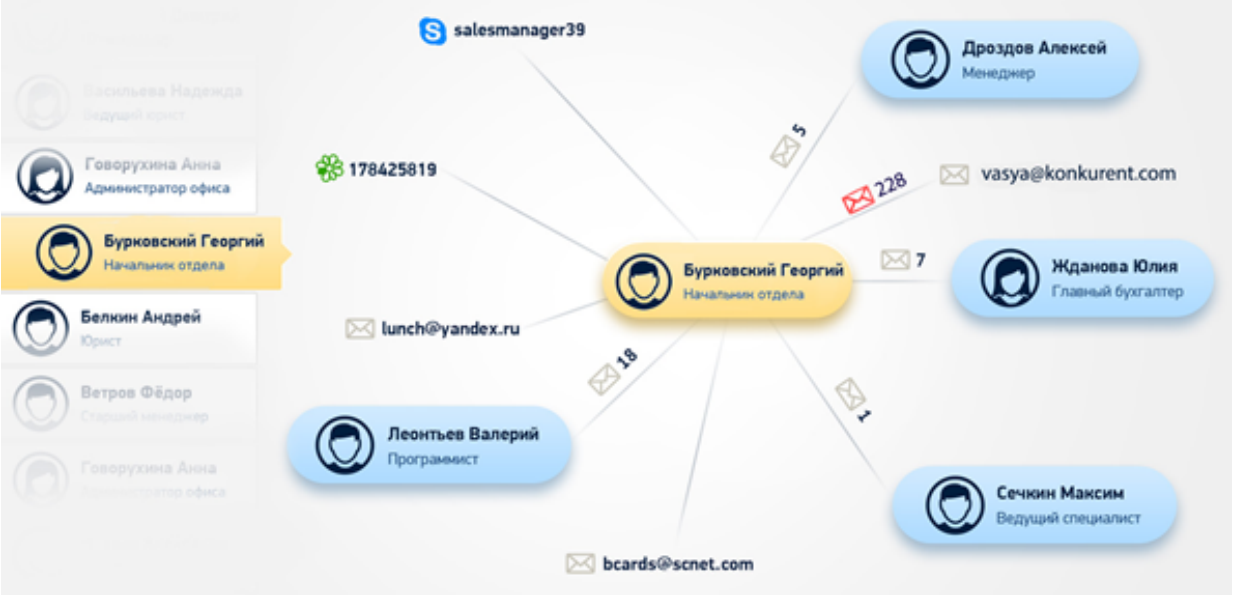

Рисунок 2.2 – Контроль корпоративної пошти

3. Контроль друку. Модуль дозволяє контролювати файли, які користувач відправляє на друк, зберігаючи їх у базах даних DLP. Також може контролюватися обсяг друку та здійснюватися збір статистики по друку.

4. Контроль зовнішніх накопичувачів. DLP-система фіксує та розпізнає пристрої, які підключаються до робочого місця. Мається можливість задання переліку дозволених пристроїв і шифрування даних на них. У разі відповідного налаштування система здатна зробити копію всієї інформації, що зберігається на підключеному зовнішньому пристрої користувача, або тільки файлів, які зчитуються/записуються на зовнішній пристрій.

5. Контроль пристроїв вводу. Найчастіше це логгер клавіатури і миші, які при відповідних настройках записують в бази даних DLP все натискання на клавіатуру і рухи миші користувача. У деяких DLP-системах при цьому відбувається аналіз словоформ, і при відповідних настройках відбувається спрацьовування на певні слова (поєднання) з оповіщенням оператора DLP.

6. Контроль пристроїв відеовиводу. Дозволяє при відповідних настройках з необхідною періодичністю проводити знімки екрану монітора користувача із записом їх в бази даних DLP для подальшого перегляду та аналізу оператором.

7. Контроль роботи програмного забезпечення (ПЗ) робочого місця користувача. Веде фіксацію початку і закінчення використання ПЗ користувача. Може також контролювати завантаження ресурсів робочого місця користувача, дозволяє оцінити активність та ефективність роботи персоналу.

8. Контроль роботи користувача в браузерах (http, https). Модуль фіксує всі відвідувані сайти (або сторінки) та час, проведений на кожному сайті.

9. Контроль обміну файлами (ftp, sftp). Виробляє запис копій переданих користувачем файлів з фіксацією адреси одержувача.

10. Аудіоконтроль роботи користувача (при наявності підключеного мікрофона). Дозволяє вести запис з мікрофону, підключеного до робочого місця користувача за заданим розкладом або в центрі онлайн-контролю.

11. Відеоконтроль роботи користувача (при наявності підключеної камери). Дозволяє налаштувати відеозапис з камери, підключеної до робочого місця. У більшості випадків використовується спільно з модулем аудіо-контролю.

До складу більшості DLP-систем входять також центри: адміністратора, звітності, повідомлень, онлайн-контролю.

DLP-система може бути інтегрована в IT-інфраструктуру компанії та поєднана з іншими системами і рішеннями щодо захисту інформації.

Розглянемо можливу архітектуру DLP-системи (рисунок 2.3).

Всі інформаційні потоки в компанії перехоплюються сервером перехвату з мережевого адаптера, потім аналізуються і зберігаються в базі.

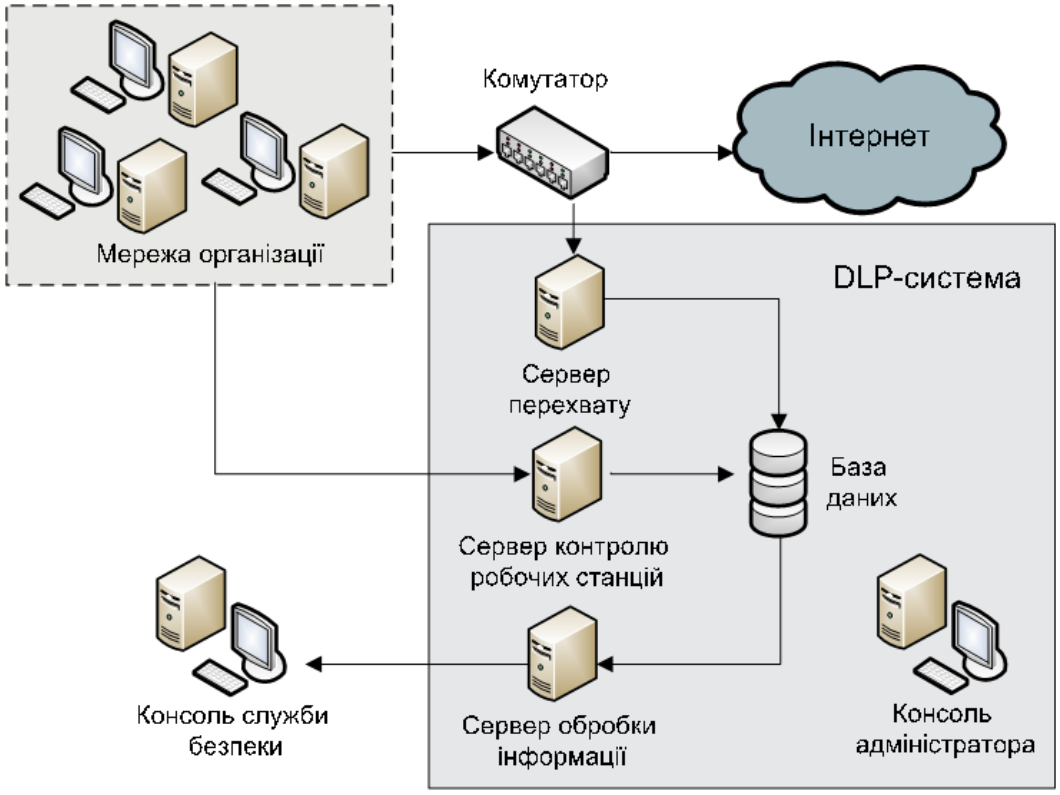

Рисунок 2.3 – Архітектура DLP-системи

Інформація, отримана за допомогою сервера перехвату (повідомлення в месенджерах, вкладені файли, електронні листи і т.п.), зберігається на сервері баз даних.

Після збереження в базі даних вся перехоплена інформація надходить на сервер обробки даних, який відповідає за виконання завдань:

– індексування перехопленої інформації;

– повнотекстовий пошук по інформації;

– автоматичний аналіз і відправка на задані адреси електронної пошти повідомлень про факт передачі інформації з порушенням прийнятої в компанії політики безпеки.

Сервер контролю робочих станцій призначений для централізованої установки на комп'ютери програм-агентів, призначених для перехоплення безпосередньо з робочих станцій користувачів трафіку, в тому числі шифрованого, а також даних, що передаються для друку на принтери і зовнішні пристрої. Програми агенти відповідають також за збір статистичної інформації

про активність співробітників на робочих місцях. Крім того, сервер контролю робочих станцій здійснює моніторинг стану всіх встановлених в мережі агентів і в разі виявлення збою або примусового відключення агента користувачем будь-якого комп'ютера автоматично здійснює повторну установку.

Консоль адміністратора використовується в DLP-системі для централізованої установки і настройки роботи всіх елементів програми та для віддаленої установки програм-агентів на робочі станції користувачів. Через консоль адміністратора здійснюється настройка параметрів перехоплення і періодичність індексування даних, перегляду статистики по перехопленому трафіку в режимі реального часу, а також налаштовується система повідомлень про збої в роботі системи перехоплення.

Через консоль служби безпеки здійснюється робота з DLP-системою. Відбувається редагування існуючих і створення нових правил безпеки, проводиться оцінка зібраних даних, аналіз звітів, які надають інформацію як про активність окремих співробітників, так і всієї організації в цілому.

Весь нешифрований трафік, який циркулює в мережі компанії, перехоплюється централізовано або за допомогою програм-агентів, встановлених на комп'ютери. Перехоплений трафік передається на сервер перехоплення за допомогою керованого комутатора. На сервері перехоплення проводиться аналіз отриманого трафіку, в ході якого виділяються необхідні дані (список месенджерів, електронні листи, файли і т.п.) і зберігаються у базах даних DLP-системи.

