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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Ковриги Данила Андрійовича*

академічної групи *125м-19-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методика виявлення порушень політики безпеки оператора call-центру при обробці запитів клієнта*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Флоров С.В.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту *Ковризі Данилу Андрійовичу* **академічної групи** *125м-19-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Методика виявлення порушень політики безпеки оператора call-центру при обробці запитів клієнта***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Виконати аналіз побудови call-центру, систем контролю оператора call-центру та DLP систем.	10.10.2020
Розділ 2	Виконати аналіз моделі загроз call-центру, вибрати профіль захищеності, сконфігурувати політики безпеки та розробити методику виявлення порушень політики безпеки оператора call-центру при обробці запитів клієнта.	20.11.2020
Розділ 3	Виконати розрахунок витрат на розробку методики виявлення порушень політики безпеки оператора call-центру при обробці запитів клієнта.	05.12.2020

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

Дата видачі: 01.09.2020р.

Дата подання до екзаменаційної комісії: 11.12.2020р.

Прийнято до виконання _____ Коврига Д.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 135 с., 10 рис., 6 табл., 5 додатків, 14 джерел.

Метою дипломної роботи є: розробка методики виявлення порушень політики безпеки оператора call-центра при обробці запитів.

Предмет досліджень: методика виявлення порушень політики безпеки оператора call-центра при обробці запитів.

Практична цінність: підвищення рівня контролю за конфіденційною інформацією при обробці запита клієнта оператором call-центру.

В першому розділі кваліфікаційної роботи було розглянуто: архітектуру call-центру, актуальність DLP систем, функціональні можливості DLP систем, принципи роботи оператора call-центру та інформаційні потоки.

В другому розділі кваліфікаційної роботи було розглянуто моделі загроз та порушника, профіль захищеності, політики безпеки, архітектура call-центру після впровадження методики та конфігурацію Forcepoint DLP.

В третьому розділі кваліфікаційної роботи було проведено розрахунки капітальних витрат, збитків від атаки на вузол мережі, були визначені та проаналізовані показники економічної ефективності методики.

DLP, ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ,CALL-ЦЕНТР,SPEECH-TO-TEXT, FORCEPOINT,CALL-ЦЕНТР.

РЕФЕРАТ

Пояснительная записка: 135 с., 10 рис., 6 табл., 5 приложений, 14 источников.

Целью работы является разработка методики выявления нарушений политики безопасности оператора call-центра при обработке запросов.

Предмет исследований: методика выявления нарушений политики безопасности оператора call-центра при обработке запросов.

Практическая ценность: повышение уровня контроля над конфиденциальной информацией при обработке запроса клиента оператором колл-центра.

В первой главе квалификационной работы были рассмотрены: архитектуру call-центра, актуальность DLP систем, функциональные возможности DLP систем, принципы работы оператора call-центра и информационные потоки.

Во втором разделе квалификационной работы были рассмотрены модели угроз и нарушителя, профиль защищенности, политики безопасности, архитектура call-центра после внедрения методики и конфигурацию Forcepoint DLP.

В третьем разделе квалификационной работы было проведено расчеты капитальных расходов, убытков от атаки на узел сети, были определены и проанализированы показатели экономической эффективности методики.

DLP, ИНФОРМАЦИЯ С ОГРАНИЧЕНЫМ ДОСТУПОМ,CALL-ЦЕНТР,SPEECH-TO-TEXT, FORCEPOINT, CALL-ЦЕНТР.

ABSTRACT

Explanatory note: 135 pp., 10 fig., 6 table, 5 appendix, 14 source.

The purpose of the thesis is: to develop a method of detecting violations of the security policy of the call center operator when processing requests.

Subject of research: methods of detecting violations of the security policy of the call center operator when processing requests.

Practical value: increasing the level of control over confidential information when processing a customer request by a call center operator.

In the first section of the qualification work were considered: the architecture of the call center, the relevance of DLP systems, the functionality of DLP systems, the principles of the call center operator and information flows.

In the second section of the qualification work, threat and intruder models, security profile, security policy, call-center architecture after the implementation of the methodology and Forcepoint DLP configuration were considered.

In the third section of the qualification work, calculations of capital costs, losses from the attack on the network node were performed, indicators of economic efficiency of the methodology were determined and analyzed.

DLP, INFORMATION WITH RESTRICTED ACCESS, CALL-CENTER, SPEECH-TO-TEXT, FORCEPOINT, CALL CENTR.

