ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«Технології захисту конфіденційних даних організації на базі SecureTower»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та
кібернетична безпека»
(шифр і назва спеціальності)
Бутковський С.В.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2021 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Бутковський Семен Валерійович
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: Технологія захисту конфіденційних даних організації на базі "SecureTower"

керівник магістерської роботи Гайдур Галина Іванівна,
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «___» _____ 2021 року №____.

2. Строк подання студентом магістерської роботи 15.12.2021 р.

3. Вихідні дані до магістерської роботи
корпоративна інформаційна система;
програмні комплекси захисту конфіденційних даних;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту конфіденційної інформації в корпоративних інформаційних систем.
2. Склад та умови функціонування систем запобігання витоку інформації.
3. Методи та засоби управління захистом конфіденційної інформації.
4. Рекомендації щодо вибору систем захисту від витоку конфіденційної інформації в корпоративній інформаційній системі.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу складу та умов функціонування корпоративної інформаційної системи.

4. Результати аналізу методів та засобів захисту конфіденційної інформації.

5. Аналіз сучасних DLP-систем

6. Призначення та можливості рішення DLP-системи Falcongaze SecureTower.

7. Аналіз методів ідентифікації і аналізу конфіденційних даних в DLP-системах.

8. Рекомендації щодо застосування системи захисту від витоку конфіденційної інформації в корпоративній інформаційній системі. Falcongaze SecureTower.

9. Висновки за результатами роботи.

6. Дата видачі завдання 27.09.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту конфіденційної інформації в корпоративних інформаційних систем.	27.09.2021 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	1.10.2021 р.	
3.	Аналіз методів та засобів захисту конфіденційної інформації.	20.10.2021 р.	
4.	Аналіз методів ідентифікації і аналізу конфіденційних даних в DLP-системах.	5.11.2021 р.	
5.	Розроблення рекомендацій щодо застосування систем захисту конфіденційної інформації.	20.11.2021 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	8.12.2021 р.	
7.	Підготовка доповіді до захисту.	15.12.2021 р.	

Студент Бутковський С.В.
(підпис) прізвище та ініціали

Керівник магістерської роботи Гайдур Г.І.
(підпис) прізвище та ініціали

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Бутковський С.В. до захисту магістерської роботи
(прізвище та ініціали)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технології захисту конфіденційних даних організації на базі SecureTower».

Магістерська робота і рецензія додаються.
Директор інституту _____ _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Бутковський С.В. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту _____ Журенко О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерськоїї роботи

Студент ***Бутковський С.В.*** обрав тему роботи, метою якої було дослідити зміст технології управління захистом конфіденційної інформації в корпоративних інформаційних системах на базі Falcongaze SecureTower та розробити рекомендації щодо застосування системи управління захистом від витоку інформації на підприємстві. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Бутковський С.В. показав відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану магістерську роботу студента Бутковського Семена Валерійовича на оцінку **«відмінно»** та присвоїти йому кваліфікацію 2149.2 магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи _____ Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута.
Студент Бутковський С.В.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

ВІДГУК РЕЦЕНЗЕНТА

на магістерську роботу

студента Бутковського Семена Валерійовича

на тему: «Технології захисту конфіденційних даних організації на базі SecureTower»

Актуальність:

Забезпечення захисту конфіденційної інформації стає все більш складним у зв'язку зі зростаючим числом можливостей для їх крадіжки. Одним із способів захисти цінну інформацію є DLP-системи, одна з них це SecureTower. Реалізація цієї технології в організації створить захисний кордон між вашою інформацією та зовнішнім світом, що створить умови забезпечення захисту від витоку. Тому тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми забезпечення захисту конфіденційної інформації в корпоративній інформаційній системі від новітніх загроз, визначено мета та завдання управління захистом конфіденційної інформації в корпоративній інформаційній системі.
2. Досліджено методи та засоби управління захистом конфіденційної інформації в організації на базі рішення SecureTower.
3. Запропоновано інструкцію з підбору DLP-систем, та технологію застосування системи захисту конфіденційної інформації від витоку.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У магістерській роботі бажано було б провести більш детальну роботу з рішенням SecureTower .
2. Оформлення дипломної роботи не відповідає усім вимогам.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку «**відмінно»**, а студент **Бутковський Семен Валерійович** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

РЕФЕРАТ

Текстова частина магістерської роботи: 82 сторінки, 22 рисунків, 4 таблиці, 30 джерел.

Об'єкт дослідження – процес забезпечення захисту конфіденційної інформації в організації.

Предмет дослідження – технологія захисту конфіденційної інформації.

Мета роботи – проаналізувати технологію захисту конфіденційної інформації SecureTower.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, порівняння декількох систем DLP.

В роботі проведено аналіз проблеми забезпечення кібербезпеки корпоративної інформації, та визначена мета та завдання для системи управління захистом від витоку інформації. Проаналізовано існуючі системи управління захистом від витоку інформації.

Досліджено методи та засоби системи захисту конфіденційної інформації на прикладі рішення SecureTower. Визначено призначення, основні функції та склад DLP системи SecureTower. На основі досліджень проведених в роботі складено рекомендації щодо застосування технології SecureTower для захисту конфіденційної інформації на підприємстві.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ЗАХИСТОМ DLP СИСТЕМ, ТЕХНОЛОГІЯ УПРАВЛІННЯ ЗАХИСТОМ ВІД ВИТОКУ ІНФОРМАЦІЇ

ABSTRACT

Text part of the master's thesis: 72 pages, 22 figures, 4 tables, 35 sources.

The object of research - is the process of ensuring the protection of confidential information.

The subject of research - the technology of protection of confidential information.

The purpose of the work - is to analyze the technology of protection of confidential information SecureTower.

Research methods - processing the literature on this topic, analysis of operating documentation, international standards and their comparison, comparison of several DLP systems.

The analysis of the problem of cybersecurity of corporate information is carried out in the work, and the purpose and tasks for the information leakage management system are determined. Existing information leakage management systems are analyzed.

The methods and means of the system of protection of confidential information on the example of the SecureTower solution are investigated. The purpose, main functions and composition of DLP SecureTower system are defined. Based on the research conducted in this work, recommendations for the use of SecureTower technology to protect confidential information in the enterprise.

Field of use - cybersecurity of corporate information system.

CORPORATE INFORMATION SYSTEM, CYBER SECURITY, METHODS AND MEANS OF DLP SYSTEM PROTECTION MANAGEMENT, TECHNOLOGY OF MANAGEMENT OF PROTECTION AG

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ…….. 8

ВСТУП ……..……. 9

1 ОСНОВНІ ПОНЯТТЯ ЗАХИСТУ ІНФОРМАЦІЇ І ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ……... 11

1.1. Поняття та призначення конфіденційної інформації в організації 11
1.2. Аналіз проблеми забезпечення захисту конфіденційної інформації в організації ……. 15
1.3. Цілі та завдання систем управління захистом конфіденційної інформації в організації ……..… 21
1.4. Аналіз існуючих технологій захисту конфіденційної інформації в організації ……..……. 31

2 АНАЛІЗ СУЧАСНИХ СИСТЕМ ЗАХИСТУ ВІД ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ…… 35

2.1. Система захисту від витоку конфіденційної інформації…….. 35
2.2. Аналіз сучасних DLP-систем ……..... 46
2.2.1 DLP-система SearchInform ……..……. 46
2.2.2 DLP-система Falcongaze SecureTower……..……..... 48
2.2.3 Система запобігання витоку даних Infowatch ……..…... 49
2.2.4 DLP-система Zecurion ……...…… 51
2.2.5 DLP-система Symantec……... 53
2.3. Порівняльний аналіз сучасних DLP-систем…..…… 54

3 АНАЛІЗ МЕТОІВ ІДЕНТИФІКАЦІЇ І АНАЛІЗУ КОНФІДЕНЦІЙНИХ ДАНИХ В DLP-СИСТЕМАХ..... 58

3.1. Принципи лінгвістичного аналізу інформації ……..…... 59
3.2. Статистичні методи аналізу інформації ……..…… 61
3.3. Технології аналізу конфіденційних даних в DLP системах …….. 63
3.4. Розробка рекомендацій щодо вибору системи захисту від витоку конфіденційної інформації……..... 67
3.4.1 Рекомендацій щодо вибору DLP-систем…….. 67
3.4.2 Проблемні питання при застосуванні DLP-систем…….. 74

ВИСНОВКИ……. 80
ПЕРЕЛІК ПОСИЛАНЬ..... 82
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)..... 84

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ – інформаційна безпека

ІТ – інформаційна технологія

ПІБ – подія інформаційної безпеки

ПЗ – програмне забезпечення

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

FTP – file transfer protocol, протокол передачі файлів
OCR – optical character recognition, аналіз графічних файлів

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

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 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 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 організаціях 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 Loss 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 DLP-система SecureTower.

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 ОСНОВНІ ПОНЯТТЯ ЗАХИСТУ ІНФОРМАЦІЇ І ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Поняття та призначення конфіденційної інформації.

В організації завжди є документи, витік змісту яких небажаний або просто небезпечний, тому що може бути використаний прямо або безпосередньо на шкоду їх авторам. Така інформація і відповідно документи, що її містять, вважаються конфіденційними. Обов'язковою ознакою конфіденційного документа є наявність у ньому інформації, що підлягає захисту. Особливістю конфіденційного документа і те, що він є одночасно як саму інформацію - обов'язковий об'єкт захисту, а й масовий носій інформації, основне джерело накопичення і поширення цієї інформації, зокрема і витоку. Конфіденційний документ містить відомості, що не належать до державної таємниці, а становлять інтелектуальну власність юридичної або фізичної особи. Тобто конфіденційна насамперед інформація, а потім уже стають конфіденційними і документи, в яких ця інформація зафіксована.

Конфіденційна інформація компанії складається з:

1. відомостей, що становлять комерційну таємницю;
2. відомостей, що становлять персональні дані працівників та інших осіб, які передали свої персональні дані Компанії у зв'язку з бізнес-діяльністю компанії;
3. конфіденційних відомостей інших юридичних та фізичних осіб, переданих компанії відповідно до законодавства та/або на договірній основі;
4. іншої інформації компанії, щодо якої запроваджено режим її обмеженого поширення та захисту.

Сучасні методи обробки, передачі та зберігання інформації сприяють появі загроз, пов'язаних з можливістю втрати, спотворення та розкриття конфіденційної інформації. Тому забезпечення захисту інформації комп'ютерних систем та мереж є одним із провідних напрямів розвитку інформаційних технологій.

В умовах ринку та конкуренції виникають проблеми, пов'язані із забезпеченням безпеки не тільки фізичних та юридичних осіб, їх майнової власності, а й інформації, що має комерційну цінність, інших відомостей, зокрема, результати інтелектуальної діяльності: секрети виробництва, службові тощо.

Корисність інформації полягає в тому, що вона створює суб'єкту вигідні умови для ухвалення оперативного рішення та отримання ефективного результату.

У свою чергу корисність інформації (особливо комерційної) залежить від своєчасного її доведення до суб'єкта підприємництва. Наприклад, через несвоєчасне надходження корисних за змістом відомостей упускається можливість укласти вигідну торгову чи іншу угоду. Результат – час втрачено, інформація втрачає свою корисність.

За даними експертів з безпеки, на сьогоднішній день найбільш поширеним і небезпечним видом внутрішньої загрози стає витік інформації. Нерідко джерелом такої загрози є недобросовісні працівники установи, які згідно з своїми службовими обов'язками мають доступ до конфіденційної інформації та використовують її на користь третіх осіб. Як свідчить судова практика, втрати підприємства у такому разі нерідко бувають більш значними, ніж від шахрайства чи крадіжки.

Нижче наведено основні визначення захисту інформації та інформаційної безпеки комп'ютерних систем та мереж.

Сам термін «конфіденційний» походить від англійської confidence – довіра, необхідність запобігання втраті будь-якої інформації. Іншими словами, конфіденційна інформація має бути відома чи довірена вузькому колу осіб. Загальний для всіх видів конфіденційної інформації той факт, що вільний доступ до неї обмежений відповідно до приписів чинного законодавства чи внутрішніх нормативних документів установи чи органу, які здійснюють її управління.

Захист інформації - організаційні заходи, спрямовані на запобігання витоку конфіденційної інформації та небажаних впливів на інформацію, що захищається.

Захист інформації від витоку - організаційні та технічні заходи, спрямовані на запобігання неконтрольованому поширення/копіювання конфіденційної інформації внаслідок її розголошення та НСД до неї.

Захист інформації від розголошення - організаційні та технічні заходи, спрямовані на запобігання несанкціонованого доступу до конфіденційної інформації та розголошення її суб'єктам, які мають права доступу до цієї інформації.