Програми-агенти дозволяють перехоплювати як нешифровані, так і зашифровані дані. Агенти віддалено встановлюються на комп'ютери сервером контролю робочих станцій. Агенти відстежують дані, що пересилаються в месенджерах і по електронній пошті, всі випадки відправки інформації користувачами на зовнішні пристрої та принтери, та передають все перехоплені дані на сервер обробки. Також за допомогою програм-агентів здійснюється моніторинг діяльності співробітників на робочих місцях і збір статистичних даних для формування звітів.

Після перехоплення вся інформація надходить на сервер обробки даних, де проводиться побудова індексів інформації, що знаходиться в базі, з подальшим збереженням індексів в сховище сервера обробки інформації. Надалі пошук здійснюється по файлах пошукового індексу, тоді як вміст всіх знайдених документів автоматично завантажується з бази даних і відображається в клієнтській консолі.

2.2 Аналіз сучасних DLP-систем

Проведемо аналіз найпопулярніших DLP-систем, порівняємо їх функції та характеристики, розглянемо для яких цілей краще використовувати ці системи захисту [9, 11-13].

2.2.1 DLP-система SearchInform

DLP SearchInform – система з вбудованими аналітичними інструментами та орієнтована на дослідницьку та аналітичну роботу.

Функції DLP-системи:

– система в режимі реального часу аналізує комп'ютери співробітників в офісі і на видаленні;

– всі дії співробітників поміщаються в архів, після чого отримана інформація підлягає аналізу і, при необхідності, дії співробітників блокуються;

– блокування для пристроїв (передачі файлів або печаті);

– розслідування факту витоку інформації с використанням баз перехоплених даних для відновлення деталей минулих подій.

Являє собою велику кількість програм як для клієнтів, так і для серверів. Після її інсталяції на робочому столі з'являється безліч ярликів, що спочатку призводить користувача в замішання. Всі компоненти системи працюють на ОС Windows.

Переваги DLP-системи SearchInform:

– велика кількість різних каналів і способів перехоплення конфіденційної інформації;

– безліч додаткових функцій (аудит пристроїв, кодування, блокування різних об'єктів файлових систем);

– зручне обладнання пошукового рядку в архіві; багато різних опцій, видів пошуку, фільтрів, вибірок і угрупувань;

– відсутність обмежень при створенні безпекової політики;

– стабільна робота системи.

Система побудована як аналітична система, яка має потужні пошукові механізми, що працюють зі всіма видами конфіденційної інформації (рисунок 2.4) [11].

Рисунок 2.4 – Пошукові механізми DLP-системи SearchInform

Система має потужні механізми контролю діючих співробітників (рисунок 2.5).

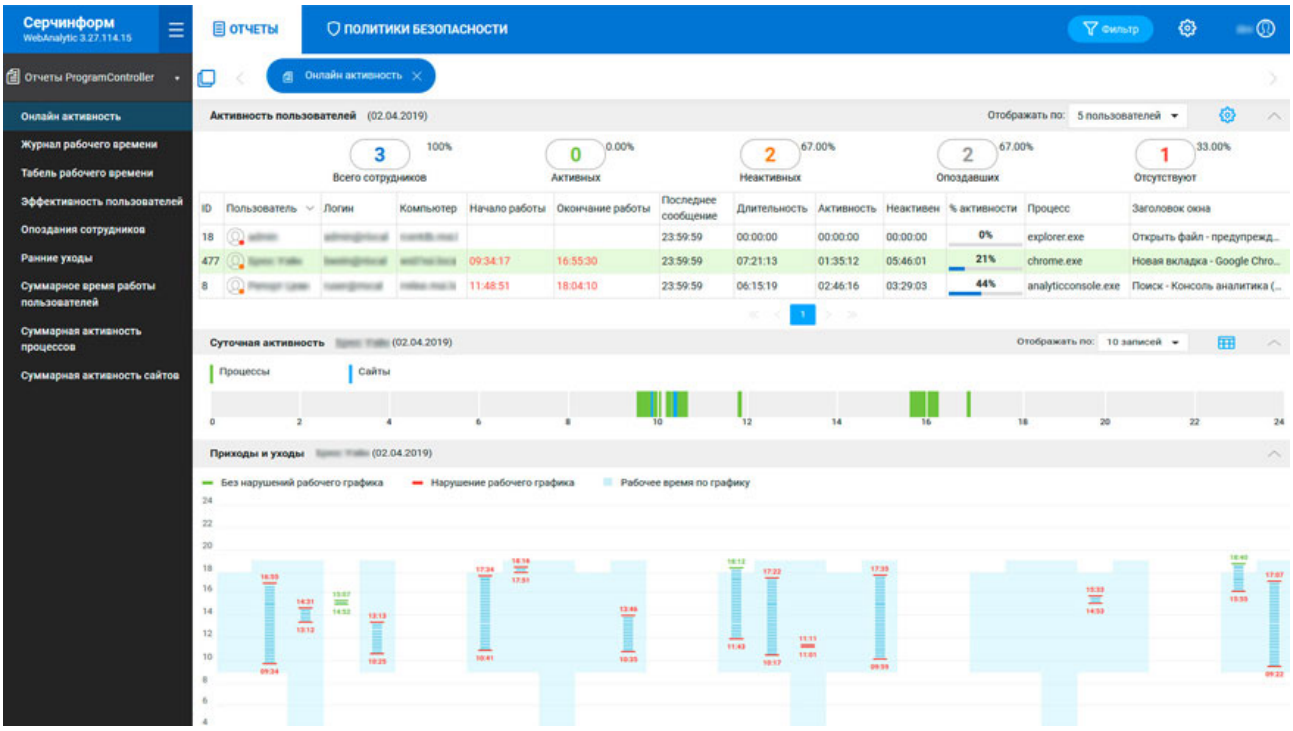

Рисунок 2.5 – Екран звітів контролю діючих співробітників

В якості недоліків можна виділити:

– не кожен канал, що перехоплює система, можна заблокувати;

– складна панель управління, велика кількості консолей, в яких потрібно встановити налаштування системи.

Таким чином аналіз даної системи показав недоліки функціональності блокування по вмісту (файли відправляються в карантин, поки адміністратор особисто не перегляне інцидент) і велика кількість консолей. Відповідно, встановлювати і працювати з системою достатньо важко.

2.2.2 DLP-система Falcongaze SecureTower

SecureTower є комплексним програмним рішенням для захисту бізнесу від внутрішніх загроз.

Основними функціями DLP-системи Falcongaze є:

– створення скріншотів робочих комп'ютерів (що дозволяє частково контролювати діяльність співробітників);

– достатньо широкий інструментарій перегляду та аналізу архіву;

– можливість переходу зі звіту до зазначеної в ньому події;

– можливість призначення категорії для інцидентів (досліджені, не досліджені, відкладені);

– можливість моніторингу месенджерів Телеграм та Viber.

В якості недоліків можна виділити:

– відсутність можливості блокування принтерів;

– відсутність блокування для мережевих каналів.

Перевагою даної системи є зручність у використанні. SecureTower легко встановлюється без поглибленого вивчення інструкцій. Системою зручно управляти, працювати з архівною інформацією.

Робочий екран центру контролю агентів SecureTower представлений на рисунку 2.6

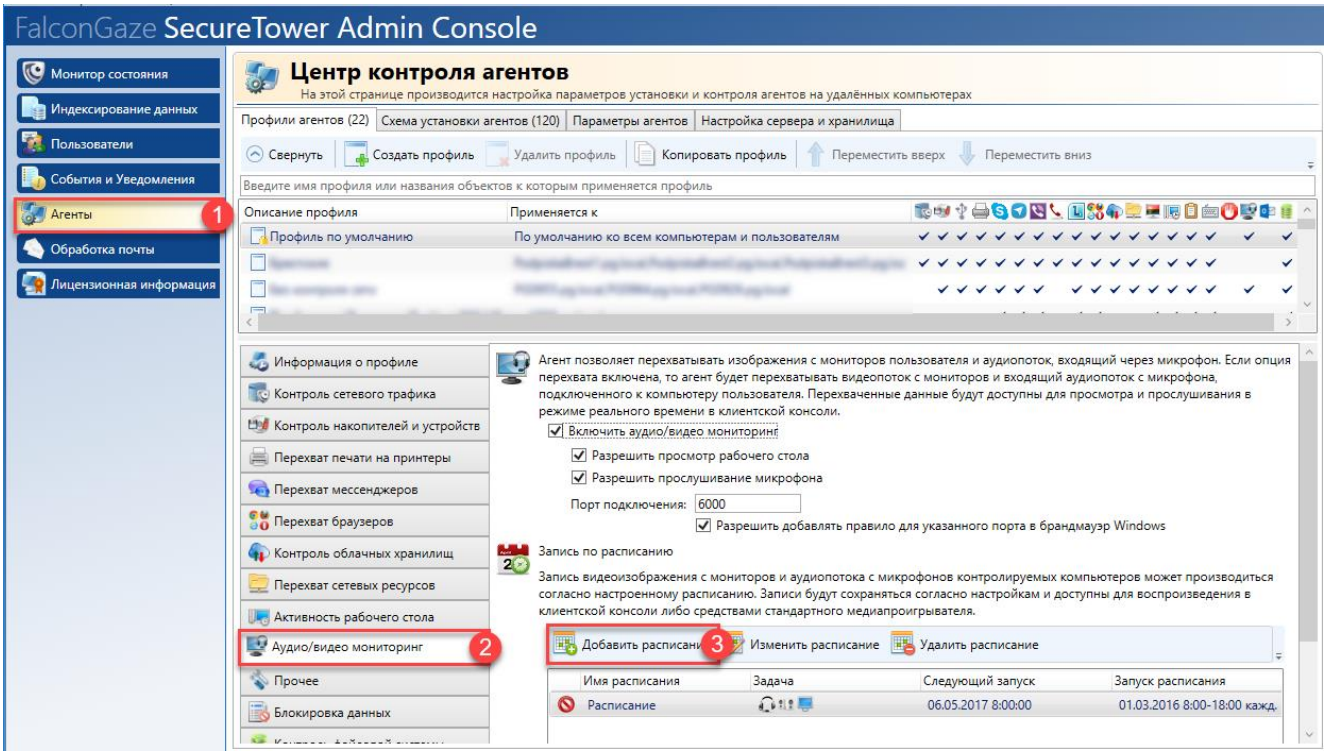

Рисунок 2.6 – Робочий екран центру контролю агентів SecureTower

Таким чином аналіз даної системи показав, що DLP-рішення Falcongaze SecureTower просте в установці і настройці, має зручний інтерфейс, розвинені засоби аналізу інформації, можливість моніторингу дій співробітників на робочих станціях, граф-аналізатор взаємозв'язків персоналу, масштабованість,

швидкий пошук по перехоплених даними, наочну систему звітності за різними критеріями, здійснює контроль більшої кількості каналів передачі даних. Але в системі не передбачена робота в розрив на рівні шлюзу, обмежені можливості блокування передачі конфіденційних даних (тільки smtp, http і https), відсутній модуль пошуку конфіденційних даних в мережі підприємства.