СПИСОКУ МОВНИХ СКОРОЧЕНЬ

АРМ	–	автоматизоване робоче місце;
АС	–	автоматизована система;
ОС	–	операційна система;
ПЗ	–	програмне забезпечення;
КС	–	комп’ютерна система;
DLP	–	data lose prevention;
KPI	–	key performance indicators;

ЗМІСТ

с.

ВСТУП

У цифровому світі все - це дані - інформація про банківський рахунок та інші офіційні документи, електронні листи та повідомлення тощо. Будь-яка організація має документи з обмеженим доступом, яка містить ту або іншу конфіденційну інформацію. Виток цієї конфіденційної інформації може призвести до фінансових, репутаційних втрат. Виток конфіденційної інформації пов'язаний не тільки з взломом і вторгненням до інформаційної системи зовнішніх зловмисників, а й з необережними і зловмисними діями співробітників організації . За даними дослідницького центру компанії InfoWatch за 2018 рік, 42% витоку інформації відбувається внаслідок порушень політики безпеки організації за недбалістю користувачів. Дослідження, проведене компанією Intel, показало, що інформація з 70% випадків втрати даних була публічного розголошенна, або мала негативний фінансовий ефект. Виходячи з цього сьогодні велику актуальність у бізнесі маюсь системи запобігання втраті даних, оскільки будь-яка організація залежить від великої кількості конфіденційних даних, які класифікуються як корпоративні активи.

До систем запобігання втраті даних входять такі як DLP (Data Loss Prevention) – системи, яка захищають конфіденційну інформацію від витоку за межі інформаційної системи. Організації користуються DLP системами через небезпечність внутрішніх та зовнішніх загроз та через суворі закони про конфіденційність даних, багато з яких мають жорсткі вимоги щодо захисту даних або доступу до даних. Особливо доцільне використання DLP систем є в таких організаціях як call-центр, так як існує великий ризик людської помилки. Окрім моніторингу та контролю діяльності кінцевих точок, деякі інструменти DLP також можуть використовуватися для фільтрації потоків даних у корпоративній мережі та захисту даних у русі.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Архітектура call-центру

Call-центр - це окрема служба або навіть спеціальна компанія, що надає послуги на аутсорсинг, яка займається обробкою вхідних голосових дзвінків від клієнтів і здійснює вихідні дзвінки. Ця організація може виробляти додатково обробку електронних звернень громадян, приймаючи їх по електронній пошті або SMS, проводити опитування, приймати і відправляти факси, вести Інтернет-чати і т.д.

З технічної точки зору схема типового call-центру - це програмно-апаратний комплекс, всередині якого відбувається маршрутизація вхідних і вихідних телефонних викликів. Устаткування контактного центру дозволяє вести запис розмов, реєструвати голосові виклики, автоматично визначати номер абонента, наповнювати бази даних клієнтів, надавати послуги автоматично відповідав на телефонні без участі оператора, проводити контроль зайнятості операторів. Всі ці інтелектуальні послуги здійснюються на сервері під керуванням програмного забезпечення, в сучасних системах це поєднане з CRM. На сервері колл-центру розміщуються додатки, які необхідні для ведення додаткових функцій, наприклад, це система інтерактивної мовної взаємодії, яка дозволяє без участі оператора дати типову інформацію про послуги компанії.

З точки зору організаційної, call-центр влаштований таким чином: це колектив операторів, які ведуть діалог з клієнтами, один або кілька супервайзерів, які стежать за роботою операторів і перерозподіляють навантаження на них, група технічної підтримки та адміністративні служби. Причому у великих організаціях, робота операторів зводиться до надання найнеобхіднішої інформації про компанію і послуги. Для отримання специфічної інформації клієнт перемикається на менеджера.

1.1.1 Обладнання

Найбільш поширений сьогодні на ринку проект для цього сегмента бізнесу - це організація call-центру з використанням IP АТС. Дана система являє клієнтам послуги IP-телефонії на базі програмної АТС, яка обробляє вхідні та вихідні дзвінки. Вона дозволяє маршрутизовати дзвінки, налаштовувати автоматичне інформування клієнтів за типовими питань, надає послуги голосового меню, записи розмов, організації голосових конференцій, прийому і відправки факсів. Є можливість для виділення багатоканальних номерів, підключення стільникових абонентів і DECT-радіотелефонів та інші опції.

Для зберігання даних використовується сервер,для роботи з ПЗ використовується персональний комп'ютер. Якщо необхідно, то купується VoIP-шлюз, GSM-модем і обов'язково комп'ютерні гарнітури для операторів.