Захист інформації від НСД - організаційні та технічні заходи, спрямовані на запобігання одержанню захищається інформації заінтересованими суб'єктами з порушенням встановлених нормативними та правовими документами (актами) або власниками інформації прав чи правил розмежування доступу до захищається інформації.

Система захисту інформації — раціональна сукупність напрямків, методів, засобів та заходів, що знижують уразливість інформації та перешкоджають несанкціонованому доступу до інформації, її розголошенню чи витоку. Головними вимогами до організації ефективного функціонування системи є: персональна відповідальність керівників та співробітників за збереження носія та конфіденційність інформації, регламентація складу конфіденційних відомостей та документів, що підлягають захисту, регламентація порядку доступу персоналу до конфіденційних відомостей та документів, наявність спеціалізованої служби безпеки, що забезпечує практичний захист та нормативно-методичного забезпечення діяльності цієї служби.

Цінність інформації – це комплекс показників її якості, міра придатності для прийняття рішень у конкретній сфері. Звідси комерційна цінність інформації – це її придатність (корисність) для прийняття рішень у комерційній діяльності. Цінність інформації складається з достовірності, актуальності, повноти, корисності та своєчасності інформації.[2]

Сучасна автоматизована система обробки конфіденційної інформації є складною системою, що складається з великої кількості компонентів різного ступеня автономності, які пов'язані між собою та обмінюються даними. Практично кожен компонент може піддатися зовнішньому
впливу або вийти з ладу. Компоненти АС можна розбити на наступні групи[2]:

- Апаратні засоби - комп'ютери та їх складові (процесори, монітори, термінали, периферійні пристрої дисководи, принтери, контролери, кабелі, лінії зв'язку тощо).

- Програмне забезпечення — різні програми, утиліти тощо.
- Дані - різна інформація, що зберігається на дисках, дискетах, у журналах тощо.
- Персонал - користувачі системи та обслуговуючі співробітники.

Хто володіє інформацією – той володіє світом. Цей крилатий вираз у наш час набув особливої актуальності. Сьогодні важливо не лише швидко знайти потрібну інформацію, а й уміти захистити власну. Немає інформації, якою ніхто не цікавиться. Особливо, коли завдяки цій інформації хтось заробляє гроші. Далі ми поговоримо про те, яку інформацію можна відносити до "закритої" та як її краще захищати.

Конфіденційна інформація - це відомості, які перебувають у володінні, користуванні чи розпорядженні окремих фізичних чи юридичних осіб та розповсюджуються за їх бажанням.

Фізичні та юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру або є предметом їхнього професійного, ділового, виробничого, банківського, комерційного та іншого інтересу та не порушує передбаченої законом таємниці, самостійно встановлюють режим доступу до неї, включаючи належність її до категорії конфіденційної, та впроваджують систему (способи) її захисту. Виняток становить інформація, приховування якої загрожує життю та здоров'ю людей.

Відповідно до Закону «Про доступ до публічної інформації» конфіденційною є інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Схоже визначення нам дає Закон «Про інформацію» у статті 21, а саме: «конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом».

1.2 Аналіз проблеми забезпечення захисту конфіденційної інформації в організації

В даний час досить актуальною є проблема забезпечення інформаційної безпеки корпоративних систем, для яких одним із основних завдань при створенні систем захисту є блокування каналів витоку інформації.

Не слід вважати, що ваша інформація (інформація, якою ви володієте, або ваше підприємство) нікому не потрібна. Особливо складним є захист від витоків конфіденційної інформації в великих організаціях, як правило, вони мають значну кількість різноманітних інформаційних ресурсів, у тому числі ресурсів з обмеженим доступом.

Практичною реалізацією політики (концепції) інформаційної безпеки фірми є технологічна система захисту. Захист інформації є жорстко регламентований і динамічний технологічний процес, що попереджає порушення доступності, цілісності, достовірності і конфіденційності цінних інформаційних ресурсів і, зрештою, забезпечує досить надійну безпеку інформації у процесі управлінської та виробничої діяльності фірми.

Інформаційна інфраструктура підприємства постійно наражається на численні загрози, які за своїм походженням діляться на кілька видів:

- Природні. Загрози, причини які не залежать від людини. До них належать урагани, пожежі, удари блискавки, повені, інші природні катаклізми.
- Штучні. Комплекс загроз інформаційної безпеки створених людиною. Штучні загрози, у свою чергу, поділяють на навмисні та ненавмисні.
- Навмисні загрози виникають внаслідок дії конкурентів, хакерських атак, шкідництво скривджених працівників.

  Наприклад:

  1. Фізичне руйнування системи (шляхом вибуху, підпалу тощо) або виведення з ладу всіх або окремих найважливіших компонентів

комп'ютерної системи (пристроїв, носіїв важливої системної інформації, осіб із числа персоналу тощо).

2. Вимкнення або виведення з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження та вентиляції, ліній зв'язку та ін.).
3. Дії щодо дезорганізації функціонування системи (зміна режимів роботи пристроїв або програм, страйк, саботаж персоналу, постановка потужних активних радіоперешкод на частотах роботи пристроїв системи тощо).
4. Впровадження агентів до персоналу системи (зокрема, можливо, й у адміністративну групу, яка відповідає за безпеку).
5. Вербування (шляхом підкупу, шантажу тощо) персоналу або окремих користувачів, які мають певні повноваження.
6. Застосування підслуховуючих пристроїв, дистанційна фотографія та відео зйомка тощо.
7. Перехоплення побічних електромагнітних, акустичних та інших випромінюючих пристроїв та ліній зв'язку, а також наведення активних випромінювань на допоміжні технічні засоби, що безпосередньо не беруть участі в обробці інформації (телефонні лінії, мережі живлення, опалення тощо).
8. Перехоплення даних, що передаються каналами зв'язку, та їх аналіз з метою з'ясування протоколів обміну, правил входження у зв'язок та авторизації користувача та подальших спроб їх імітації для проникнення в систему.
9. Розкрадання носіїв інформації (магнітних дисків, стрічок, мікросхем пам'яті, пристроїв, що запам'ятовують, і цілих ПЕОМ).
10. Несанкціоноване копіювання носіїв інформації.
11. Розкрадання виробничих відходів (роздруківок, записів, списаних носіїв інформації тощо).
12. Читання залишкової інформації з оперативної пам'яті та з зовнішніх пристроїв.

13. Читання інформації з областей оперативної пам'яті, що використовуються операційною системою (у тому числі підсистемою захисту) або іншими користувачами, використовуючи в асинхронному режимі недоліки мультизадачних операційних систем та систем програмування.
14. Незаконне отримання паролів та інших реквізитів розмежування доступу (агентурним шляхом, використовуючи недбалість користувачів, шляхом підбору, шляхом імітації інтерфейсу системи тощо) з подальшим маскуванням під зареєстрованого користувача.
15. Несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізична адреса, адреса в системі зв'язку, апаратний блок кодування тощо.
16. Розкриття шифрів криптозахисту інформації.
17. Використання апаратних спеціалістів, програмних закладок і вірусів, тобто. таких ділянок програм, які не потрібні для здійснення заявлених функцій, але що дозволяють долати систему захисту, потай і незаконно здійснювати доступ до системних ресурсів з метою реєстрації та передачі критичної інформації або дезорганізації функціонування системи.
18. Незаконне підключення до ліній зв'язку з метою роботи «між рядків», з використанням пауз у діях законного користувача від його імені з подальшим введенням хибних повідомлень або модифікацією повідомлень, що передаються.
19. Незаконне підключення до ліній зв'язку з метою прямої заміни законного користувача шляхом його фізичного відключення після входу в систему та успішної автентифікації з подальшим введенням дезінформації та нав'язуванням хибних повідомлень.

- Ненавмисні загрози виникають внаслідок дій, вчинених через незнання, неуважність чи недбалість, з цікавості, але без злого наміру.

  Наприклад:

1. Ненавмисні дії, що призводять до часткової або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів системи (ненавмисне псування обладнання, видалення, спотворення файлів з важливою інформацією або програм, у тому числі системних тощо).
2. Неправомірне вимкнення обладнання або зміна режимів роботи пристроїв та програм.
3. Ненавмисне псування носіїв інформації.
4. Запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання чи зациклювання) або які здійснюють незворотні зміни у системі (форматування чи реструктуризацію носіїв інформації, видалення даних тощо).
5. Нелегальне використання та використання неврахованих програм (ігрових, навчальних, технологічних та інших., які є необхідні виконання порушником своїх службових обов'язків) з наступним необгрунтованим витрачанням ресурсів (завантаження процесора, захоплення оперативної пам'яті та пам'яті на зовнішніх носіях).
6. Зараження комп'ютера вірусами.
7. Необережні дії, що призводять до розголошення конфіденційної інформації або роблять її загальнодоступною.
8. Розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, перепусток).
9. Проектування архітектури системи, технології обробки даних, розробка прикладних програм з можливостями, що становлять небезпеку для працездатності системи та безпеки інформації.
10. Ігнорування організаційних обмежень (встановлених правил) під час роботи у системі.
11. Вхід до системи в обхід засобів захисту (завантаження сторонньої операційної системи зі змінних магнітних носіїв тощо).
12. Некомпетентне використання, налаштування або неправомірне відключення засобів захисту персоналом служби безпеки.

13. Пересилання даних на помилкову адресу абонента (пристрою).
14. Введення хибних даних.
15. Ненавмисне пошкодження каналів зв'язку.

- Внутрішні. Загрози, що виникають усередині інформаційної інфраструктури підприємства.
- Зовнішні. Загрози, які мають походження поза інформаційної інфраструктури підприємства.

Найчастіше задля досягнення поставленої мети зловмисник використовує не один, а деяку сукупність із вище перерахованих шляхів.

Порушник - це особа, яка зробила спробу виконання заборонених операцій (дій) помилково, з незнання або усвідомлено зі злим наміром (з корисливих інтересів) або без такого (заради гри чи задоволення, з метою самоствердження тощо) і використовує для цього різні можливості, методи та засоби.

При поділі порушників безпеки за класами можна виходити з їхньої належності певним категоріям осіб, мотивів дій і переслідуваних цілей, характеру методів досягнення поставлених цілей, кваліфікації, технічної оснащеності та знань про інформаційну систему, що атакується.

Насамперед порушників можна розділити на внутрішніх та зовнішніх. Потенційно до внутрішніх порушників належать працівники або співробітники організацій зі сфери IT, які надають аутсорсингові телекомунікаційні та інші інформаційні послуги.

Серед внутрішніх порушників насамперед можна виділити такі категорії:

1. Безпосередні користувачі та оператори інформаційної системи, у тому числі керівники різних рівнів.
2. Адміністратори ЛОМ та інформаційної безпеки.
3. Програмісти.
4. Технічний персонал з обслуговування будівель та обчислювальної техніки, від прибиральниці до ремонтної бригади.
5. Допоміжний персонал та тимчасові працівники.
6. Спеціально запроваджені агенти.

Залежно від характеру впливу загрози інформаційній безпеці поділяються на пасивні та активні. Пасивні загрози - чинники впливу, які не можуть змінювати зміст та структуру інформації. Активні загрози - можуть вносити такі зміни. До них відносять, наприклад, вплив шкідливого ПЗ. Головну небезпеку становлять штучні навмисні небезпеки. З огляду на дедалі більшу комп'ютеризацію всіх сфер бізнесу та зростання кількості електронних транзакцій ці загрози також бурхливо розвиваються. У пошуках способів отримання секретних відомостей та заподіяння шкоди компаніям зловмисники активно використовують сучасні технології та програмні рішення. Їхні дії можуть завдавати значних збитків, у тому числі у вигляді прямих фінансових втрат або втрати інтелектуальної власності. Тому інформаційна безпека підприємства також має будуватись на базі передових технологій з використанням актуальних засобів захисту даних.

Відповідно до прийнятого в ITIL (бібліотека інфраструктури інформаційних технологій) визначенню «інцидент» означає «будь-яка подія, яка не є елементом нормального функціонування послуги і в той же час здатна вплинути на роботу служби шляхом її переривання чи зниження
якості» [3].

Під подією інформаційної безпеки (ПІБ) розуміється стан системи, сервісу або мережі, що свідчить про можливе порушення політики безпеки, або про невідому ситуацію, яка може мати відношення до безпеки, в той час як інцидент інформаційної безпеки (ІІБ) – це одна чи серія подій інформаційної безпеки, які можуть призвести до збитків та втрат для організації. Втрати можуть бути як матеріальними (вартість, експлуатаційні витрати тощо) та нематеріальними (репутація організації, зміна морально-психологічного клімату тощо) [3].