2.2.3 Система запобігання витоку даних Infowatch

Infowatch одна з поширеної DLP-систем. Пропонує повний спектр DLP-рішень як середнього бізнесу так і великих корпорацій та держструктур.

Основними перевагами рішень є:

– розвинений функціонал;
– унікальні запатентовані технології аналізу трафіку;
– гібридний аналіз;
– підтримка безлічі мов;
– вбудований довідник веб-ресурсів;
– масштабність;
– велика кількість попередньо встановлених конфігурацій та політик для різних галузей.

DLP-система має єдину консоль управління, здійснює контроль діючих співробітників, створює ролі користувачів.

Можливості системи Infowatch:

– аналіз креслень та конструкторської документації;
– канали перехвату повідомлень у Telegram, прикріплених файлів, голосових повідомлень;
– створення скриншотів робочих комп'ютерів співробітників;
– відкритий інтерфейс, інструменти для аналізу даних у архіві;
– можливість блокування діючих користувачів.

Робочий екран служби безпеки Infowatch представлений на рисунку 2.7.

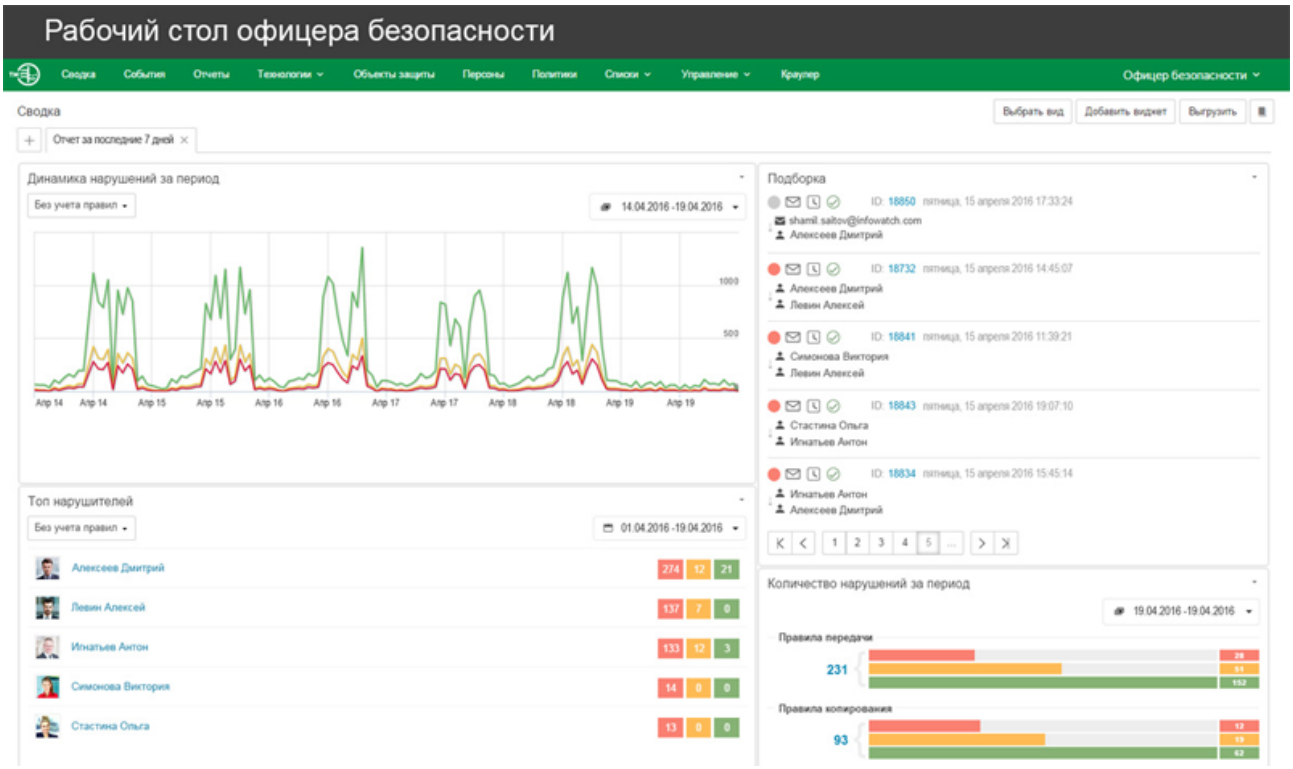

Рисунок 2.7 –Робочий екран служби безпеки Infowatch

Перевагами DLP-системи Infowatch є

– гарно побудований та комфортний інтерфейс користувача;
– простота експлуатації системи;
– структурованість перехоплених даних;
– наявні чіткої та зрозумілої інструкції;
– логічність структури та простота використання.

Але система має достатньо недоліків:

– велика кількість агентів робота яких не пов’язана між собою (для кожного додатку є свій агент);
– для роботи системи необхідні дві платформи Windows та Unix (різні монітори працюють на різних платформах, хоча і входять до однієї системи);
– при блокуванні діючих користувачі важко знайти в системі тіньові копії файлів;
– висока вартість.

Таким чином, DLP-система Infowatch має простий інтерфейс, часто оновляється розробниками та зручна в експлуатації, має функціональну програму моніторингу мережних каналів. Але функція блокування реалізована погано.

2.2.4 DLP-система Zecurion

Комплексна система захисту від витоків корпоративної інформації Zecurion DLP на ринку близько 10 років.

Функції системи Zecurion:

– контроль корпоративної електронної пошти, листів і вкладень, надісланих через сервіси веб-пошти, спілкування в соціальних мережах, на форумах і блогах (http/https);

– контроль повідомлень інтернет-месенджерів (більше десяти систем, включаючи Skype);

– контроль FTP, POP3, IMAP, SMTP та інших мережних каналів, файлів, що записуються на USB-накопичувачі і будь-які зовнішні пристрої;

– контроль друку на локальних і мережних принтерах;

– контроль наявності конфіденційних даних, що зберігаються на комп'ютерах користувачів і серверах, доступу до інформації, що зберігається на серверах, оптичних дисках.

Управління системою Zecurion здійснюється через єдину консоль для всіх дій. З її допомогою адміністратор може встановлювати, оновлювати і видаляти клієнтські модулі, переглядати дані тіньового копіювання, а також надавати миттєвий доступ за запитом співробітника.

Екран звіту DLP-системи Zecurion представлений на рисунку 2.8.

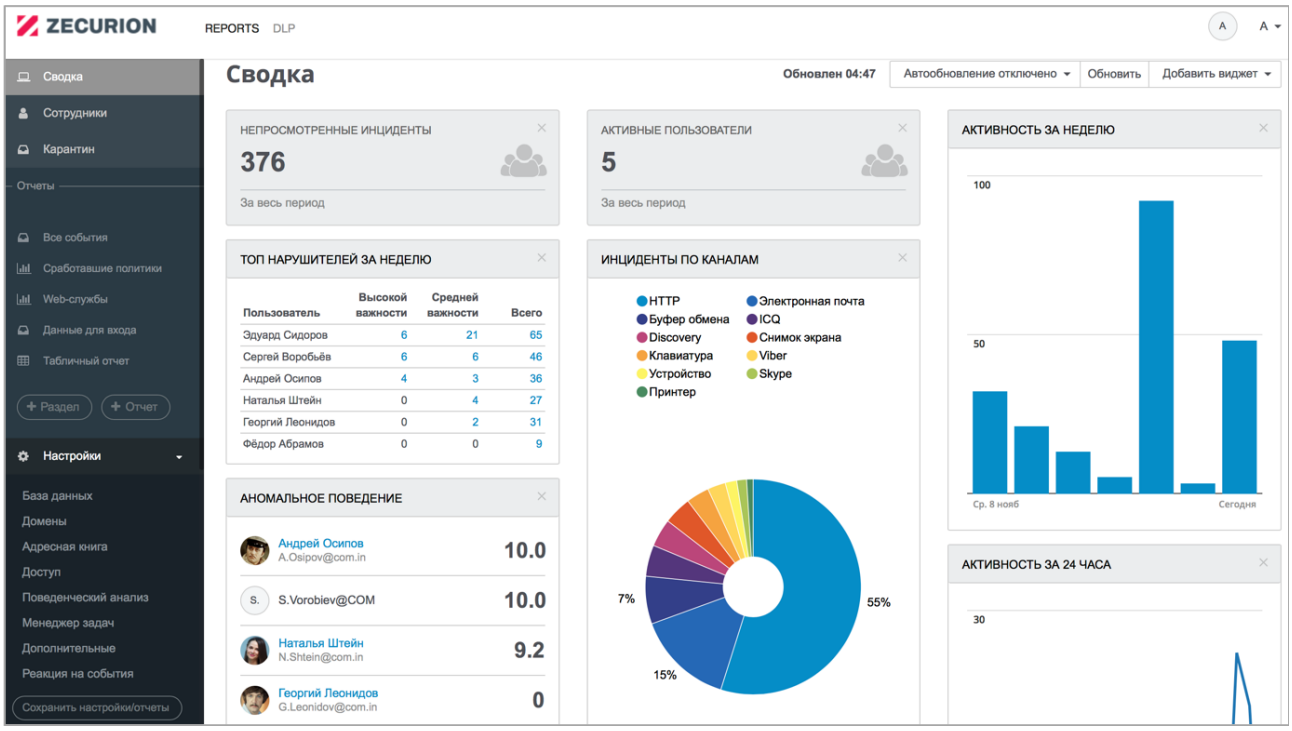

Рисунок 2.8 – Екран звіту DLP-системи Zecurion

Провести процедуру інсталяції та налаштування системи Zecurion може будь-який користувач, який навіть не має спеціальних навичок роботи з персональним комп'ютером. Існує велика кількість робочих моделей, включаючи повноцінне перехоплювання даних, захисту, проведення аудиту та блокування.