Схема побудови типового кол-центру наведена на рис.1.1.

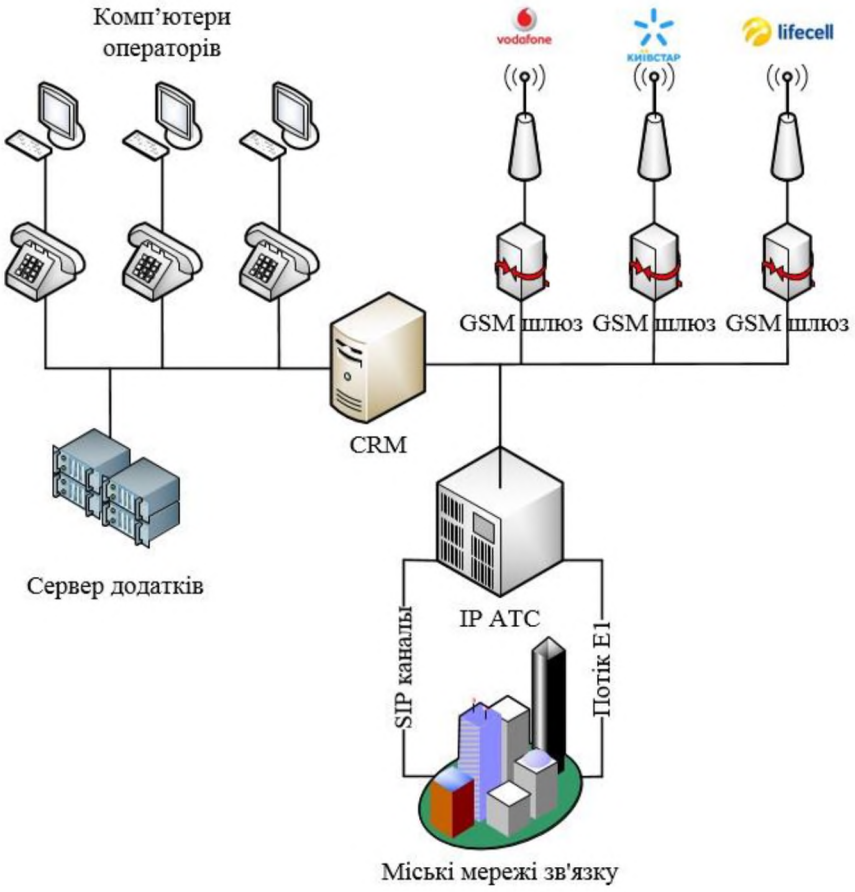


Рисунок 1.1 – Типова схема кол-центру

1.1.2 Програмне забезпечення

Програмне забезпечення контактного центру надає простий та швидкий доступ до звітів, необхідних для покращення роботи працівників та оцінки статистики кол-центру.

На комп'ютерах встановлюється одна з найважливіших частин ПЗ – операційна система

Дуже важлива частина Call-центру - це CRM-система. Вона управляє взаємовідносинами з клієнтами: в ній ведеться статистична звітність, облік контактів, документообіг.

1.1.3 Персонал

У кол-центрі є загальні ролі та посади, включаючи менеджера кол-центру, керівників команд та агентів.

Є також інші посади, такі як директор служби обслуговування споживачів, аналітики з планування ресурсів та аналітики якості, котрі всі відіграють важливу роль у допомозі контактному центру досягти своїх цілей.

Повний перелік типових ролей кол-центру наведено нижче:

- агент колл-центру;
- керівник групи;
- менеджер телефонного центру;
- директор з обслуговування клієнтів;
- аналітик з планування ресурсів;
- аналітик якості;
- керівник кол-центру;
- директор з цифрових контактів;
- операційний менеджер;
- менеджер з персоналу;
- системний адміністратор;
- спеціаліст з безпеки;

– тренер.

Розуміння кожної з цих ролей може стати в нагоді при спробі створити кол-центр або просто для ознайомлення з галуззю.

Однак у багатьох кол-центрах не буде персоналу для кожної з цих ролей. Розмір центру визначатиме наявні посади, а також кількість керівників команд та додаткові посади підтримки.

Типове дерево організації для кол-центру відображено на рис. 1.2.