Інцидент інформаційної безпеки – це єдина подія чи низка небажаних
та непередбачених подій, за якими існує ймовірність компрометація бізнес-інформації та загрози інформаційної безпеки[2].

Як приклад інцидентів можна навести такі події, як неавторизована зміна даних на сайті організації незаблокованим без нагляду.

Жоден досконалий спосіб зниження ризиків інформаційної безпеки, чи це досконало опрацьована політика безпеки чи найсучасніший брандмауер не може

захистити від виникнення в інформаційному середовищі подій, що потенційно становлять небезпеку діяльності організації. Статистика загроз безпеці інформації організації представлена на рис. 1.1.

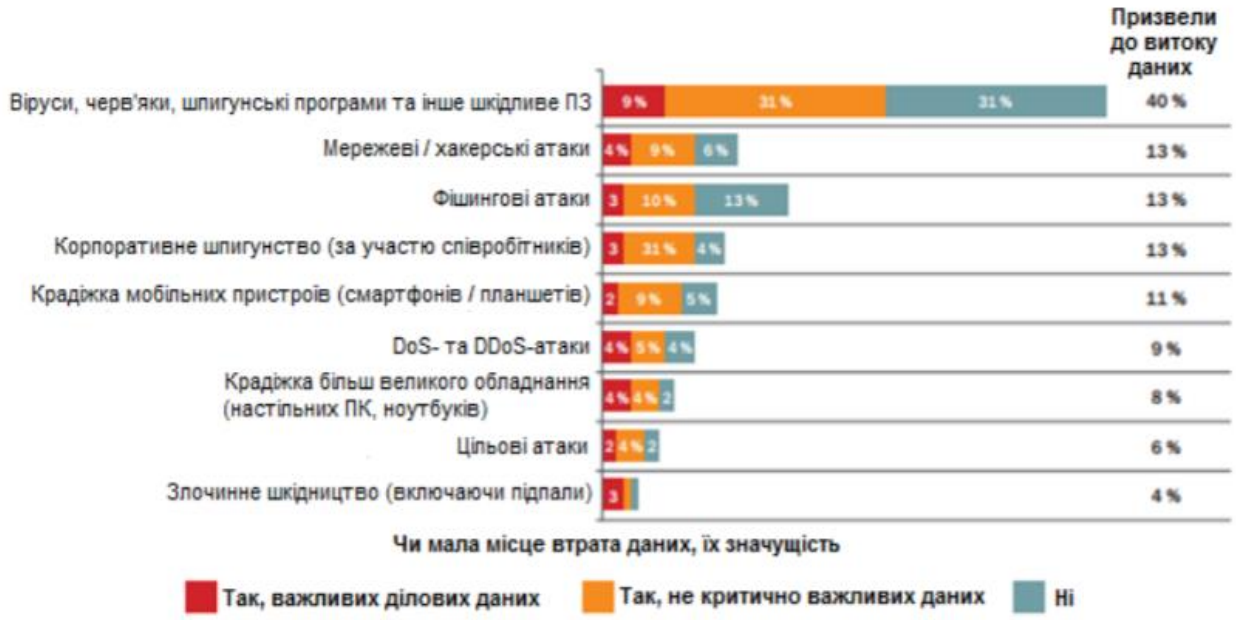


Рисунок 1.1 – Статистика загроз безпеці інформації

Різноманітність та складність середовища діяльності підприємства у сучасному світі, зумовлюють наявність залишкових ризиків незалежно від впровадження заходів протидії та якості підготовки. Також завжди існує ймовірність реалізації, невідомих дотепер, загроз інформаційної безпеки. Неготовність організації до обробки подібних ситуацій може суттєво ускладнити відновлення бізнес-процесів та потенційно збільшити завдані збитки.

1.3 Цілі та завдання систем управління захистом конфіденційної інформації в організації

Формулювання цілей і завдань захисту, як будь-якій іншій діяльності, представляє початковий і значимий етап забезпечення безпеки інформації. Важливість цього етапу часто недооцінюється та обмежується цілями та завданнями, що нагадують гасла. У той же час фахівці в галузі системного аналізу

вважають, що від чіткості та конкретності цілей та постановок завдань багато в чому залежить успіх у їхньому досягненні та вирішенні. Провал багатьох, у принципі корисних, починань обумовлений саме невизначеністю і розпливчастістю цілей і завдань, у тому числі незрозуміло, хто, що з допомогою якого ресурсу передбачає вирішувати продекларовані завдання.

Організація системи захисту інформації починається з визначення переліку відомостей, що становлять комерційну таємницю та які є конфіденційною інформацією, керівник підприємства повинен затвердити наказом положення про комерційну таємницю та про конфіденційну інформацію на підприємстві, в яких вказати, що нерозголошення комерційної таємниці та конфіденційної інформації входить до трудових обов'язки працівників та визначити відповідальність за невиконання цих обов'язків.

Кожен працівник повинен ознайомитися з цими переліками та підписати зобов'язання про нерозголошення комерційної таємниці та конфіденційної інформації. Крім цього, важливо стежити за дисципліною працівників щодо охорони інформації. Прийміть за правило не викидати документи (проекти договорів, факси, листи тощо) у сміття, не залишати їх на столі, доводити до працівників лише ту інформацію, яку їм необхідно знати для виконання своїх службових обов'язків.

Для запобігання порушень необхідно проводити спеціальну підготовку персоналу, підтримувати здоровий робочий клімат у колективі, проводити ретельний відбір найманих працівників, своєчасно виявляти зловмисників.

Групу зовнішніх порушників можуть становити:

1. Запрошені відвідувачі.
2. Представники конкуруючих організацій.
3. Співробітники органів відомчого нагляду та управління.
4. Порушники пропускного режиму.
5. Спостерігачі за межами території, що охороняється.
6. Кримінальні структури.
7. Недобросовісні партнери.

За рекомендацією експертів у галузі інформаційної безпеки, особливу увагу слід звертати на новоприйнятих працівників у таких професіях як: адміністратори,

програмісти, фахівці у галузі комп'ютерної техніки та захисту інформації. Надзвичайну небезпеку становлять фахівці такого рівня під час вступу в змову з керівництвом підрозділів та служби безпеки, а також з організованими злочинними групами. В даному випадку можливі збитки та тяжкість наслідків багаторазово збільшуються.

Керівництво компанії має чітко визначати, від яких видів порушень необхідно захиститися насамперед.

Також можна провести класифікацію порушників за використовуваними методами та засобами:

1. Збір інформації та даних.
2. Пасивні засоби перехоплення.
3. Використання коштів, що входять до інформаційної системи або системи її захисту, та їх недоліки.
4. Активне відстеження модифікацій існуючих засобів обробки інформації, підключення нових засобів, використання спеціалізованих утиліт, впровадження програмних закладок та «чорних ходів» у систему, підключення до каналів передачі даних.

За рівнем знань порушника про організацію інформаційної структури можна виділити такі категорії:

1. Типові знання методи побудови обчислювальних систем, мережевих протоколів, використання стандартного набору програм.
2. Високий рівень знань мережевих технологій, досвід роботи зі спеціалізованими програмними продуктами та утилітами.
3. Високі знання у галузі програмування, системного проектування та експлуатації обчислювальних систем.
4. Володіння відомостями про засоби та механізми захисту системи, що атакується.
5. Порушник був розробником або брав участь у реалізації системи забезпечення інформаційної безпеки.

За часом інформаційного впливу порушник може діяти:

1. На момент обробки інформації.
2. У момент передачі.

3. У процесі зберігання даних (враховуючи робочий та неробочий стан системи).

За місцем здійснення дії:

1. Видалено з використанням перехоплення інформації, що передається каналами передачі даних, або без її використання.
2. Доступ на територію, що охороняється.
3. Безпосередній фізичний контакт із обчислювальною технікою, у своїй можна назвати:
   3.1. Доступ до термінальних операторських станцій.
   3.2. Доступ до важливих послуг підприємства (сервера).
   3.3. Доступ до систем адміністрування, контролю та управління інформаційною системою.
   3.4. Доступ до програм управління системою забезпечення інформаційної безпеки.

Схема класифікації порушників. У таблиці 1.1 представлено узагальнену модель порушника. Таблиця 1.2 містить опис повноважень порушників.

Таблиця 1.1

Узагальнена модель порушника:

Положення в системі	Кваліфікація	Рівень можливостей	Опис
Внутрішній	Низька – висока	1	Користувачі, оператори, з числа працівників та тимчасових працівників.
	Висока	2	Прикладні програмісти.
	Висока	3	Адміністратори БД та користувачі, які мають необмежені повноваження щодо доступу до даних
	Висока	4	Адміністратори обчислювальної мережі

	Низька	Не мають легального доступу до системи	Технічний, обслуговуючий персонал (прибиральниці, водії тощо)
Зовнішній	Низька – висока	Не мають легального доступу до системи	Порушники пропускного режиму тимчасові працівники (не фахівці з технічних засобів АС), відвідувачі, представники органів нагляду та управління.
	Низька – висока	Не мають легального доступу до системи	Порушники за межами території, що охороняється: хакери та ін.
Зовнішній	Висока	Отримують тимчасовий доступ за рівнями 1-4	Фахівці сторонніх організацій, що здійснюють постачання, монтаж та ремонт обладнання обчислювальної системи.

Таблиця1.2

Рівні можливостей порушників:

Рівень	Можливості порушника
1	Запуск завдань (програм) з фіксованого набору, що реалізують заздалегідь передбачені функції обробки інформації
2	Створення та запуск власних програм з новими функціями обробки інформації
3	Управління функціонуванням системи, тобто, вплив на базове програмне забезпечення системи та на склад та конфігурацію її обладнання
4	Весь обсяг можливостей осіб, які здійснюють проектування, реалізацію та ремонт технічних засобів, аж до включення до складу системи власних технічних засобів з новими функціями обробки інформації

До того ж, велику увагу потрібно приділити інформації, яку отримують сторонні особи. Існує поняття інсайдерської інформації, тобто інформації, якою володіють інсайдери - особи, які не працюють на підприємстві, але мають закриту інформацію про це підприємство. Так, інсайдерами є колишні топ-менеджери, акціонери, ділові партнери, співробітники юридичних, аудиторських, консалтингових фірм, які надають послуги вашому підприємству. Звичайно, для багатьох із них нерозголошення інсайдерської інформації є принципом ділової етики та репутації. Однак є випадки, коли інсайдери можуть навмисне розголосити вашу комерційну таємницю або конфіденційну інформацію. Наприклад, це може зробити партнер, з яким ви розірвали стосунки, або звільнений вам топ-менеджер. Будьте обережні у стосунках із такими особами. Бажано отримати від них письмове зобов'язання про нерозголошення тих відомостей, що вони отримали від вас.

Основними цілями захисту інформації є:

- уникнення витоку, розкрадання, спотворення, підробка;
- забезпечення безпеки особистості, суспільства, держави;
- уникнення несанкціонованого ознайомлення, знищення, спотворення, копіювання блокування інформації в інформаційних системах;
- захист прав громадян на збереження особистої таємниці та конфіденційності персональних даних;
- збереження державної таємниці, конфіденційності задокументованої інформації;
- дотримання правового режиму використання масивів, програм обробки інформації, забезпечення повноти, цілісності, достовірності інформації у системах обробки;
- охорона можливості управління процесом обробки та користування інформацією.

Одні технології захисту системи та забезпечення обліку всіх подій можуть бути вбудовані в сам комп'ютер, інші - в програми. Деякі технології виконуються людьми і є реалізацією вказівок посібника, які містяться у відповідних керівних документах. Ухвалення рішення про вибір рівня складності технологій для захисту системи потребує встановлення критичності інформації та подальшого визначення

адекватного рівня безпеки. До критичних даних слід віднести такі відомості, які вимагають захисту від можливого завдання шкоди та її величини в тому випадку, якщо відбудеться випадкове або навмисне розкриття, зміна або руйнування даних.

Основним завданням захисту інформації традиційно вважається забезпечення:

- доступність (можливість за прийнятний час отримати необхідну інформаційну послугу);
- конфіденційності (захищеність інформації від несанкціонованого ознайомлення);
- цілісності (актуальність та несуперечність інформації, її захищеність від руйнування та несанкціонованої зміни);

Проблеми інформаційної безпеки вирішуються, як правило, через створення спеціалізованих систем захисту інформації, які повинні забезпечувати безпеку інформаційної системи від несанкціонованого доступу до інформації та ресурсів, несанкціонованих та ненавмисних шкідливих впливів. Система захисту є інструментом адміністраторів інформаційної безпеки, виконують функції із забезпечення захисту інформаційної системи та контролю її захищеності.