До недоліків Zecurion можна віднести наступні:

– нелогічна процедура поділу системи на ряд внутрішньо пов'язаних один з одним модулів;

– робота з архівними даними має багато складнощів, а саме дуже незручні вибірка інформації та ознайомлення з знайденими порушеннями;

– при роботі з агентом система починає зависати (причина нез'ясована).

Функціонал інструментів, які потрібні для роботи з архівними даними, недороблений, що є істотним недоліком DLP-системи.

2.2.7 DLP-система Symantec

DLP-система Symantec виконує 3 основні функції:

– контроль дій користувачів;

– моніторинг переміщення секретних даних по мережних каналах зв'язку;

– сканування локальної мережі на предмет невпорядкованого зберігання важливих документів.

Symantec забезпечує:

– виявлення конфіденційної інформації у відкритому доступі, в системах документообігу, поштового обміну, базах даних, на серверах і файлових сховищах;

– відстеження і блокування переміщення інформації усередині корпоративної мережі і за її межі;

– контроль веб-сервісів і хмарних сховищ, мобільних додатків, вхідних і вихідних повідомлень електронної пошти на мобільних пристроях.

Система має зручний інтерфейс, зрозумілий на інтуїтивному рівні функціонал управління політиками безпеки і інцидентами.

Екран контролю інцидентів DLP-системи представлений на рисунку 2.9.

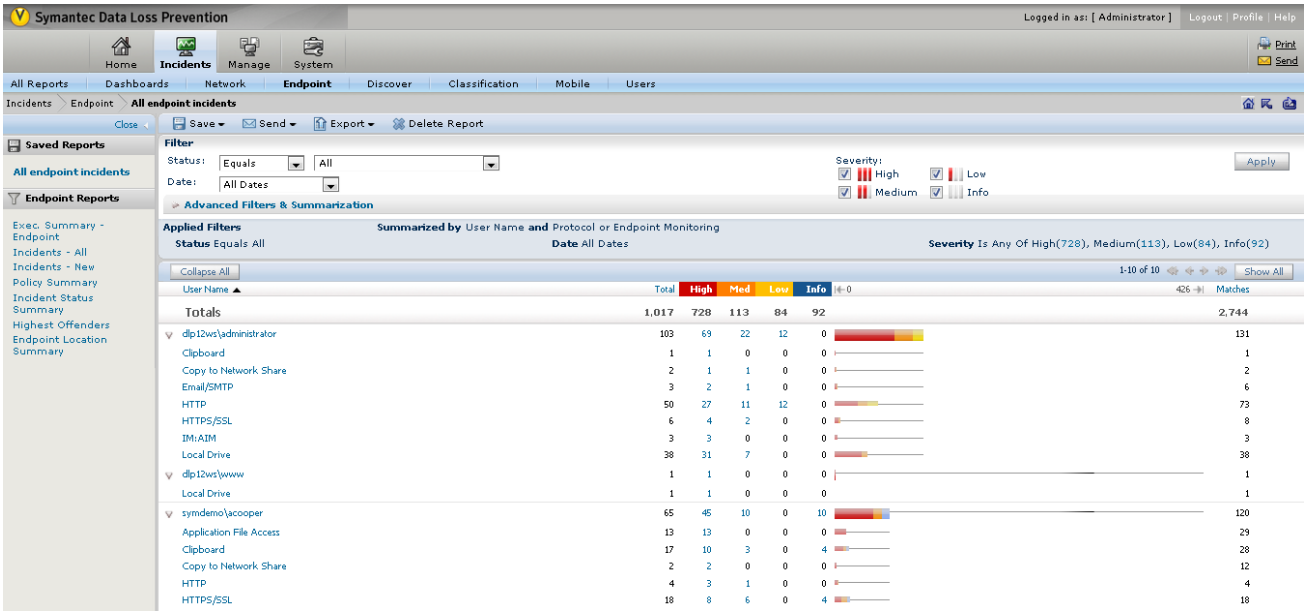

Рисунок 2.9 – Екран контролю інцидентів DLP-системи Symantec

Компанія Symantec є світовим лідером в розробці і впровадженні DLP систем і вже давно зарекомендувала себе на цьому ринку.

DLP-система Symantec є продуктом корпоративного класу зі зручним інтерфейсом, широкими можливостями контролю та аналітичними функціями.

2.3 Порівняльний аналіз сучасних DLP-систем

В роботі був проведений порівняльний аналіз розглянутих DLP-систем як по загальним характеристикам, так і функціоналу з виявлення інцидентів. Результати аналізу представлені в таблиці 2.1 [12-15].

Таблиця 2.1 – Порівняння сучасних DLP-систем

DLP-система / Параметр	Symantec	Zecurion	Infowatch	Falcongaze	SearchInform
Споживачі	Найбільші корпорації, що налічують до 100 тисяч працівників	Державний сектор, як маленькі, так і великі компанії	Як маленькі, так і великі компанії	Великі фірми і невеликі підприємства	Великі корпорації, співробітники малого і середнього бізнесу
Термін впровадження	Від одного дня (залежить від масштабу впровадження)	Від одного дня (залежить від масштабу впровадження)	2-7 робочих днів	Від пари годин до декількох днів	Від одного робочого дня (залежить від попередньої підготовки і числа станцій)
Місце встановлення	Сервер, клієнт	Сервер, клієнт	Сервер, клієнт	Сервер, клієнт	Сервер, клієнт
Надання	Навчання	Проведення	Послуги	Техпідтримка,	Допомога по

DLP-система / Параметр	Symantec	Zecurion	Infowatch	Falcongaze	SearchInform
послуг	персоналу за допомогою партнерів, впровадження	аудиту, надання консалтингових послуг, надання техпідтримки, проведення навчання	консалтингу в системі інформаційної безпеки	допомога по впровадженню, проведення навчання, а також надання допомоги по формуванню інформаційного захисту в організації	впровадженню, техпідтримка, навчання в навчальному центрі, аутсорсинг
Мова панелі управління	Англійська, японська, китайська, французька, російська	Англійська, російська	Українська, англійська, білоруська, російська	Англійська, французька, іспанська, італійська, корейська, турецька, російська	Англійська, французька, іспанська, італійська, корейська, турецька, російська
Запис в журнал	+	+	+	+	+
Збереження файлів (тіньове копіювання)	+	+ для Zlock і Zgate	+	+	+
Повідомлення адміністратора безпеки	+ по електронній пошті або системі реєстрація подій через SMTP, Syslog повідомлення	+ по електронній пошті	+ по електронній пошті	+ по електронній пошті	+ по електронній пошті
Блокування з'єднання	Так, будь-який протокол	всі контрольовані	Так, SMTP, HTTP, HTTPS	Так, SMTP, HTTP, SMTPs,	Так, тільки для SMTP

DLP-система / Параметр	Symantec	Zecurion	Infowatch	Falcongaze	SearchInform
	розпізнаний системою	канали (близько 150 штук)		HTTPS	
Автоматична зміна повідомлень	Так	Так	Ні	Ні	Ні

Проведений аналіз підтвердив той факт, що виробники програмних продуктів DLP світового рівня (такі як McAfee, Symantec, RSA та інші) представляють на ринок системи корпоративного класу зі зручним інтерфейсом, широкими можливостями контролю та аналітичними функціями.

Менш відомі компанії SearchInform, Falcongaze представляють DLP системи з достатньо широкими можливостями.

3 АНАЛІЗ МЕТОДІВ ІДЕНТИФІКАЦІЇ І АНАЛІЗУ КОНФІДЕНЦІЙНИХ ДАНИХ В DLP-СИСТЕМАХ

Під DLP-системами прийнято розуміти програмні продукти, що захищають організації від витоків конфіденційної інформації. Подібного роду системи створюють захищений цифровий «периметр» навколо організації, аналізуючи всю інформацію, що виходить, а в ряді випадків і вхідні дані. Контрольованої інформацією повинен бути не тільки інтернет-трафік, але і ряд інших інформаційних потоків: документи, які виносяться за межі контуру безпеки, що захищається, на зовнішніх носіях, роздруковуються на принтерах, що відправляються на мобільні носії і т.п.

Оскільки DLP-система повинна перешкоджати витоку конфіденційної інформації, то вона в обов'язковому порядку має вбудовані механізми визначення ступеня конфіденційності документа, виявленого в перехопленому трафіку. Як правило, найбільш поширені два способи: шляхом аналізу спеціальних маркерів документа і шляхом аналізу вмісту документа. В даний час більш поширений другий варіант, оскільки він стійкий перед модифікаціями, внесеними в документ перед його відправкою, а також дозволяє легко розширювати число конфіденційних документів, з якими може працювати система.

DLP-системи перехоплюють весь трафік, що виходить за межі корпоративної мережі підприємств, і аналізують його на предмет наявності конфіденційної інформації. У передових DLP-системах для виявлення конфіденційних даних зазвичай використовуються такі технології як цифрові відбитки, лінгвістичний аналіз, аналіз графічних файлів (OCR), технології, що самонавчаються, і ін.

Технології категоризації інформації складають ядро DLP-систем. Кожен виробник вважає свої методи детектування конфіденційної інформації унікальними, захищає їх патентами і придумує для них спеціальні торгові

марки. Адже інші, відмінні від цих технологій, елементи архітектури (перехоплювачі протоколів, парсери форматів, управління інцидентами і сховища даних) у більшості виробників ідентичні, а у великих компаній навіть інтегровані з іншими продуктами безпеки інформаційної інфраструктури. В основному для категоризації даних в продуктах по захисту корпоративної інформації від витоків використовуються дві основні групи технологій - лінгвістичний (морфологічний, семантичний) аналіз і статистичні методи (Digital Fingerprints, Document DNA, антиплагіат) [16]. Кожна технологія має свої сильні і слабкі сторони, які визначають область їх застосування.