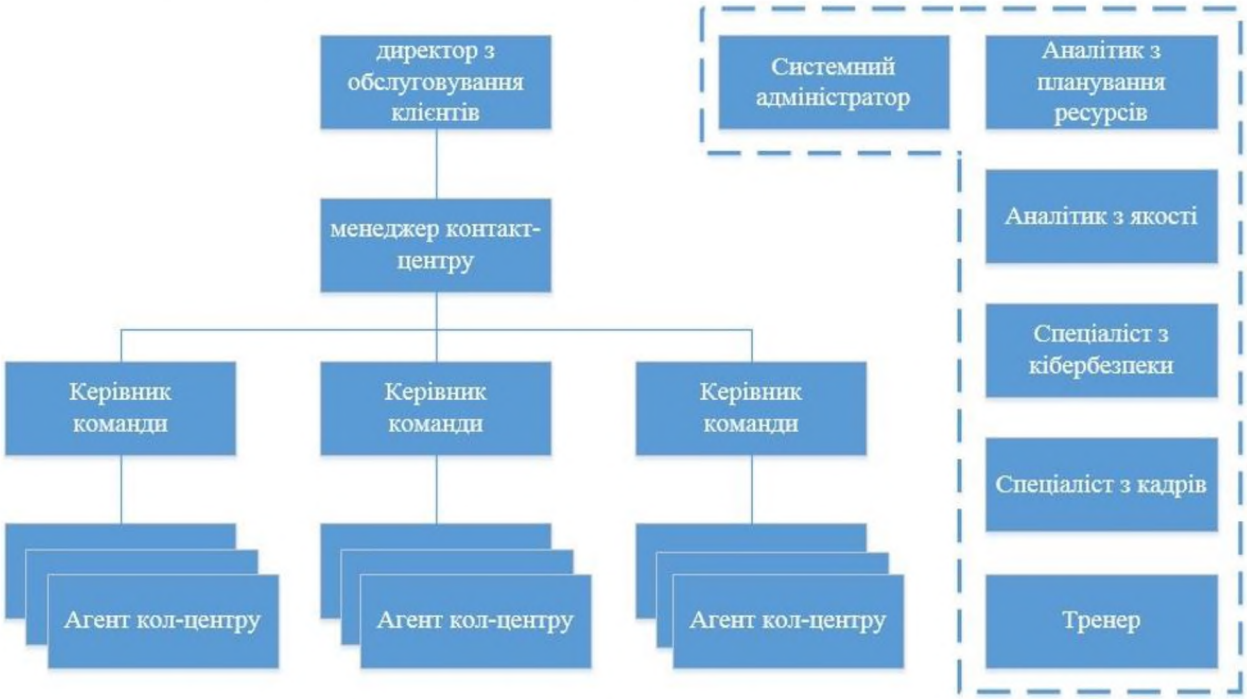


Рисунок 1.2 – типове дерево організації кол-центру

Нижче опис робочих місць для більшості ролей, представлених на цій блок-схемі - з додатковими введеннями завдань для інших ролей кол-центру.

Агент колл-центр.

Мета та обов'язки.

Як правило, від агента кол-центру вирішують запити, коли клієнт телефонує в контактний центр.

Агент може також зв’язатись із клієнтами самостійно, можливо, з метою дослідження споживачів або, можливо, щоб щось їм продати.

Агенти часто спілкуються з клієнтами електронною поштою, у чаті чи повідомленнями.

На додаток до телефонних дзвінків, агенти часто спілкуються з клієнтами електронною поштою, чатом або поштою - або "равликовою поштою", як це часто називають.

Агентів часто називають іншими іменами, включаючи агентів, представників служби обслуговування клієнтів тощо.

Повсякденна діяльність агента кол-центру включає:

- своєчасне та ефективне управління великими обсягами дзвінків;
- визначення потреб клієнтів;
- дослідження проблем клієнтів;
- надання правильних рішень споживачам;
- ведення записів усіх розмов клієнтів у базі даних кол-центру;
- і досягнення цілей щодо якості розмов;
- дотримання сценаріїв спілкування;
- управління соціальними медіа та сторонніми оглядами;
- користуючись можливостями для подальшого продажу для споживачів;
- проведення досліджень замовника;
- відвідування навчальних занять для постійного вдосконалення знань та ефективності.

Керівник команди кол-центру.

Мета та обов'язки.

Керівник команди кол-центру несе відповідальність за управління командою агентів кол-центру. Цифри зазвичай коливаються від восьми до дванадцяти.