Система захисту інформації повинна виконувати такі функції:

- реєстрація та облік користувачів, носіїв інформації, інформаційних масивів;
- забезпечення цілісності системного та прикладного програмного забезпечення та оброблюваної інформації;
- захист комерційної таємниці, у тому числі з використанням сертифікованих засобів криптозахисту;
- створення захищеного електронного документообігу з використанням сертифікованих засобів криптоперетворення та електронного цифрового підпису;
- централізоване керування системою захисту інформації, реалізоване на робочому місці адміністратора інформаційної безпеки;
- захищений віддалений доступ мобільних користувачів на основі використання технологій віртуальних приватних мереж (VPN);
- керування доступом;

- забезпечення ефективного антивірусного захисту.

Організація фізичного захисту повинна зменшити можливість несанкціонованих дій сторонніх осіб та персоналу підприємства, а також знизити вплив техногенних джерел.

Захист на технологічному рівні спрямований на зменшення можливих проявів загроз безпеці інформації, пов'язаних з використанням неякісного програмного продукту та технічних засобів обробки інформації та некоректних дій розробників програмного забезпечення. Система захисту на цьому рівні має бути автономною, але забезпечувати реалізацію єдиної політики безпеки та будуватися на основі використання сукупності захисних функцій вбудованих систем захисту операційної системи та систем управління базами даних та знань.

На локальному рівні організується поділ інформаційних ресурсів інформаційної системи на сегменти за рівнем конфіденційності, територіальним та функціональним принципом, а також виділення в відокремлений сегмент засобів роботи з конфіденційною інформацією. Підвищенню рівня захищеності сприяють обмеження та мінімізація кількості точок входу/виходу (точок взаємодії) між сегментами, створення надійної оболонки по периметру сегментів та інформаційної системи загалом, організація захищеного обміну інформацією між сегментами.

На мережному рівні має бути організований захищений інформаційний обмін між автоматизованими робочими місцями, у тому числі віддаленими та мобільними, створена надійна оболонка по периметру інформаційної системи загалом. Система захисту на цьому рівні має будуватися з урахуванням реалізації захисту попередніх рівнів. Основою організації захисту може бути застосування програмно-апаратних засобів підвищеної автентифікації та захисту від несанкціонованого доступу до інформації. Крім того, можливе використання між сегментами і по периметру інформаційної системи спеціальних однокомпонентних або розподілених засобів захисту, що виключають проникнення в межі периметра сторонніх користувачів, що захищається (міжмережеві екрани, технології аутентифікації) і забезпечують розмежування доступу до захищених баз даних, що розділяються, та інформаційних ресурсів. Додатково можуть використовуватися

засоби побудови віртуальних мереж (VPN-технологій) та криптографічного захисту інформації при передачі відкритими каналами.

На рівні користувача повинен бути забезпечений допуск лише авторизованих користувачів до роботи в інформаційній системі, створена захисна оболонка навколо її елементів, а також організовано індивідуальне середовище діяльності кожного користувача.[4]

Найбільш повно критерії для оцінки механізмів безпеки організаційного рівня представлені в міжнародному стандарті ISO 17799: Практичні правила управління інформаційною безпекою (Code of Practice for Information Security Management), прийнятому в 2000 р. Цей стандарт є міжнародною версією британського стандарту BS 7799. Він містить практичні правила з управління інформаційною безпекою і може використовуватися як критерії для оцінки механізмів безпеки організаційного рівня, включаючи адміністративні, процедурні та фізичні заходи захисту.

Модель системи захисту є сукупність об'єктивних зовнішніх і внутрішніх чинників і відбиває їх впливом геть стан інформаційної безпеки об'єкта і збереження інформаційних ресурсів. При цьому доцільно розглядати такі об'єктивні фактори:

- загрози інформаційної безпеки, що характеризуються певною ймовірністю виникнення та ймовірністю реалізації;
- вразливість об'єкта чи системи контрзаходів (комплексної системи захисту), що впливає ймовірність реалізації загрози;
- ризик, тобто можливість заподіяння шкоди організації внаслідок реалізації загрози інформаційній безпеці: витоку інформації та її неправомірного використання.

Для побудови збалансованої комплексної системи захисту інформації проводиться аналіз ризиків, потім визначається оптимальний рівень ризику для компанії на основі заданого критерію. Комплексна система захисту інформації (сукупність контрзаходів) будується таким чином, щоб досягти заданого рівня ризику.

Наразі у міжнародній практиці розроблено достатню кількість нормативних документів, що регламентують питання управління інцидентами інформаційної безпеки. Для найефективнішої реалізації системи управління інцидентами інформаційної безпеки необхідно спиратися на вимоги міжнародних та галузевих стандартів, таких як ISO\IEC 27001-2013 "Information security management systems. Requirements" та ITU-T X-1051 "Information security management systems. Rechuirements for telecommunication".

У рамках цих стандартів встановлюються загальні вимоги до побудови системи управління інформаційною безпекою, що відносяться до процесів управління інцидентами, даються практичні підходи з виявлення, реєстрації та оцінки випадків порушення інформаційної безпеки та уразливостей.

Специфічні питання управління інцидентами інформаційної безпеки розглядаються у наступних документах:

1. 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, наводитись докладні рекомендації щодо необхідних процедур [4].
2. CMU/SEI-2004-TR-015 Defining incident management processes for CISRT (Software Engineering Institute/Carnegie Mellon University) описує методологію планування, впровадження, оцінки та покращення процесів управління інцидентів. Основний акцент робиться на організації роботи CISRT (Critical Incident Stress Response Team) – групи чи підрозділів, які забезпечують сервіс і підтримку запобігання, обробки та реакції на інциденти інформаційної безпеки. Вводити ряд критеріїв, на підставі яких можна оцінювати ефективність даних сервісів, наводяться докладні процесні карти [5].
3. NIST SP 800-61 Computer security incident handling guide – збірка "кращих практик" щодо побудови процесів управління інцидентами та реакції на них. Детально розбираються питання реакції на різні типи загроз, такі як розповсюдження шкідливого програмного забезпечення, несанкціонованого доступ тощо. [6].

1.4 Аналіз існуючих технологій захисту конфіденційної інформації

Сучасні технології захисту інформації представлені великою кількістю різноманітних програмних та апаратних засобів. Завдання, які вирішуються будь-яким системним засобом, у тому числі і засобом захисту інформації, повністю визначаються областю його практичного використання. Особливістю побудови системи захисту є те, що користувач повинен розглядатися як основний потенційний зловмисник (інсайдер). Це обумовлюється тим, що користувач у цьому випадку обробляє власну інформацію і, отже, може бути зацікавлений у її розкраданні. У зв'язку з цим основу забезпечення інформаційної безпеки в даному випадку становлять механізми захисту, що реалізують розмежувальну політику доступу до інформаційних ресурсів.

Далі розглянемо технології захисту від несанкціонованого доступу, криптографічного захисту, антивірусного захисту та міжмережевих екранів, які найчастіше застосовуються для організації захисту.

Під несанкціонованим доступом (НСД) до інформації розуміється такий доступ, який порушує правила використання інформаційних ресурсів комп'ютерної системи, встановлених для його користувачів. Несанкціонований доступ є реалізацією навмисної загрози безпеці конфіденційної інформації і часто називається атакою або нападом на комп'ютерну систему.

Захист від НСД здійснюється за допомогою програмних чи технічних засобів управління доступом. Управління доступом включає такі функції захисту:

1. Ідентифікація користувачів, персоналу та ресурсів системи (присвоєння кожному об'єкту персонального ідентифікатора).

2. Впізнання (встановлення справжності) об'єкта чи суб'єкта за пред'явленим ним ідентифікатором.
3. Перевірка повноважень (перевірка відповідності дня тижня, часу доби, ресурсів та процедур, що запитуються, встановленому регламенту).
4. Дозвіл та створення умов роботи в межах встановленого регламенту.
5. Протоколювання звернень до ресурсів, що захищаються.
6. Реєстрація (сигналізація, відключення, затримка робіт, відмова у запиті) при спробах несанкціонованих дій.

Програмні засоби захисту від НСД є програмним забезпеченням, спеціально призначеним для виконання функцій управління доступом до інформації, що захищається. Програмні засоби реалізують механізми контролю доступу, цифрового підпису, захисту під час введення та виведення інформації тощо.

Технічні засоби реалізуються у вигляді електричних, електромеханічних та електронних пристроїв. Вся сукупність технічних засобів поділяється на апаратні та фізичні. Під апаратними засобами прийнято розуміти техніку або пристрої, що сполучаються з подібною апаратурою за стандартним інтерфейсом, наприклад, система розпізнавання та розмежування доступу до інформації (за допомогою паролів, запису кодів та іншої інформації на різні картки). Фізичні засоби реалізуються у вигляді автономних пристроїв та систем: замки на дверях, де розміщена апаратура, ґрати на вікнах, джерела безперебійного живлення, електромеханічне обладнання охоронної сигналізації тощо.

Також можна виділити такі основні засади створення СЗІ:

1. Системний підхід до побудови системи захисту інформації, такий підхід включає в себе оптимальне поєднання програмних, апаратних, фізичних та інших засобів захисту.
2. Принцип сталого розвитку системи. Цей принцип є одним із основних в організації системи захисту інформації. Способи злому конфіденційної інформації постійно розвиваються, тому забезпечення захищеності інформаційної системи не може бути статичним. Це динамічний процес, який полягає в аналізі та реалізації найбільш раціональних методів, способів та шляхів перетворення системи захисту.

3. Поділ і зведення повноважень щодо доступу до захисту. інформації до мінімуму.
4. Повний контроль та реєстрація спроб НСД. Необхідність ідентифікації та аутентифікації кожного користувача та контролювання його дій з наступним наголошенням на фактах здійснення різних дій у спеціалізованих журналах. Також обмеження щодо здійснення будь-якої дії в інформаційній системі без його попередньої реєстрації.
5. Забезпечення надійності системи захисту, тобто неможливість зниження рівня надійності у разі виникнення у системі збоїв, відмов, навмисних дій зломщика або ненавмисних помилок користувачів.
6. Контроль за коректною роботою системи.
7. Забезпечення економічного обґрунтування використання системи. Це виявляється у тому, що можливі збитки від несанкціонований доступ до конфіденційної інформації в ході реалізації загроз значно перевищує вартість розробки та експлуатації СЗІ [9].

Рис. 1.2. Схема організації СЗІ

На рис.1.2. представлена схема взаємодії компонентів СЗІ. Можна зробити висновок, що така система завжди знаходиться в динамічному стані.

Для належного захисту інформації (та, яка дійсно цінна для вас) обмежте доступ до неї. Обмеження доступу полягає у зменшенні кола осіб, яким відома закрита інформація. Йдеться не лише про встановлення усіляких комп'ютерних паролів, замикання документів у сейф та знищення чернеток.

Традиційно до основних засобів запобігання витоку інформації через використання інтернет-сервісів відносяться DLP (Data Loss Prevention)-системи. Існує безліч таких систем від різних виробників та з різноманітними функціональними можливостями, проте основним призначенням подібних систем є аналіз потоків даних, що перетинають периметр інформаційної системи, що захищається. Витік даних може завдати серйозного удару по бізнесу або навіть знищити його. Оскільки з кожним роком шахраї стають винахідливішими, ринок DLP-систем активно розвивається.

Компанія DeviceLock провела дослідження, в результаті якого з'ясувалося, що понад 70% витоків даних у 2019 році сталися у B2C-компаніях, 20% – у B2B-компаніях та ще близько 10% – у державних структурах. При цьому лідерами серед каналів витоку стали вивантаження з корпоративних інформаційних систем (понад 80%), що дозволяють зберегти дані у вигляді текстів або таблиць, і фотографії екрана, зроблені мобільними телефонами (близько 10%).

Щодня конкуренти або інтернет шахраї зливають колосальні обсяги даних, тому дуже важливо правильно вибрати систему, що запобігає витоку конфіденційної інформації. На прикладі декількох DLP розробок я розповім, що потрібно врахувати при виборі програмного забезпечення для вашої компанії.

2 АНАЛІЗ СУЧАСНИХ СИСТЕМ ЗАХИСТУ ВІД ВИТОКУКОНФІДЕНЦІЙНИХ ДАНИХ

2.1Система захисту від витоку конфіденційної інформації

Сьогодні питання інформаційної безпеки актуальне практично для будь-якої організації. Незважаючи на те, що системи безпеки зберігання інформаційних даних постійно оновлюються, проблема продовжує існувати. Через неправильні дії співробітників, а також у зв'язку з навмисними крадіжками корпоративних даних, компанії зазнають збитків, які значно перевищують витрати на забезпечення інформаційної безпеки.