3.1 Принципи лінгвістичного аналізу інформації

Прообразом сучасних DLP-систем можна вважати використання в поштових серверах для блокування вихідних електронних повідомлень слів, що зупиняють передачу ("секретно", "конфіденційно" і тому подібних). Але цей метод не може захистити від зловмисників, так як доволі просто видалити з документа ці слова, найчастіше винесені в окремий гриф документу.

Для захисту електронної пошти від спаму на початку цього століття були запропоновані email-фільтри, які поклали основу розвитку лінгвістичних технологій.

На початку століття почалася лінгвістична війна між спамерами і антіспамерами. Для обходу фільтрів, які базуються на ключових словах, здійснювалась заміна букв на схожі букви з інших кодувань або цифри, трансліт, випадковим чином розставлені пробіли, підкреслення або переходи рядків в тексті. Антіспамери досить швидко навчилися боротися з такими методами, але тоді з'явився графічний спам і інші різновиди небажаної кореспонденції.

Але для боротьби зі спамом досить ділити інформаційний потік на дві категорії: спам і не спам. Для захисту корпоративних даних від витоків цього недостатньо - не можна просто ділити інформацію на конфіденційну і

неконфіденційну. Необхідно вміти класифікувати інформацію за функціональною приналежністю (фінансова, виробнича, технологічна, комерційна, маркетингова), а всередині класів - категоризувати її за рівнем доступу (для вільного поширення, для обмеженого доступу, для службового використання, секретна, цілком таємна) [17].

В системах лінгвістичного аналізу почали використовувати контекстні методи, коли проводиться пошук не тільки конкретних слів, але і в поєднанні з якими іншими словами використовується конкретний термін, тобто в якому контексті.

Більшість сучасних систем лінгвістичного аналізу використовують не тільки контекстний аналіз, але і семантичний аналіз тексту. Ці технології працюють тим ефективніше, чим більше аналізований фрагмент. На великому фрагменті тексту точніше проводиться аналіз, з більшою ймовірністю визначається категорія і клас документа [16]. При аналізі коротких повідомлень (SMS, повідомлення месенджерів) кращім рішенням є використання ключових слів.

Розглянемо переваги лінгвістичних технологій.

1. Лінгвістичні технології працюють безпосередньо з вмістом документів, тобто не зважаючи на те, де і як був створений документ, який на ньому гриф і як називається файл – при наявності необхідного збігу документи захищаються негайно. Конфіденційні документи, які створені і використовуються всередині компанії, можуть мати специфічні імена, бути грифовані або помічені. Але вхідні документи можуть не мати прийнятих в організації грифів і міток. Чернетки (якщо вони, звичайно, не створюються в системі захищеного документообігу) теж можуть вже містити конфіденційну інформацію, але ще не містити необхідних грифів та позначок.

2. Перевагою лінгвістичних технологій є їх здатність до навчання.

3. Гідністю лінгвістичних технологій є їх масштабованість. Швидкість обробки інформації пропорційна її кількості і абсолютно не залежить від кількості категорій.

4. Можливість детектувати в інформаційних потоках категорії, не пов'язані з документами, що знаходяться всередині компанії. Інструмент для контролю вмісту інформаційних потоків може визначати такі категорії, як протиправна діяльність (піратство, поширення заборонених товарів), використання інфраструктури компанії у власних цілях, нанесення шкоди іміджу компанії (наприклад, поширення ганебних чуток) і так далі [16].

Лінгвістичних технологій мають також і недоліки.

1. Основним недоліком лінгвістичних технологій є їх залежність від мови. Неможливо використовувати лінгвістичні методи, розроблені для однієї мови, з метою аналізу іншої. Особливо це було помітно при виході на український ринок міжнародних виробників. Недостатньо було перевести на українську мову категорії і ключові слова - в англійській мові зовсім інший словотвір. У Німеччині американських виробників лінгвістичних технологій зустріла інша проблема - так звані "компаунди", складові слова. У німецькій мові прийнято приєднувати визначення до головного слова, в результаті чого виходять слова, що складаються з десятка коренів. В англійській мові такого немає.

Крім того складно обробляти лінгвістичними технологіями мультимовні тексти. Однак з двома мовами більшість методів все-таки справляються, зазвичай це національна мова + англійська - для більшості бізнес-завдань цього цілком достатньо.

2. Ще одним недоліком лінгвістичних технологій для контролю всього спектру корпоративної конфіденційної інформації є те, що не вся конфіденційна інформація знаходиться в вигляді зв'язкових текстів. Отримана інформація найчастіше містить прізвища, адреси, назви компаній, а також цифрову інформацію - номери рахунків, кредитних карт, їх баланс та інше. Обробка подібних даних за допомогою лінгвістики неможлива. Також до інформації, яку неможливо перевірити лінгвістичним аналізом відносяться креслення, програмні коди і медійні (відео/аудіо) файли, в яких часто міститься інтелектуальна власність.

3. Найбільшим недоліком лінгвістичних технологій є імовірнісний підхід до категоризації. Хоча навчанням системи можна досягти 92-95% точності, але можливе помилкове зарахування інформації не до тієї категорії з усіма можливими наслідками (витік або переривання легітимного процесу).

4. Також до недоліків можна віднести складність розробки технології. Розробка серйозного лінгвістичного рішення з категоризацією текстів більш ніж за двома категоріями - наукомісткий і досить складний технологічно процес. Прикладна лінгвістика швидко розвивається, але сьогодні на ринку присутні одиниці працездатних рішень категоризації.

3.2 Статистичні методи аналізу інформації

Ще в 70-х роках минулого століття лінгвістів зацікавила задача комп'ютерного пошуку значущих цитат [16]. Рішення цієї задачі було основане на побудові геш-функцій. Текст розбивався на частки певного розміру, з кожного з яких знімався геш. Якщо деяка послідовність гешів зустрічалася в двох текстах одночасно, то з великою ймовірністю тексти в цих областях збігалися.

Статистичні технології відносяться до текстів не як до зв'язної послідовності слів, а як до довільної послідовності символів, тому однаково добре працюють з текстами будь-якою мовою. Оскільки будь-який цифровий об'єкт теж послідовність символів, то ті ж методи можуть застосовуватися для аналізу не тільки текстової інформації, але і будь-яких цифрових об'єктів. Статистичні методи є ефективними засобами захисту від витоку аудіо і відео, що активно застосовуються в музичних студіях і кінокомпаніях.

Ключовою характеристикою складного гешу, що знімається з об'єкта, що захищається (Digital Fingerprint або Document DNA), є крок, з яким знімається геш-функція. Але для зберігання геш-функцій мільйонів документів знадобиться достатня кількість дискового простору. Від кроку хешу залежить їх

кількість - чим менше крок, тим більше геш-функцій. Однак, якщо збільшувати розмір кроку, то збільшується ймовірність пропуску конфіденційної інформації.

З іншого боку, якщо для збільшення точності детектив брати дуже невеликий крок в кілька символів, то можна збільшити кількість помилкових спрацьовувань та обсяг, необхідний для зберігання гешей.

Зазвичай виробники самі рекомендують певний оптимальний крок зняття гешей, щоб розмір цитати був достатній і при цьому вага самого відбитка була невелика - від 3% (текст) до 15% (стисле відео). У деяких продуктах виробники дозволяють змінювати розмір значущості цитати, тобто збільшувати або зменшувати крок хешу.

Розглянемо переваги даної технологій

1. Щоб статистичний метод зміг з хорошою точністю (до 100%) сказати, що в файлі, що перевіряється, є значуща цитата для детектування потрібен об'єкт-зразок. Тобто необхідно категоризувати файли перед зняттям відбитків. Це сильно полегшує захист інформації в разі, якщо на підприємстві зберігаються файли, які нечасто змінюються і вже категоризовані. Тоді досить з кожного з цих файлів зняти відбиток, і система буде блокувати пересилку або копіювання файлів, що містять значущі цитати із зразків.

2. Перевагою також є незалежність статистичних методів від мови тексту і нетекстової інформації. Даний метод можливо використовувати при захисті статичних цифрових об'єктів будь-якого типу - картинок, аудіо/відео, баз даних.

Розглянемо недоліки технології.

1. Простота навчання системи перекладає на користувача відповідальність. Якщо раптом конфіденційний файл виявився не в тому місці або не був проіндексований по недбалості або злому намірі, то система не буде його захищати. Відповідно, компанії, що піклуються про захист конфіденційної інформації від витоку, повинні передбачити процедуру контролю того, як індексуються DLP-системою конфіденційні файли.

2. Ще один недолік - фізичний розмір відбитка та кількість відбитків-зразків. При порівнянні вихідного листа з мільйонами відбитків-зразків робота поштової системи істотно сповільнюється, викликаючи затримки в десятки хвилин.

3. Час зняття відбитка безпосередньо залежить від розміру файлу і його формату. Для текстового документа це займає частки секунди, для півторагодинного MP4-фільму - десятки секунд. Тому, якщо об'єкт динамічний та постійно, то виникає проблема: після кожної зміни об'єкта з нього потрібно зняти новий відбиток. Якщо час зняття відбитка більше, ніж час незмінності об'єкта, то завдання рішення не має.

3.3 Технології аналізу конфіденційних даних в DLP системах

В DLP-системах як правило використовують три технології ідентифікації:

– імовірнісний;

– детермінований;

– комбінований.

Системи, засновані на першому методі, здебільшого використовують лінгвістичний аналіз інформації і «цифрові відбитки» даних. Такі системи прості в реалізації, але з-за високого рівня помилкових спрацьовувань є недостатньо ефективними.

Системи, що використовують детермінований підхід (мітки файлів), дуже надійні, але їм не вистачає гнучкості.

Комбінований підхід поєднує обидва методи з аудитом середовища зберігання і обробки даних, що дає можливість досягти оптимального вирішення проблеми захисту конфіденційності інформації.