Виконання корпоративних завдань у компаніях малого, середнього та великого бізнесу передбачає роботу з конфіденційними даними. Вони повинні бути надійно захищені від вилучення в загальний доступ. Вирішити проблему допоможе захист від витоків конфіденційної інформації.

Практично у будь-якої компанії зараз існує чимало даних, наслідки несанкціонованого витоку яких можуть завдати їй відчутних збитків. Наперед оцінити розмір цієї шкоди майже неможливо. Але в більшості випадків, для того щоб усвідомити небезпеку, що виходить від витоків інформації, достатньо уявити навіть загальні наслідки: зниження довіри та відтік клієнтів, проблеми в конкурентній боротьбі, витрати на PR, витік програмного коду, технологій, ноу-хау та багато іншого. Існує чотири класичні підходи до управління ризиками: прийняття, виняток, передача, зниження.

Для вирішення завдань захисту від витоків багато компаній використовують традиційні способи:

1. організаційні заходи - підписання працівниками положень щодо використання корпоративної інформації, проходження інструктажу та контроль за дотриманням норм;
2. використання систем архівування вихідної пошти з можливістю подальшого аналізу інцидентів;
3. розмежування прав доступу до інформації, призначеної для виконання службових обов'язків;
4. перекриття комп'ютерних портів введення-виведення інформації;
5. установка на локальні комп'ютери програм, що стежать за операціями користувачів (перехоплення клавіатури, зняття скріншотів, контроль операцій з буфером обміну);
6. фізичні обмеження - поводження з інформацією, що захищається в замкнутому сегменті мережі (без інтернету, без USB-портів тощо).

По мірі використання таких традиційних методів боротьби з внутрішніми порушниками та зі зростанням розмірів компанії, обсягу оброблюваної інформації стали посилюватися такі недоліки:

1. кількість фінансово-значимих інцидентів витоку інформації збільшується з кожним роком;
2. з'являються нові джерела внутрішніх загроз (технічні шляхи виведення інформації із корпоративної інформаційної системи);
3. щонайменші обмеження користувачів інформаційних систем призводять до порушення налагоджених бізнес-процесів (співробітники не можуть виконувати свої службові обов'язки);
4. юридичні департаменти компаній на законній основі протистоять службам безпеки, які розкривають електронне листування працівників;
5. невеликий відділ інформаційної безпеки повинен вирішувати завдання обробки величезної кількості подій від різноманітних систем безпеки, серед яких доводиться вручну виявляти інциденти.

У зв'язку з описаними тенденціями у світовій практиці протягом років сформувалися вимоги, притаманні систем запобігання витоків інформації (Data Loss Prevention чи Data Leak Prevention, DLP).

Незважаючи на свою назву, так звані системи запобігання витоку даних (DLP)

не можуть у прямому сенсі запобігти всім витокам, оскільки існують людський фактор, хакерські способи обходу системи. Комерційна доцільність даних систем полягає у значному зниженні ризиків витоку інформації з необережності та у частковому зниженні ризиків навмисного крадіжки конфіденційних відомостей.

DLP-системи будуються на аналізі потоків даних, що перетинають периметр інформаційної системи, що захищається. При детектуванні в цьому потоці конфіденційної інформації спрацьовує активний компонент системи, і передача повідомлення (пакета, потоку, сесії) блокується.

Важливим доповненням до визначення є також те, що DLP-система повинна охоплювати всі основні канали витоку конфіденційної інформації. Даної позиції дотримується сьогодні більшість експертів у цій галузі. Крім того, DLP-система повинна бути чутливою по відношенню до вмісту (контенту), що перевіряється, і забезпечувати автоматизований механізм відстеження порушень заданих правил, тобто, без залучення значної кількості співробітників-контролерів. З урахуванням сказаного можна запропонувати таке визначення системи захисту від витоків даних: автоматизований засіб, що дозволяє розпізнавати та/або блокувати переміщення конфіденційних даних за межі інформаційної системи, що захищається, по всіх каналах, що використовуються в повсякденній роботі.

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: ненавмисні і навмисні.

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

Навмисний витік конфіденційної інформації характеризуються тим, що зловмисник, маючи доступ до інформації, яка знаходиться під захистом, усвідомлює протиправність своїх дій і розуміє їх можливі негативні наслідки. Причому основною мотивацією для здійснення подібних злочинів є, в більшості випадків, грошова нажива або отримання будь якої вигоди. Крім того, крадіжка важливих даних хакерами, які обманним або іншим шляхом отримали прямий доступ до них за допомогою співробітників організації, теж відноситься до

навмисного витоку інформації, навіть якщо протиправних намірів у співробітника не було.

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 засобів захисту, таких як антивіруси, міжмережеві екрани, системи автентифікації та контролю доступу не здатні забезпечити ефективний захист від внутрішніх загроз.

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

Рисунок 2.1 – Поширені помилки користувачів, що призводять до ненавмисного витоку даних

Здійснити запобігання витоку конфіденційної інформації дозволяють DLP-системи.

DLP-системи забезпечують блокування загроз, дбають про безпеку інформації, контролюють роботу персоналу. Це комплексне програмне забезпечення, що запобігає несанкціонованому доступу і втраті важливої, для

вашої організації, інформації. Завдяки глибокому аналізу вхідних і вихідних даних, DLP-система розпізнає загрози, наприклад при спробі скопіювати інформацію на інший пристрій, та сповістить про це її власника. Також система визначає рівень конфіденційності документів, аналізуючи відповідні маркери або їх вміст.

DLP-системи не тільки захищають від витоку конфіденційної інформації, а й дозволяють виконувати широкий спектр інших не менш важливих завдань захисту інформації. Ці системи можуть забезпечити контроль роботи за співробітниками, перевірку їх комунікацій, правомірність дій та 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 вжити відповідних заходів.

Основні функції DLP-систем [10, 11]:

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

– контроль збереження інформації на зовнішніх носіях та мобільних пристроях;

– захист інформації від витоку шляхом контролю за друком даних;

– блокування спроб відсилання або збереження конфіденційних даних, інформування адміністраторів ІБ про інциденти та спроби створення копій важливої інформації;

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

– запобігання витоку інформації контролюючи життєвий цикл і рух конфіденційних даних.

В результаті використання DLP-систем можуть бути вирішені наступні питання:

– запобігання витокам і несанкціонованої передачі конфіденційної інформації;

– мінімізація ризиків фінансових і репутаційних збитків;

– підвищення дисципліни працівників та користувачів;

– розслідування інцидентів та їх наслідків;

– ліквідація загроз безпеці персональних даних, відповідності вимогам, щодо захисту персональних даних.

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

Сучасна DLP-система, як правило, являє собою розподілений програмно-апаратний комплекс, що складається з кількох модулів, які функціонують на виділених серверах, на робочих місцях співробітників компанії (персональних комп'ютерах, робочих станціях та 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 за якими закладено в систему;

– модулі пасивного і (або) активного спостереження, контроль за діями співробітників компанії (користувачів). Перелік дій, що відслідковує і контролює система, встановлюється заздалегідь, і як правило носить обмежений характер. Стандартний перелік, зазвичай, включає в себе контроль входу і виходу з системи, безпровідної 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-систем можуть зберігатися всі поштові повідомлення контрольованого користувача, незважаючи на те, що користувач може видаляти отримане або відправлене повідомлення, а відновлення з резервної копії може займати багато часу або ж резервування пошти може не бути зовсім. За адресатами листів може бути

побудований відповідний звіт, який дасть зрозуміти, з ким і в якому обсязі взаємодіяв користувач (рисунок 2.2). Також здійснюється аналіз тексту листів на збіг з певними словоформами.

2. Контроль програм обміну повідомленнями. Всі повідомлення месенджерів користувача за яким здійснюється контроль, можуть зберігатися в базах даних DLP. Згідно з політикою і правилами, що налаштовані в DLP, відбувається спрацьовування на певний контент, оператор DLP оповіщається про відповідні повідомлення. Незважаючи на те, що обмін між клієнтом і сервером месенджера може відбутися за допомогою засобів шифрування месенджера, DLP-система отримає незашифровані дані, якщо вона підтримує відповідний месенджер.

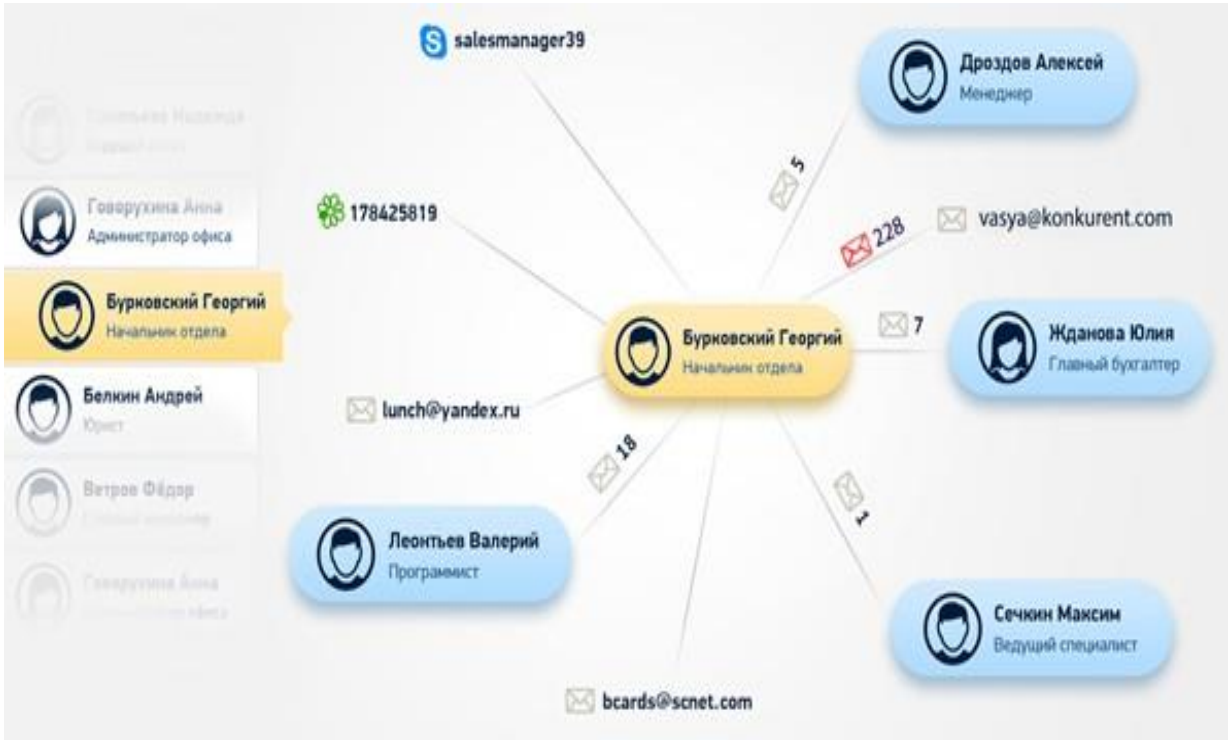


Рисунок 2.2 – Контроль корпоративної пошти

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

4. Контроль зовнішніх накопичувачів. DLP-система фіксує та розпізнає пристрої, які підключаються до робочого місця. Також мається можливість задання переліку дозволених пристроїв і шифрування даних на них. У разі відповідного

налаштування система здатна зробити копію всієї інформації, що зберігається на підключених зовнішніх пристроях користувача, або тільки файлів, які зчитуються/записуються на зовнішні пристрої.

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

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

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

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

9. Контроль обміну файлами (ftp, sftp). Створює запис копій файлів, що передаються користувачем 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 камер, підключених до робочого місця. У частіше 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 важливої інформації.

Розглянемо можливу архітектуру DLP-системи (рисунок 2.3).

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

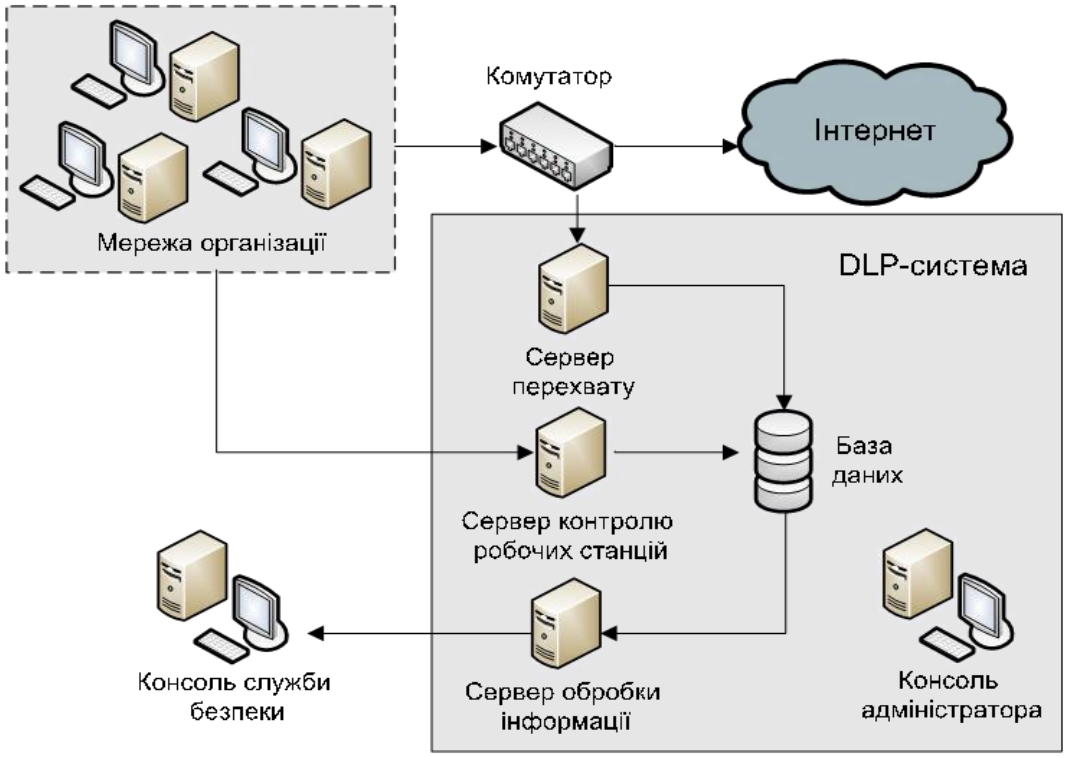


Рисунок 2.3 – Архітектура DLP-системи

Інформація, отримана за допомогою сервера перехвату (повідомлення в мессенджерах, вкладені файли, електронні листи тощо), зберігається на сервері баз даних.

Після збереження в базі даних, вся перехоплена інформація надходить до сервера 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 передачу інформації з порушенням прийнятої в компанії політики безпеки.

Сервер контролю робочих пристроїв призначений для централізованої установки на комп'ютери програм-агентів, призначених для перехоплення безпосередньо з робочих пристроїв користувачів трафіку, в тому числі

шифрованого, а також інформації, 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 на всіх встановлених в мережі агентів та в разі виявлення збою або примусового відключення агента користувачем будь-якого комп'ютера автоматично здійснить повторну установку.

Консоль адміністратора використовується в DLP-системі для централізованої установки і настройки роботи всіх елементів програми та для віддаленого встановлення програм-агентів на робочі станції користувачів. Через консоль адміністратора здійснюється налаштування 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 та 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 мессенджерів, електронні листи, файли тощо) і зберігаються у базах даних DLP-систем.

Програми-агенти дозволяють перехоплювати як нешифровані, так і зашифровані дані. Агенти віддалено встановлюються на комп'ютери сервером контролю за робочими станціями. Агенти відстежують дані, що пересилаються в мессенджерах і по електронній пошті, всі випадки відправки інформації, яка є під захистом, користувачами на зовнішні пристрої або принтери та передають всі перехоплені дані на сервер обробки. Також за допомогою програм-агентів здійснюєтьсямоніторинг діяльності співробітників на робочих місцях та 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 консолі адміністратора.

Практика показує, що повноцінне використання системи протидії витокам інформації на основі одного з DLP-продуктів можливе лише за активної участі спеціалізованого системного інтегратора. Якщо компанія планує зайнятися питаннями захисту конфіденційних даних, то перше, з чого слід почати, - звернутися до консультанта. Це може бути IT-компанія, що має значний досвід застосування систем протидії витокам інформації. Спільно вони пройдуть три початкові етапи:

1. обговорити з групою експертів консультанта поточну ситуацію та мету впровадження DLP-системи в компанії;
2. взяти участь у "живій" демонстрації пропонованих до впровадження DLP-систем та в рамках показу разом з експертами вибрати одну з них для пілотного розгортання;
3. погодити з консультантом параметри пілотного запуску системи, зафіксувати очікування від його реалізації та провести розгортання.

Крім встановлення програмного забезпечення та створення оптимальної конфігурації системи служби безпеки підприємств у рамках реалізованих організаційних та технічних рішень повинні систематично проводитись перевірки для виявлення заставних пристроїв – електронних пристроїв перехоплення інформації – та для проведення спеціальних досліджень на побічні електромагнітні випромінювання та наведення. Для організації таких перевірок також потрібна спеціальна апаратура. Забезпечуючи охорону певної зони, необхідно приділяти увагу пропускному режиму на контрольованій території та забезпечувати виявлення прихованими засобами електромагнітних випромінювань, що виходять від усіх візитерів – від клієнтів та контрагентів до ремонтних служб. Кожен з них може пронести в периметр закладний пристрій-

перехоплювач звукової інформації.

Тільки комбінація всіх сучасних засобів технічного захисту з організаційними заходами дозволить досягти успіху у боротьбі з витоком інформації.

2.2 Аналіз сучасних DLP-систем

Проведемо аналіз найпопулярніших DLP-систем, порівнявши їх функції та характеристики, розглянемо для яких цілей краще використовувати ці системи захисту [9, 12-13,17].

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 віддалених пристроях;

– всі дії співробітників зберігаються в архів, після чого отримана інформація підлягає аналізу і, при необхідності, дії співробітників будуть заблокованими;

– блокування для пристроїв (передача файлів або печаті);

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

Система 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;

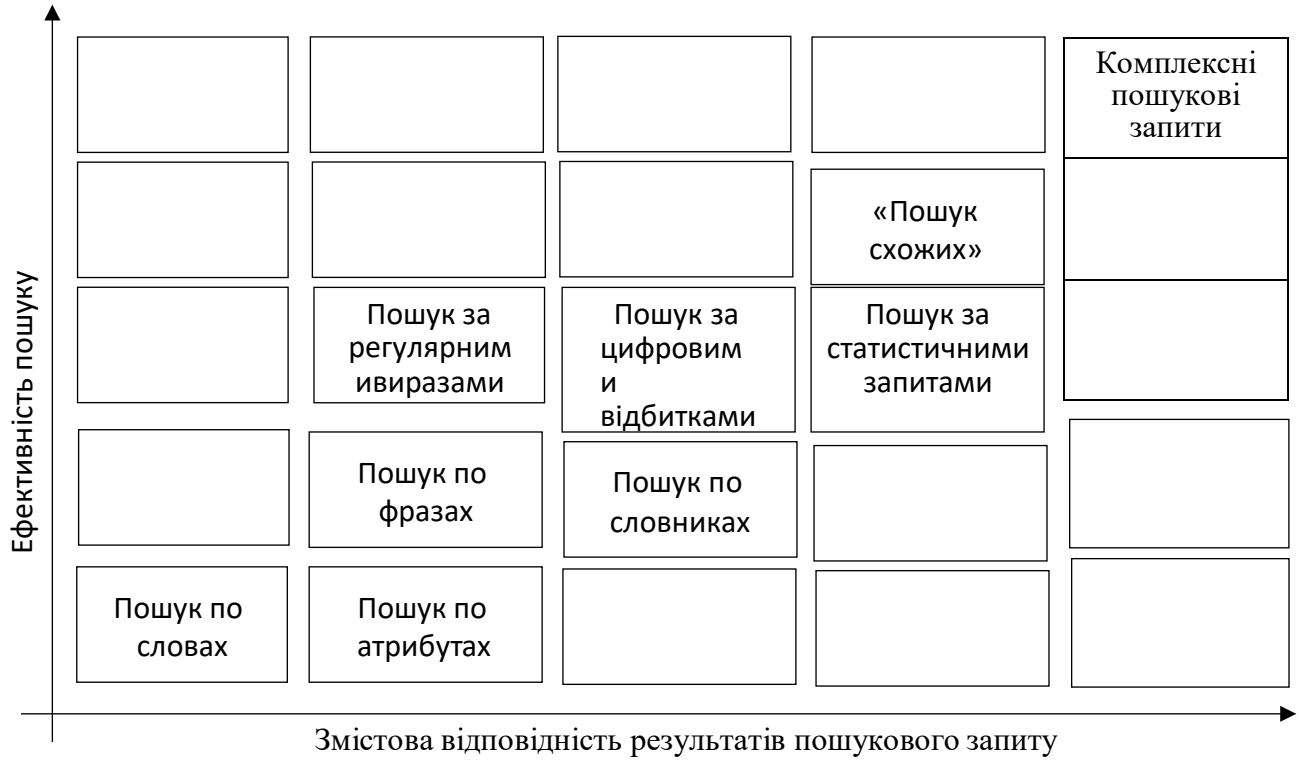
– безліч додаткових функцій (аудит пристроїв, кодування, блокування різних об'єктів файлових систем);

– 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 (таблиця 2.4) [12].



Таблиця 2.4 – Пошукові механізми DLP-системи SearchInform

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

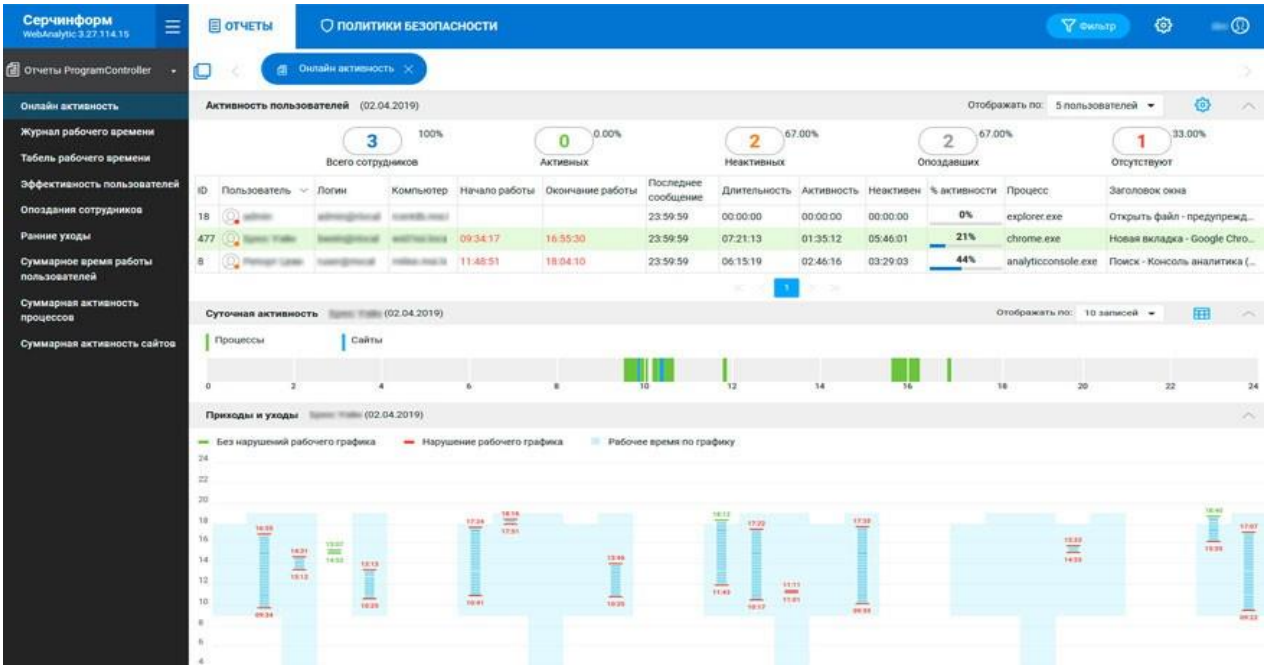


Рисунок 2.5 – Екран звітів контролю діючих співробітників

В якості недоліків можна виділити наступне:

– 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

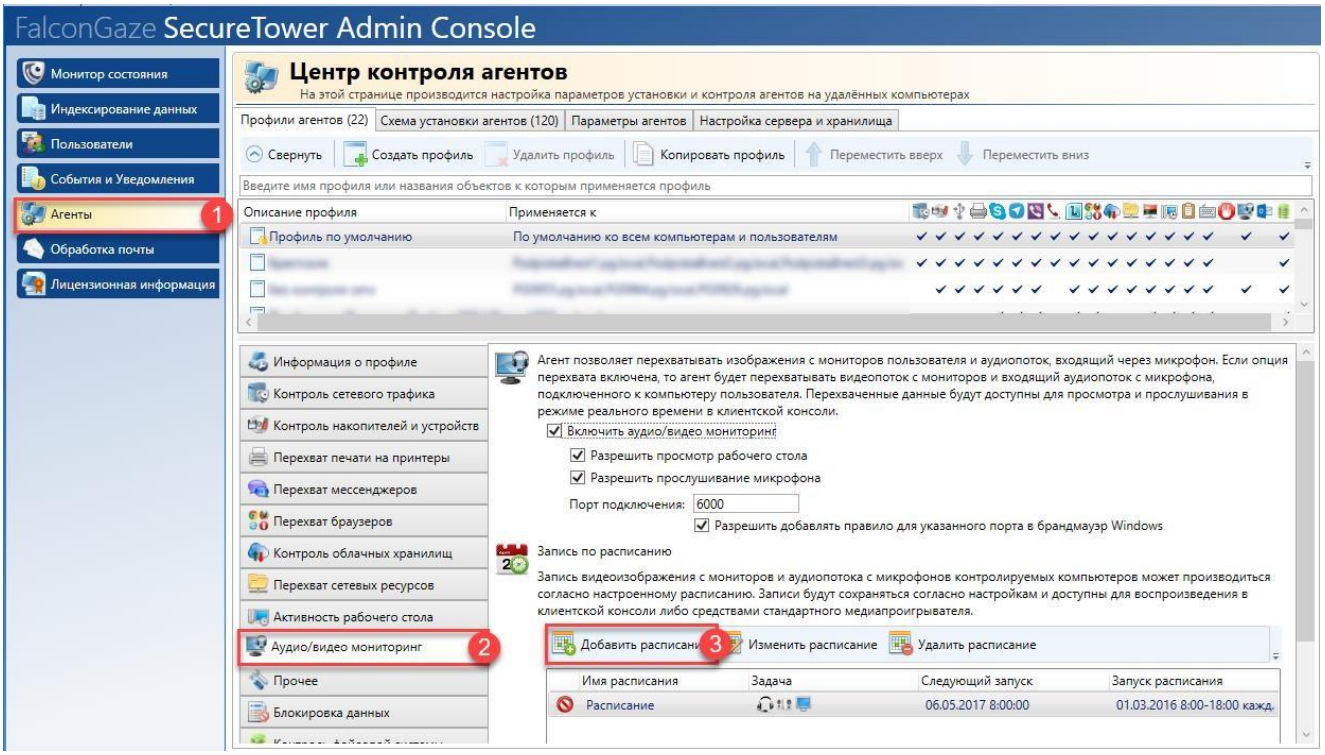


Рисунок 2.6 – Робочий екран центру контролю агентів SecureTower

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 політикдля 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 скріншотів 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.

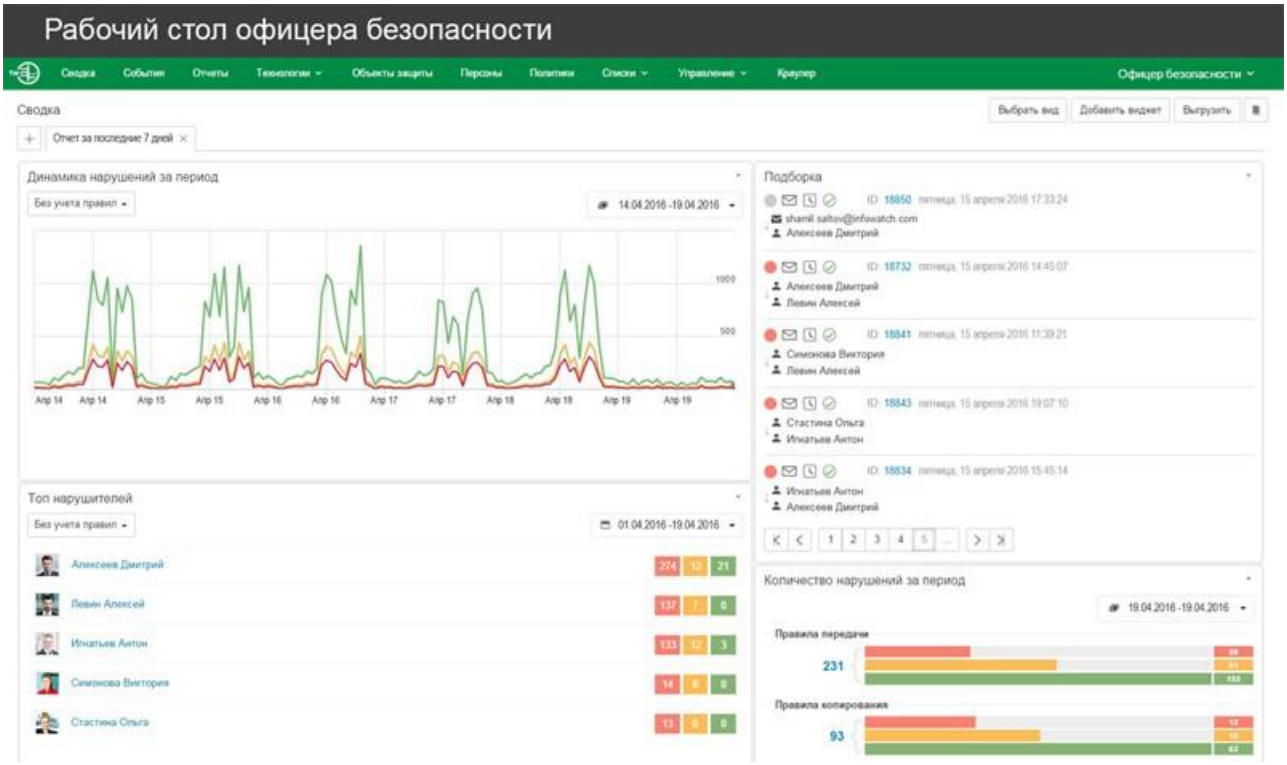


Рисунок 2.7 –Робочий екран служби безпеки Infowatch

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.

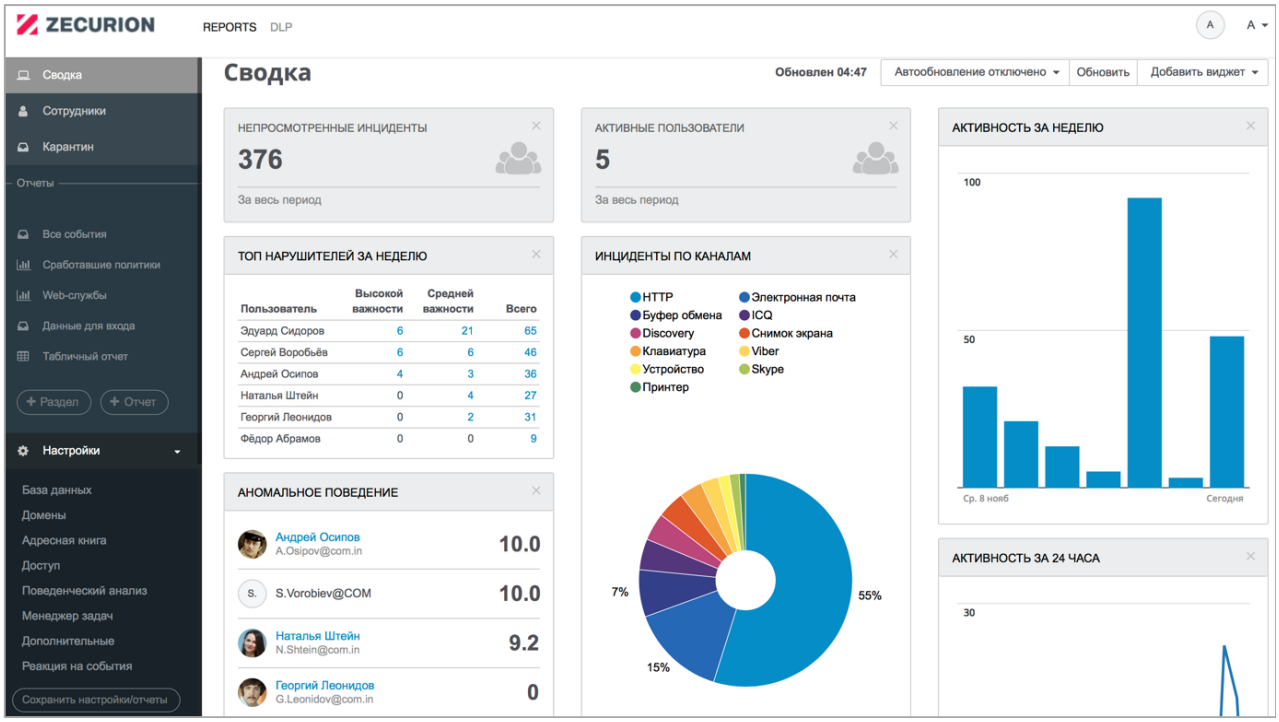


Рисунок 2.8 – Екран звіту DLP-системи Zecurion

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.

2.2.5. 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.

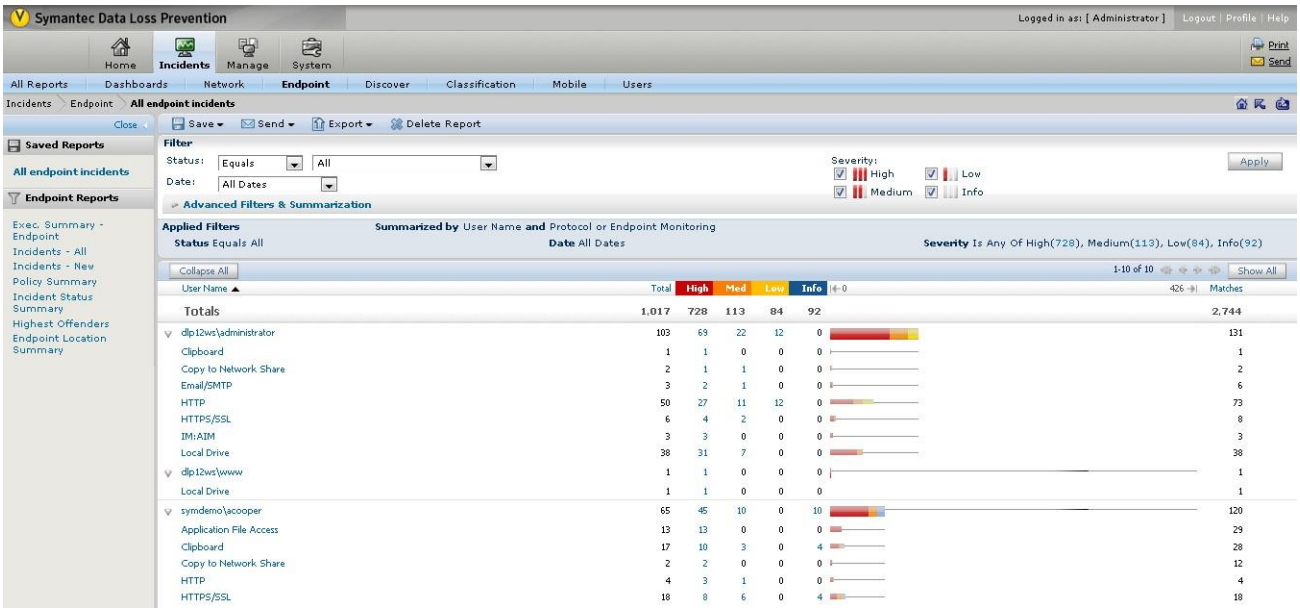


Рисунок 2.9 – Екран контролю інцидентів DLP-системи Symantec

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.

2.3Порівняльний аналіз сучасних DLP-систем

В роботі був проведений порівняльний аналіз розглянутих DLP-систем якпо загальним характеристикам, так і функціоналу з виявлення інцидентів. Результати аналізу представлені в таблиці 2.1 [20-23].

Таблиця 2.3

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, Falcongaze та інші) представляють на ринок системи корпоративного класу зі зручним інтерфейсом, широкими можливостями контролю та аналітичними функціями.

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

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

Системи DLP — це програмні продукти, які захищають організації від втрати конфіденційної інформації. Такі системи створюють безпечний цифровий «периметр» навколо організації та аналізують всю інформацію, що виходить, а в деяких випадках і вхідну інформацію. Контрольованою інформацією має бути не тільки інтернет-трафік, а й ряд інших інформаційних потоків: документи, які вилучаються із захищеного контуру захисту, надсилаються на зовнішні носії, друкуються на принтерах, надсилаються на мобільні носії тощо.