Більшість компаній-лідерів на ринку використовують в своїх розробках технології як лінгвістичні, так і статистичні методи аналізу, при цьому одна з них є основною, а інша - додатковою. Це пов'язано з тим, що спочатку продукти компанії використовували тільки одну технологію, в якій компанія

просунулася далі, а потім, на вимогу ринку, була підключена друга. Так, раніше компанія InfoWatch використовувала тільки ліцензовану лінгвістичну технологію Morph-OLogic, а Websense - технологію PreciseID, що відноситься до категорії Digital Fingerprint, але зараз компанії використовують обидва методи. Для кращого виявлення конфіденційної інформації ці дві технології потрібно використовувати не паралельно, а послідовно. Так, відбитки краще впораються з визначенням типу документа (наприклад, це договір або балансова відомість). Потім можна підключати вже лінгвістичну базу, створену спеціально для цієї категорії. Це сильно зекономить обчислювальні ресурси.

В сучасних системах DLP застосовуються складні механізми аналізу: порівняння по шаблонах з використанням словників і регулярних виразів, лінгвістичний і контекстний аналіз, цифрові відбитки.

Словники і шаблони зручно застосовувати в конкретних областях, наприклад, для контролю номерів кредитних карт і інших персональних даних [15, 16].

У лінгвістичному і контекстному аналізі використовуються морфологія і статистичні моделі, враховується контекст, характер відправника і одержувача інформації. Цей метод також застосовують для динамічних даних. Цифрові відбитки (аналогічні сигнатурам в антивірусних продуктах) підходять для контролю статичних даних, наприклад, для захисту інтелектуальної власності.

Для пошуку конфіденційних даних використовують наступні методи:

− сигнатури – пошук "заборонених" слів, послідовності стоп-слів;

− лінгвістичні методи;

− цифрові відбитки (статистичний метод) – геш-функції зразків конфіденційних документів;

− регулярні вирази – дозволяють знаходити збіги за формою даних (а не за самими даними), типу номерів кредитних карток;

– порівняння за типами файлів. Політиками безпеки може бути заборонена відправка зовні деяких типів файлів. При цьому якщо користувач

змінить розширення файлу, то система все одно повинна «впізнати» тип файлу і вжити необхідних заходів;

− мітки – установка на файли, що містять конфіденційну інформацію, спеціальних міток;

– аналіз інформації по діям користувачів (поведінковий);

− штучний інтелект – самонавчальний алгоритм аналізу даних.

Метод аналізу за допомогою сигнатур є пошуком деякої послідовності символів (стоп-слів). Найчастіше ці системи налаштовані на пошук декількох слів або частоту їх появи в тексті. Метод аналізу масок є розширенням технології сигнатур і є пошуком такого змісту, який неможливо точно вказати в базі "стоп-слів", але можна вказати його елемент або структуру. До такої інформації слід віднести будь-які коди, які характеризують персону або підприємство: ІНН, номери рахунків документів та інше.

Технологія лінгвістичного аналізу автоматично визначає тематику і ступінь конфіденційності аналізованого фрагмента інформації на підставі термінів, що зустрічаються в ньому, і їх поєднань. Лінгвістичний аналіз виконується на основі заздалегідь створеної бази контентної фільтрації (БКФ). База контентної фільтрації – це база даних, яка представляє собою виділений на основі імовірнісних і математичних методів ієрархічно організований список категорій, що містить слова і вирази, наявність яких в документі дозволяє визначити тематику і ступінь конфіденційності інформації [18].

БКФ не тільки описує категорії інформації, але і враховує різні атрибути її конфіденційності, а також специфіку діяльності компанії, вимоги до безпеки. В результаті проведення лінгвістичного аналізу інформації автоматично ставиться у відповідність категорії, що відповідають її тематиці і змісту.

Точність ідентифікації конфіденційних даних за допомогою технології лінгвістичного аналізу залежать від створеної БКФ, на основі якої здійснюється аналіз.

Створення бази контентної фільтрації починають з побудови її структури дерева контентних категорій (рубрикатору). Це ієрархічний список з

категоріями і підкатегоріями, які наповнюються списком термінів, ключових слів, словосполучень і фраз, поява яких в аналізованому фрагменті інформації вказує на його приналежність до певної контентної категорії.

Для кожного терміну/словосполучення в категорії ставиться у відповідність вага. Рішення про те, чи відноситься текст до категорії, приймається за порівнянням суми ваги термінів, знайдених в тексті, з порогом для цієї категорії. Для забезпечення якісної категоризації необхідно постійно редагувати категорії, додавати і/або видаляти терміни і словосполучення, змінювати їх вагу.

Технології цифрових відбитків основана на створенні цифрових відбитків конфіденційних документів на математичних перетворень початкового файлу. Таким перетворенням може бути геш-функція, але найчастіше алгоритми перетворень виробниками не розкриваються. При цьому відбитки файлу, що передається, і «модельного» файлу можуть співпадати не обов’язково на 100%, відсоток збігу може задаватися. Технології цифрових відбитків стійкі до редагування файлів і використовуються для захисту багатьох типів файлів: текстових, графічних, аудіо, відео.

Кількість помилкових спрацьовувань для даного методжу не перевищує одиниць відсотків (для порівняння інші технології дають 20-30% помилкових спрацьовувань).

Пошук за регулярними виразами – система синтаксичного розбору текстових фрагментів за формалізованим шаблоном, що заснована на системі запису зразків для пошуку. Даний метод використовують для пошуку номерів телефонів, кредитних карт, e-mail адрес, номерів документів.

Статистичні методи здійснюють пошук інформації не як окремого тексту, а як послідовності бітів, тому однаково працюють з об’єкт різних типів та текстами на будь-яких мовах.

Контейнерний аналіз (аналіз по мітках) оцінює властивості файлу або іншого контейнера (архіву), в якому знаходиться інформація. Кожен контейнер містить мітку, яка однозначно визначає тип контенту, що міститься усередині.

Даний метод практично не вимагають обчислювальних ресурсів для аналізу інформації, так як мітка повністю описує права користувача на переміщення контенту.

Найбільш перспективним є використання алгоритму аналізу даних Vector Machine Learning на основі штучного інтелекту. VML здатний самостійно ідентифікувати дані, доступ до яких повинен бути обмежений. Використовуючи зразки наявних даних, програмне рішення на базі алгоритмів VML можна навчити дізнаватися ключові характеристики і визначати внутрішні відмінності конфіденційних і неконфіденційних даних.

Згідно з дослідженнями компанії ABI Research вважає, що уряд і сфера оборони, банківські системи і ринок технологій стануть головними силами і користувачами, які будуть просувати технологій машинного навчання [18]. DLP-системи разом з алгоритмом глибокого навчання є двома найвідомішими технологіями в області кібербезпеки.

Розробники DLP-систем, такі як Symantec, продовжують роботу з перетворення деяких з своїх рішень на технологій машинного навчання.

Великі компанії, такі як IBM, змінять спосіб застосування машинного навчання в кожному секторі ринку, починаючи від охорони здоров'я і закінчуючи корпоративної аналітикою і кібербезпекою. Такі компанії, як Gurucul, Niara, Splunk, StatusToday, Trudera і Vectra Networks намагаються взяти на себе провідну роль в застосуванні інноваційних програм DLP-систем. Інші учасники ринку, такі як Deep Instinct і Spark Cognition застосовують більш функціональні моделі, глибоке навчання і обробку природної мови.

4 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИБОРУ СИСТЕМИ ЗАХИСТУ ВІД ВИТОКУ КОНФІДЕНЦІЙНИХ ДАНИХ

4.1 Рекомендацій щодо вибору DLP-систем

Для багатьох компаній актуальна проблема захисту від витоку корпоративний (конфіденційної) інформації. Рішення даної проблеми можливо при використанні в корпоративній мережі організації системи захисту від витоку конфіденційних даних (DLP-системи). Тому проблема вибору менеджерами і співробітниками служб безпеки DLP-системи, яка б задовольняла їх вимогам та була в змозі захисти дані від крадіжок і витоків, є досить актуальною.

Вибір DLP залежить від поставлених перед системою завдань. Універсального алгоритму роботи системи не буває - кожен інструмент підбирається індивідуально, тестується і налаштовується для вирішення конкретних завдань.

Перед вибором DLP-системи потрібно визначити:

– критерії порівняння;

– основні канали передачі інформації, які необхідно контролювати;

– 2-3 системи для тестування;

– період тестування.

В якості критеріїв вибору системи можна обрати такі:

– склад продукту;

– масштабність системи (кількість робочих місць (користувачів) компанії);

– наявність необхідних модулів для вирішення конкретного спектру завдань;

– кількість каналів, що контролюються;

– функціонал і об'єкти спостереження системи;

– уніфікованість управління системою;

– спроможність здійснювати активний захист;

– використання системою методів аналізу інформації за вмістом та контентом, категорювання інформації;

– надійність і швидкість роботи системи;

– аналітичні можливості;

– підтримки спеціальних технологій, сумісність в іншими продуктами і рішеннями, можливість і умови інтеграції в діючу інфраструктуру;

– наявність, якість та швидкість технічної підтримки;

– експертиза, досвід та надійність вендора;

– ціна, вартість розгортання та обслуговування системи.

1. Склад продукту обирається виходячи з завдань, які покладаються на систему та результатів, що планується отримати від застосування системи.

2. Масштабність системи обирається виходячи з кількості наявних робочих місць (користувачів) компанії з урахуванням тенденцій розвитку компанії на найближчі 10 років.

3. Наявність необхідних модулів для вирішення конкретного спектру завдань обирається в залежності від задач, які покладаються на систему та враховуючи можливість поетапного підключення різних модулів для контролю різних каналів.

4. Для визначення кількості контрольованих каналів необхідно перелічити канали, які колектив використовує для роботи і особистого спілкування, а також види інформації, що обробляється та зберігається в компанії: персональні дані, комерційна таємниця, конфіденційна документація і т.п. Необхідно визначити у розробника DLP-системи (вендора) політику ліцензування і можливість покупки окремих модулів, при цьому враховуючи можливість використання в організації в майбутньому нових каналів комунікації. Кращим буде виробник продукт якого має широкий набір модулів, з яких можна обрати окремі елементи в будь-який час.

Далі потрібно визначити, які канали блокувати, а які контролювати. Можна заблокувати все, що не відноситься до роботи. Але тоді службі безпеки буде складніше контролювати людей, які хочуть цілеспрямовано злити

інформацію, неважливо яким способом. При впровадженні DLP-рішення оцінюйте пріоритети захисту: перекрити можливі способи передачі інформації або відстежити потенційного порушника.