Оскільки система DLP повинна запобігати витоку конфіденційної інформації, вона повинна мати вбудовані механізми визначення рівня конфіденційності документа, виявленого в перехопленому трафіку даних. Зазвичай два найпоширеніші методи: аналізуючи конкретні маркери документа та аналізуючи вміст документа. Наразі другий варіант є більш поширеним, оскільки він стійкий до змін у документі перед його відправкою, а також дозволяє легко розширити кількість конфіденційних документів, з якими може працювати система.

Системи DLP перехоплюють весь трафік даних, що виходить за межі компанії, і аналізують його на предмет конфіденційної інформації. Передові системи DLP зазвичай використовують такі технології, як цифровий відбиток, лінгвістичний аналіз, аналіз графічних файлів (OCR), технології самонавчання та інші для ідентифікації конфіденційних даних.

Технологія категоризації інформації є основою систем DLP. Кожен виробник вважає свої методи виявлення конфіденційної інформації унікальними, захищаючи їх патентами та створюючи для них спеціальні торгові марки. Адже, інші елементи архітектури, крім цих технологій (перехоплювачі протоколів, синтаксичний аналізатор форматів, управління інцидентами та сховища даних), ідентичні для більшості виробників і навіть інтегровані в інші продукти безпеки для інформаційної інфраструктури великих компаній. В основному, для категоризації даних у продуктах з метою захисту інформації компанії від витоку

використовуються дві основні групи технологій - лінгвістичний (морфологічний, семантичний) аналіз та статистичні методи (Digital Fingerprints, Document DNA, антиплагіат) [24]. Кожна технологія має свої сильні та слабкі сторони, які визначають область її застосування.

3.1 Принципи лінгвістичного аналізу інформації

Використання поштових серверів для блокування вихідної електронної пошти зі словами, які зупиняють передачу («секретно», «конфіденційно» тощо) можна розглядати як прототип сучасних систем DLP. Однак цей метод не може забезпечити захист від зловмисників, оскільки досить легко видалити ці слова з документа, які часто ставлять окремим грифом на документі.

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

На початку століття між спамерами та антиспамерами спалахнула мовна війна. Щоб обійти фільтри на основі ключових слів, літери були замінені аналогічними літерами з інших кодувань або цифр, трансліт, випадкових пробілів, підкреслення або розривів рядків у тексті. Антиспамери швидко навчилися використовувати такі методи, але потім з'явився графічний спам та інші види спаму.

Однак для боротьби зі спамом не достатньо розділити потік інформації на дві категорії: спам і не спам. Цього недостатньо, щоб захистити корпоративні дані від витоку – не можна просто розділити інформацію на конфіденційну та неконфіденційну. Необхідно вміти класифікувати інформацію за функціональною приналежністю (фінансова, виробнича, технологічна, комерційна, маркетингова) і в межах класів - класифікувати її за рівнем доступу (для вільного розповсюдження, для обмеженого доступу, для службового користування, секретна, надсекретна) [25].

У системі лінгвістичного аналізу контекстуальні прийоми почали використовуватися не тільки пошуку певних слів, а й уживанні певного терміна в поєднанні з цими словами, тобто в якому контексті.

Більшість сучасних систем лінгвістичного аналізу використовують не лише контекстний аналіз, а й семантичний аналіз. Чим більший аналізований фрагмент, тим ефективніші ці технології. На великому фрагменті тексту є більш детальним аналіз, який точніше визначає категорію та клас документа [16]. При аналізі коротких повідомлень (SMS, повідомлення мессенджера) найкращим рішенням є використання ключових слів.

Розглянемо переваги лінгвістичних технологій.

1. Лінгвістичні технології працюють безпосередньо зі змістом документів, тобто незалежно від того, де і як створено документ, який на ньому штамп і як називається файл – якщо збіг необхідний, документи відразу захищається. Конфіденційні документи, які створюються та використовуються на підприємстві, можуть мати певні назви, мати печатку або маркування. Але вхідні дані можуть не мати прийнятих в організації штампів і ярликів. Чернетки (якщо, звичайно, не створені в захищеній системі документообігу) вже можуть містити конфіденційну інформацію, але ще не мати необхідних штампів і маркування.
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. Здатність розпізнавати категорії в інформаційних потоках, які не стосуються документів, які є в компанії. Інструмент контролю вмісту інформаційних потоків може включати такі категорії, як незаконна діяльність (піратство, розповсюдження нелегальних товарів), використання інфраструктури компанії у власних цілях, пошкодження іміджу (наприклад, поширення ганебних чуток) тощо [24].

Лінгвістичних технологій мають також і недоліки.

1. Основним недоліком лінгвістичних технологій є їх мовна залежність. Лінгвістичні методи, розроблені для однієї мови, не можна використовувати для аналізу іншої. Особливо це стало помітно, коли на український ринок вийшли міжнародні виробники. Не достатньо було перекладу на українську мову категорій та ключових слів - в англійській мові зовсім інший словотвір. У Німеччині американські виробники лінгвістичних технологій зіткнулися з іншою

проблемою, як-от "компаунди", складові слова. У німецькій мові прийнято поєднувати визначення до головного слова, в результаті чого виходять слова, що складаються з десятка коренів. В англійській мові такого немає.

Також важко обробляти багатомовні тексти за допомогою лінгвістичних технологій. Однак більшість методів все ще працюють з двома мовами, переважно національна мова + англійська - цього достатньо для більшості бізнес-завдань.

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 зкожного 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 [23, 24].

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 бутизаборонена відправка зовні деяких типів файлів. При цьому якщо користувач змінить розширення файлу, то система все одно повинна «впізнати» тип файлу івжити 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 вбазі "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 [26].

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 під-категоріями, 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 методу 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 [26]. 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 ізакінчуючи корпоративної аналітикою і кібербезпекою. Такі компанії, як Gurucul, Niara, Splunk, StatusToday, Trudera і Vectra Networks намагаються взятина себе провідну роль в застосуванні інноваційних програм DLP-систем. Інші учасники ринку, такі як Deep Instinct і Spark Cognition застосовують більшфункціональні моделі, глибоке навчання і обробку природної мови.

3.4. Розробка рекомендацій щодо вибору системи захисту від витоку конфіденційної інформації

3.4.1.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, категоріювання 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 3.4.1).

Рисунок 3.4.1 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 меншоюкваліфікацією.

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, якіпорушують 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 тощо, 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 зрозумілішеі

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 3.4.1).

Рисунок 3.4.1 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.

3.4.2.Проблемні питання при застосуванні DLP-систем

Деякі організації впроваджують DLP, не проводячи необхідного попереднього аналізу, що враховує специфіку компанії, а тому в результаті отримують паралізовані інформаційні потоки, підвисання обладнання, непотрібне додаткове завантаження офіцерів інформаційної безпеки.

Все це викликано початковим нерозумінням впливу системи на щоденні інформаційні процеси в компанії, до того ж відповідальні за впровадження співробітники не становлять обсягів «порушень», які можуть виявити некоректно налаштовані правила безпекової політики. Природно, багато повідомлень виявляються помилковими. Однак у гонитві за примарою витрачаються час, сили та нерви аналітиків і, звичайно, ресурси компанії.

Причина полягає в тому, що на попередньому етапі імплементації системи не вирішено низку завдань:

- не визначено конкретну мету впровадження DLP-рішення (контроль несанкціонованого доступу, запобігання випадковому розсиланню конфіденційних даних, дотримання вимог регуляторів щодо захисту персональних даних або посилення політики безпеки в цілому, а можливо необхідно було лише контролювати використання інтернету персоналом або зрозуміти, що зберігається на робочих станціях працівників);
- не з'ясовано, чи достатньо потужностей обладнання підприємства;
- DLP не тестувалася в пілотному режимі в середині компанії;
- блокування було обрано як основний метод запобігання переміщенню чутливих даних, у той час як принаймні на перших етапах варто вибрати опцію повідомлення співробітника безпеки. По-перше, це дозволить краще вивчити інформаційні потоки у компанії; по-друге, блокування може стати на заваді співробітнику виконувати його трудові обов'язки.

Одні компанії вирішують проблеми, що виникли, наймаючи безліч аналітиків. У їхнє завдання входить зробити все можливе, щоб відшукати серед інформаційного шуму спрацьовування інциденти, що мають під собою реальну основу, і зловити інсайдерів.

Інші налаштовують безпекові політики таким чином, щоб максимально не дати системі «завадити» вести бізнес. DLP встановлюється номінально та майже не функціонує. Тим самим було знижується та ймовірна користь, яку організації можуть отримувати від технології.

Частина компаній просто не завершують контур безпеки, залишаючи деякі канали незахищеними (порти USB, електронну пошту і т. д.).

Все вище наведене, разом із вартістю системи, і породжує ставлення до DLP як дорогої іграшки, складної у використанні або малоефективної. У той час як DLP особливо хороша у виявленні небезпечної політики поводження з даними в компанії (і подальшому її налаштуванні, відповідно), запобіганні випадковим витокам, а також загальнопоширеним способам розкрадання.

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 конкретнимиспівробітниками 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 [28-30].

Інформаційна безпека компанії – складний процес, який потребує уважного підходу. І принцип «встановив – і забув» зовсім не доречний із системами, що передбачають індивідуальне підстроювання.

Найчастіше остаточні рішення щодо придбання DLP приймаються у зв'язку з одним із низки факторів.

Перший – справді серйозні події, пов'язані з інцидентами безпеки. Коли організація на власному досвіді зазнає наслідків витоку, будь-які доводи «проти» втрачають вагу. За великим рахунком, в даний час компанії діляться на ті, які поки не мали витоків, і ті, які вже вживають захисних заходів.

Другий - зростання та ускладнення галузі інформаційних технологій. Виникла та поширилася практика використання хмарних програм, мобільних систем та віддалених підключень. В даний час дані набагато менше сконцентровані в одному місці, ніж це було всього кілька років тому, коли хмарні та мобільні сервіси лише починали набувати популярності.

Нарешті, вирішальним моментом стало запровадження нормативних вимог, які містять положення захисту конфіденційних даних і накладають значні штрафи за недотримання.

Важливо, що сучасні DLP-технологи розвиваються дуже швидкими темпами. Зросла здатність контролювати переміщення даних по численних каналах, таких як хмарні сервіси, і збільшився діапазон форматів, що охоплюються, наприклад, стали доступні для аналізу зображення і голосові повідомлення. Для оптимізації роботи з інцидентами безпеки SecureTower розробила модуль «Центр розслідувань», який спрощує роботу співробітників служби безпеки завдяки можливості не виходячи із системи розслідувати

інциденти безпеки та формувати справи, в яких можна докладно фіксувати їхній хід, виявляти фігурантів та отримувати автоматично складені звіти.

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, Falcongaze та інші) представляють на ринок системи корпоративного класу зі зручним інтерфейсом, широкими можливостями контролю та аналітичними функціями. Менш відомі компанії SearchInform, RSA 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. Бондаренко Е. М. Конфіденційна інформація у трудових відносинах / Е. М. Бондаренко, Д.В. Іванов - 2012. 8с.

15. Блінов А.М. Інформаційна безпека: Навчальний посібник. Частина 1. - СПб.: Вид-во СПбГУЕФ, 2010. - 96 с

16. Аверченков В.І. Організаційний захист інформації: навч. Посібник для вузів/В.І. Аверченко, М.Ю. Ритов. - Брянськ: БДТУ, 2005. - 184 с.

17. FalconGaze SecureTower [Електронний ресурс]. – Режим доступу:https://www.tadviser.ru/index.php/Продукт:FalconGaze_SecureTower

18. Огляд та порівняння кращих безкоштовних open source DLP систем 2021 року [Електронний ресурс]. – Режим доступу: https://www.kickidler.com/ru/info/obzor-i-sravnenie-luchshix-besplatnyix-open-source-dlp-sistem-2019-goda.html.

19. Цілі та завдання захисту інформації [Електронний ресурс]. – Режим доступу: http://csaa.ru/celi-i-zadachi-zashhity-informacii/.

20. Способи неправомірного доступу до інформації [Електронний ресурс] – Режим доступу: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/.

21. Інформаційна безпека [Електронний ресурс]. – Режим доступу: https://pirit.biz/reshenija/informacionnaja-bezopasnost.

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

23. Сравнение DLP-систем [Електронний ресурс]. – Режим доступу:https://searchinform.ru/informatsionnaya-bezopasnost/dlp-

24. sistemy/kak-vybrat-dlp- sistemu/sravnenie-dlp-sistem/ – Заголовок з екрана.

25. 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.

26. 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.

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

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

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

30. 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.

31. Ушатов В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки / В. Ушатов, О. Сєвєрінов // GLOBAL CYBESECURITY FORUM. Матеріали першого міжнародного науково-практичногофоруму – Х.: ХНУРЕ, 2019. – С. 104-105