Також потрібно визначити, які канали необхідно блокувати, а які контролювати. Можна заблокувати все, що не відноситься до роботи. Але тоді службі безпеки буде складніше контролювати співробітників, які хочуть цілеспрямовано здійснити витік інформації, неважливо яким способом. При впровадженні DLP-рішення оцінюйте пріоритети захисту: перекрити можливі способи передачі інформації або відстежити потенційного порушника (рисунок 4.1).

Рисунок 4.1 Вибір варіанту перекриття каналів

Кращі сучасні DLP мають функцію контролю великої кількості мережевих каналів.

5. При виборі функціоналу і об'єктів спостереження системи краще застосовувати впровадження сучасних DLP-рішень, що допоможе:

контролювати всі канали передачі інформації;

знаходити порушення - загальні і специфічні;

формувати зрозумілі звіти за результатами перевірок;

не включати в звіти події, які не пов'язані з погрозами;

аналізувати пов’язані події і встановлювати коло причетних осіб;

контролювати робочий час: скільки і як продуктивно працюють співробітники;

шифрувати дані при спробі їх передачі за межі компанії;

блокувати сервіси і канали на вимогу.

6. Уніфікованість управління системою дозволяє спрощувати обслуговування, настройку та роботу з системою. Також, як правило, дає можливість використовувати обслуговуючий персонал з меншою кваліфікацією.

7. Можливість використання системою різних методів аналізу інформації дозволяє охватити аналізом більш різні категорії та типи контролюємої інформації;

8. У DLP-системах є два головних робочих режими: активний і пасивний. Перший варіант вважається основним. При ньому блокуються дії, які порушують політику безпеки організації. Другий варіант застосовується в момент настроювання системи для того, щоб провести перевірку і відкоригувати настройки - порушення в системі фіксуються, але не накладаються обмеження.

Спроможність здійснювати активний захист дозволяє не тільки спостерігати за перебігом документів та інформації, але і здійснювати активний захист від витоку.

9. Для визначення надійності і швидкості роботи системи необхідно провести тестування обраного DLP-рішення. Тестування навантаження краще проводити на максимальній кількості машин. Практично будь-яка DLP буде добре працювати на 10-15 комп'ютерах, але не факт, що вона зможе контролювати 100, 500 або 5000 робочих станцій без збоїв і перевантаження системи.

Терміни повноцінного тестування DLP - від двох тижнів до місяця. За цей час можна зрозуміти, як система справляється з об'ємними навантаженнями, які специфічні настройки і канали краще використовувати. За результатами такої перевірки керівництву можна надати звіт, на прикладі якого буде видно роботу впровадженого рішення і знайдені порушення.

Також необхідно порівняти обсяги і якість перехоплення даних системами, що тестуються під навантаженням. Результати можуть відрізнятися через неправильні налаштування, різних механізмів перехоплення. Саме тому, якщо є технічна можливість, краще тестувати обрані рішення одночасно. Це допоможе коректно зіставити результати.

10. При тестуванні систем потрібно з’ясувати, як точно і тонко настроюється система. Якщо DLP-рішення не можна налаштувати під специфічні запити і документи, значить не все порушення будуть знайдені і як підсумок - можливий витік секретної інформації.

11. На пошук загроз впливають також автоматизовані можливості DLP. Якщо у системи є інструменти не тільки для фразового пошуку, але і для комплексного пошуку, а також пошуку по атрибутах, регулярних виразах, за тематичними словниками і т.п., вона знайде більше порушень. При цьому рішення автоматично виключить з результатів випадки, які не пов'язані з витоками і крадіжками.

12. Крім того, необхідно оцінити інформативність звітів: чим зрозуміліше і наочніше аналітичні повідомлення системи, тим менше часу співробітникам потрібно на розбір і систематизацію. З даними, підтвердженими наочно, зручно звітувати перед керівництвом.

13. При виборі DLP-системи обов'язково слід розглянути інструментарій для розслідування інцидентів. Аудит файлової системи, відеозапис дій користувача, аудіозапис, контроль продуктивності і знімки з веб-камери допоможуть відтворити порушення і однозначно встановити винного. Додатковий плюс системи є можливість ретроспективного аналізу, який встановить ланцюг подій з самого початку і покаже коло осіб, причетних до порушення.

14. Оперативна і якісна технічна підтримка допоможе швидко вирішувати виникаючі проблеми з системою. Якщо компанія не поспішає відповідати на питання під час тестування, то, ймовірно, після покупки DLP ситуація стане ще гірше.

При оцінці техпідтримки необхідно врахувати:

– якість роботи техпідтримки, швидкість реакції на запит;

– швидкість усунення проблеми;

– можливість виїзду фахівця до клієнта (актуально для регіональних компаній);

– допомога при впровадженні, налаштуванні і тестуванні системи. Якщо вендор допомагає співробітникам служби безпеки ретельно розібратися в DLP, система зі старту працює правильно і перехоплює більше інцидентів.

15. Надійність розробника і широкі можливості налаштування DLP - суттєвий фактор, який обов'язково потрібно враховувати при виборі системи захисту. Також при цьому необхідно оцінювати:

– набір попередньо встановлених політик безпеки. Компанії, які давно працюють на ринку, пропонують клієнтам багато універсальних налаштувань та інструментів. Це розширює можливості DLP і спрощує персональну підготовку до запуску софта;

– регулярні оновлення, стійкість до кризових явищ. Технології постійно розвиваються, і система повинна оперативно підбудовувалася під нові програми, месенджери і інші канали передачі інформації.

– галузеві практики. Чим більше можливостей для детальних налаштуваннях, тим більша ймовірність того, що система знайде специфічні порушення. Досвідчені розробники імпортують клієнту готові або налаштовують нові спеціалізовані політики безпеки.

– наявність представництв в регіонах. Як і з техпітримкою: чим ближче розробник, тим швидше призначаються зустрічі і усуваються проблеми.

– спілкування з чинними клієнтами надасть додаткову інформацію про надійність розробника. Контакти компанії можна взяти у вендора. Якщо постачальник DLP-послуг відмовляється знайомити з клієнтом, значить, він або недавно на ринку, або не впевнений в продукті.

16. Ціна і вартість встановлення та обслуговування системи. Витрати на систему захисту повинні співвідноситися з потребами і можливостями

компанії, якістю DLP. Не у всіх компаній початковий пакет послуг включає подальше обслуговування і оновлення системи. При оцінці витрат враховуйте, що вартість володіння системою складається з декількох компонентів (рисунок 4.2).

Рисунок 4.2 Компоненти вартості DLP системи

Перед обов'язковим тестуванням DLP-рішень необхідно:

– скласти програму та методику випробувань;

– обрати 2-3 системи для тестування;

– порівняти результати за всіма критеріями;

– обрати DLP-систему з урахуванням розглянутих критеріїв та характеристик.

4.2 Проблемні питання при застосуванні DLP-систем

Проведемо аналіз проблем, які можуть виникнути при використанні DLP.

Як правило, для кожного контрольованого користувача (хоста), що знаходиться під контролем DLP-системи, налаштовується свій індивідуальний набір перерахованих вище функцій. Використання всіх наявних функцій на всіх контрольованих користувачів може досить швидко і значно збільшити розмір

бази даних DLP-системи, в результаті чого формування звітів системою може стати довгим. Апаратні ресурси, які обслуговують бази даних DLP-системи, також мають обмеження, тому система може бути перевантажена надмірною, непотрібною інформацією.

Крім того, використання на підприємстві DLP-систем повинно бути відповідним чином регламентовано, а також що некоректне використання інформації, отриманої з використанням DLP-системи, може спричинити для підприємства негативні правові наслідки.

Найбільш вузькими місцями в покритті DLP-системами залишаються особисті пристрої співробітників, що знаходяться поза адміністративним контролєм підприємства, на яких допускається зберігання і доступ до корпоративної інформації і корпоративних інформаційних систем. Також проблемним питанням є використання інформаційних систем (ІС), що знаходяться в публічних або гібридних хмарах. У цих випадках захист від запобігання витоків корпоративної інформації повинний ґрунтуватися на відповідних архітектурах віддаленого доступу, адміністративних методах захисту і засобах захисту, розмежування доступу і фіксації дій самих ІС.

Крім того DLP-рішення мають ще один суттєвий недолік – їх вартість, що заважає широкому використанню в малому і середньому бізнесі.

Другим проблемним питанням є те, що через складність і високі вимоги DLP-системи безпеки часто не виправдовують очікування керівництва організацій і користувачів, і мета їх використання не досягається за рік і більше. За даними Gartner, компанії часто купують друге або третє рішення, тому що чинне рішення не виправдало очікувань [14]. Відсутність необхідних ресурсів і навичок обслуговуючого персоналу (фахівців з досвідом з розслідування інцидентів, аудиту і тестів на проникнення) - найпоширеніші причини невдалих DLP-проектів.

Проблемним питанням для більшості організацій є також трудовитрати на роботу з DLP-системою.

Таким чином, незважаючи на достатню кількість проблем застосування DLP-систем ведеться постійна робота виробниками по їх модернізації, що дозволяє організаціям ефективно використовувати ці системи для оперативного виявлення витоків конфіденційної інформації та реагування на інциденти інформаційної безпеки.

На даний час спостерігається тенденція до створення комплексних систем захисту від витоків інформації. Сучасні DLP-система повинні охоплювати всі можливі канали: Web, електронну пошту, системи обміну миттєвими повідомленнями, а також знімні носії користувачів, мережеві і локальні принтери. Важливою властивістю сучасних DLP-систем є можливість контролювати зашифровані дані, які передаються по протоколу https, що дозволяє запобігати витоку через такі додатки, як Skype або електронна пошта Gmail. Все більш стає необхідність захищатися від витоків даних по каналам, пов'язаним з мобільними пристроями. Багато виробників вже працюють в даному напрямку.

Крім того, на даний час існує тенденція додавати до DLP-систем функції, пов'язані з поведінковим аналізом UEBA (User and Entity Behavior Analytics). Засновані на машинному навчанні і ретроспективному аналізі рішення UEBA дозволяють побачити, що робив співробітник, скажімо, півроку назад і як змінилася його активність зараз. Поряд із застосуванням методів математичної статистики за допомогою систем UEBA DLP-рішення можуть виявити такі інциденти, які класичні системи пропускають.

Для підвищення точності і зниження кількості помилкових спрацьовувань необхідно зібрати якомога більше даних і сформувати профіль користувача (його своєрідний психологічний і технологічний портрет), на основі якого проводиться оцінка ризиків. Така система пов'язує всі події з конкретними співробітниками і видає звіти, які визначають найбільш підозрілих користувачів і користувачів, з діями яких пов'язані найбільші ризики інформаційної безпеки. Це завдання вбудованого в DLP UEBA-модуля.

Інтеграція DLP з системами контролю і управління доступом дозволить побачити і інші незвичайні дії, якщо співробітник, наприклад, спробує зайти в приміщення, куди зазвичай не ходить. Аналогічними способами можна виявити і зовнішню атаку з використанням скомпрометованих облікових записів - в цьому випадку незвичайні дії виконує не сам співробітник, а підключився до корпоративних ресурсів з його правами віддалено зловмисник.

Ще одна проблема - процес звільнення співробітників. Нерідко вони передають конфіденційну інформацію конкурентам або просто видаляють критичні для бізнесу дані. У класичних системах ефективні механізми контролю таких працівників зустрічаються рідко, але для системи DLP з модулем UEBA це типовий сценарій.

На жаль, жоден інструмент не дозволить повністю вирішити всі проблеми - це абсолютно точно. Якщо співробітник замислив лихе, він може, наприклад, сфотографувати екран комп'ютера на телефон, взагалі не залишаючи слідів в системі. Безліч інцидентів пов'язано з паперовими носіями, електромагнітним випромінюванням і іншими погрозами, які неможливо контролювати в корпоративній мережі.

Тільки технічними засобами вирішити проблеми безпеки неможливо - це завжди застосування комплексу заходів, які в сукупності дозволяють знизити ризики - так що «срібної кулі» з UEBA не вийде. За умови грамотної настройки і профілювання рішення UEBA можуть доповнити існуючі системи і зробити їх роботу більш ефективною - це не черговий модний тренд, поведінковий аналіз дійсно дозволяє запобігти інциденти на початковій стадії їх виникнення, ще до реалізації загрози

Все частіше DLP-системи поєднують з системами управління інформаційною безпекою та подіями безпеки SIEM (Security Information and Event Management). Функціональна модель системи SIEM об'єднує підсистеми: збору даних, попередньої їх обробки, зберігання, аналізу, уявлення. SIEM забезпечує збір подій безпеки, їх агрегацію і фільтрацію, аналіз, моніторинг, розслідування та виведення результатів (звітів) в необхідному форматі [20-22].

У підсумку можна підкреслити, що універсальних DLP-систем не існує. Вибір на користь DLP-систем тієї чи іншої залежить виключно від потреб компанії і від підходу внутрішньої служби ІБ компанії до боротьби з даним видом витоку даних.

ВИСНОВКИ

При забезпеченні інформаційної безпеки організації одним з найважливіших видів діяльності є виявлення інцидентів інформаційної безпеки. Проведені в роботі дослідження показали, що неможливо уникнути всіх інцидентів інформаційної безпеки, так як завжди можуть відбуватися події, що тягнуть за собою потенційну загрозу.

Існує безліч способів боротьби з інцидентами, як на рівні організаційних процедур, так і на рівні програмних рішень. Одним з найбільш ефективних методів є впровадження систем захисту від витоку конфіденційних даних.

Система управління інцидентами інформаційної безпеки є базовою частиною загальної системи управління інформаційною безпекою і дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти інформаційної безпеки. Таким чином, для управління інцидентами інформаційної безпеки необхідно організувати комплекс процесів управління інцидентами, забезпечити його належними ресурсами, відповідною нормативно-розпорядчою і робочою документацією, технічними засобами забезпечення механізмів контролю.

За останні кілька років кількість витоків конфіденційної інформації та персональних даних виросло більш ніж в 5 разів. Використання DLP-систем для забезпечення захисту конфіденційних даних організації створює захищений цифровий «периметр» навколо організації, аналізуючи всю інформацію, що витікає, а в ряді випадків і входить в захищену зону.

Останнім часом вимоги до функціональних можливостей DLP-систем постійно зростають, що призводить до перетворення їх в один з найефективніших, комплексних і системних рішень в сфері захисту конфіденційної корпоративної інформації.

В роботі був проведений аналіз найпопулярніших DLP-систем, розглянуті їх функції та характеристики. Проведений аналіз підтвердив той факт, що виробники програмних продуктів DLP світового рівня (такі як McAfee,

Symantec, RSA та інші) представляють на ринок системи корпоративного класу зі зручним інтерфейсом, широкими можливостями контролю та аналітичними функціями. Менш відомі компанії SearchInform, Falcongaze представляють DLP системи з достатньо широкими можливостями.

В сучасних системах DLP застосовуються складні механізми аналізу: порівняння по шаблонах з використанням словників і регулярних виразів, лінгвістичний і контекстний аналіз, цифрові відбитки. Більшість компаній-лідерів на ринку використовують в своїх розробках технології як лінгвістичні, так і статистичні методи аналізу, при цьому одна з них є основною, а інша - додатковою. Для кращого виявлення конфіденційної інформації ці дві технології потрібно використовувати не паралельно, а послідовно.

Розробники DLP-систем, такі як Symantec, IBM продовжують роботу з перетворення деяких з своїх рішень на технологій машинного навчання.

Досить актуальною є також проблема вибору менеджерами і співробітниками служб безпеки DLP-систем, які б задовольняли їх вимогам та була в змозі захисти дані від крадіжок і витоків.

Проведений аналіз показав, що в якості основних критеріїв вибору системи можна обрати такі:

– наявність необхідних модулів для вирішення конкретного спектру завдань;

– кількість каналів, що контролюються;

– функціонал і об'єкти спостереження системи;

– уніфікованість управління системою;

– спроможність здійснювати активний захист;

– використання системою методів аналізу інформації за вмістом та контентом, категорювання інформації;

– надійність і швидкість роботи системи;

– аналітичні можливості;

– підтримки спеціальних технологій, сумісність в іншими продуктами і рішеннями, можливість і умови інтеграції в діючу інфраструктуру;

– наявність, якість та швидкість технічної підтримки;

– ціна, вартість розгортання та обслуговування системи.

Крім того, на даний час існує тенденція додавати до DLP-систем функції, пов'язані з поведінковим аналізом UEBA та системами управління інформаційною безпекою та подіями безпеки SIEM.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. В.В. Домарев, Д.В. Домарев. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k), Донецьк: Велстар, 2012. – 146 с.

2. Міжнародний стандарт ISO/IEC 27001 «Інформаційні технології – Методи безпеки – Системи управління інформаційною безпекою – Вимоги».

3. Управление инцидентами ИБ на основе SIEM-систем. [Електронний ресурс]. – Режим доступу: http://lib.itsec.ru/articles2/25kadr/upravlenie-intsidentami-ib-na-osnove-siem-sistem – Заголовок з екрана.

4. ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».

5. CMU/SEI-2004-TR-015 «Defining incident management processes for CISRT».

6. NIST SP 800-61 «Computer security incident handling guide».

7. ISO/IEC 27002:2013 «Information technology. Security techniques. Code of practice for information security controls».

8. Factum. Колегія детективів і фахівців безпеки бізнесу. Витік інформації [Електронний ресурс]. – Режим доступу: http://ukr.detective-ua.com/vitik-inform – Заголовок з екрана.

9. Сравнительный обзор средств предотвращения утечек данных (DLP) [Електронний ресурс]. – Режим доступу: https://safe-surf.ru/specialists/article/5233/609990/ – Заголовок з екрана.

10. Внедрение DLP-систем [Електронний ресурс]. – Режим доступу: https://techexpert.ua/our-services/implementation-of-dlp-systems/ – Заголовок з екрана.

11. Chapple M., Stewart J. M., Gibson D. (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide. – John Wiley & Sons, 2018.

12. Обзор и сравнение лучших бесплатных open source DLP систем 2019 года [Електронний ресурс]. – Режим доступу:

https://www.kickidler.com/ru/info/obzor-i-sravnenie-luchshix-besplatnyix-open-source-dlp-sistem-2019-goda.html – Заголовок з екрана.

13. Предотвращение утечек данных – DLP [Електронний ресурс]. – Режим доступу: http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/dlp-systems – Заголовок з екрана.

14. Сайт компанії Gartner [Електронний ресурс]. – Режим доступу: https://www.gartner.com/.

15. Сравнение DLP-систем [Електронний ресурс]. – Режим доступу: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/kak-vybrat-dlp-sistemu/sravnenie-dlp-sistem/ – Заголовок з екрана.

16. DLP-системы: защита от утечки информации [Електронний ресурс]. – Режим доступу: http://pro-spo.ru/personal-data-security/3738-dlp-sistemy-zashhita-ot-utechki-informaczii – Заголовок з екрана.

17. Романюков М.Г. Категоріювання інформації у сучасній структурі кібербезпеки держави з використанням матриць цінностей / М.Г. Романюков. – Харків: Критичні комп'ютерні технології та системи: науково-технічний семінар. 23 травня 2019 року. Тема семінару – Безсерверні архітектури, хмарні технології та кібербезпека.

18. Отт А. Современные тенденции в области контентной фильтрации / А. Отт // Информационный бюллетень "JET INFO". – 2012. – С.3–23.

19. Как выбрать идеальную DLP [Електронний ресурс]. – Режим доступу: https://searchinform.ru/blog/2018/03/05/kak-vybrat-idealnuyu-dlp/ – Заголовок з екрана.

20. Johansen G. Digital forensics and incident response: an intelligent way to respond to attacks. – 2017.

21. Сєвєрінов О.В. Управління інцидентами інформаційної безпеки на основі використання SIEM систем / О.В. Севєрінов, В.В. Ушатов // Інформатика, управління та штучний інтелект. Тези шостої міжнародної науково-технічної конференції – Х.: НТУ «ХПІ», 2019. – С. 109.

22. Ушатов В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки / В. Ушатов, О. Сєвєрінов // GLOBAL CYBER

SECURITY FORUM. Матеріали першого міжнародного науково-практичного форуму – Х.: ХНУРЕ, 2019. – С. 104-105.