Повсякденна діяльність керівника команди кол-центру включає:

- проводити “ранкові зустрічі”, щоб переконатись, що ваша команда знає, якими є цілі на день;

– прослуховування дзвінків та надання відгуку агентам про те, як вони можуть покращитися;

– приймання ескалації дзвінків та перевірка вашої команди, коли агенту може знадобитися допомога;

– постійний тренінг та розвиток вашої команди;

– моніторинг та керування індивідуальними та командними показниками, як правило, на основі ключових показників ефективності (kpi);

– підготовка звітів для вашого керівника лінійних служб про ефективність цих kpi;

– постійна мотивація вашої команди забезпечувати позитивне мислення та орієнтованість на клієнта;

– виявлення та вирішення будь-яких проблем, пов’язаних з людьми, та підтримка членів вашої команди;

– також від керівника команди колл-центру можуть чекати такі обов'язки, як:

– навчання членів команди визначати можливості перехресного продажу та продажу;

– сприяти загальному досвіду споживачів, сприяючи поінформованості про будь-яку ініціативу щодо взаємодії з клієнтами у всій компанії;

– найкраще використовувати ресурс шляхом ефективного планування ресурсів.

Менеджер колл-центру

Мета та обов'язки

Менеджер кол-центру несе відповідальність за управління групою керівників команд, у яких потім команди агентів звітують перед ними.

Повсякденна діяльність менеджера колл-центру включає:

– проведення зустрічей з керівниками команд, щоб переконатися, що цілі дня повідомляються та розуміються;

– проведення коротких зустрічей із керівниками команд для обговорення будь-яких щоденних питань та надання необхідної підтримки;

– постійний тренінг та навчання та розвиток команди;

– спільна функціональна робота з іншими керівниками підрозділів, щоб забезпечити досягнення цілей бізнесу та досягнення результатів;

– моніторинг та ефективність водіння протягом вашої операції та підготовка відповідних звітів для вищого керівництва;

– перетворення короткої, середньої та довгої стратегії бізнесу на цілі, які можна поставити для керівників ваших команд;

– виявлення та вирішення проблем людей, а також відповідальність за дотримання процесів управління персоналом;

– також від менеджера колл-центру можуть чекати взяти на себе такі обов'язки, як:

– залежно від розміру бізнесу та діяльності, менеджер можете приймати ескалаційні дзвінки зі складних запитів клієнтів;

– керування будь-якими сторонніми відносинами;

– нести відповідальність за ефективне планування ресурсів.

Директор з обслуговування клієнтів.

Мета та обов'язки

Директор з обслуговування клієнтів несе відповідальність за визначення стратегії роботи з клієнтами, а потім за створення спільного бачення, щоб забезпечити ефективне здійснення цієї стратегії.

Повсякденна діяльність директора з обслуговування клієнтів включає:

– регулярні зустрічі з командою вищого керівництва, щоб гарантувати, що будь-які майбутні новини, події та зміни будуть попереджені та керовані відповідно до бізнесу;

– володіння функцією обслуговування та моніторинг щоденних, тижневих, щомісячних та річних звітів;

– забезпечення того, щоб усі ваші прямі звіти мали необхідну інформацію та підтримку, щоб мати змогу ефективно виконувати свої ролі;

– постійний тренінг та розвиток вашої структури управління;

– співпрацюючи з іншими сферами бізнесу, взаємодіючи з іншими сферами бізнесу, щоб бути в курсі всього, що може вплинути на рівень обслуговування;

– підготовка звітів до правління про рівні обслуговування та прибутки та збитки функції;

– будучи надихаючим лідером і помітним на всіх рівнях, сприяючи культурі людей та споживачів;

– визначення будь-яких проблем з продуктивністю та потреб у тренуванні.

Також від директора можуть чекати взяти на себе такі обов'язки, як:

– відповідальність за програму «голос клієнта» (voc) та покращення наскрізного досвіду роботи клієнтів шляхом взаємодії з іншими аналогами та впливу на них;

– створення стратегій залучення працівників та розробка метрик;

– досягнення цілей перехресного продажу та продажу, а також їх зміна та адаптація відповідно до вимог бізнесу;

Аналітик з планування ресурсів.

Мета та обов'язки.

Роль аналітика з планування ресурсів у кол-центрі полягає в тому, щоб переконатися, що потрібні люди перебувають у потрібному місці в потрібний час.

Повсякденна діяльність аналітика з планування ресурсів включає:

– виробництво довгострокових та короткострокових прогнозів вимог та обсягів дзвінків;

– складання та оновлення графіків для працівників кол-центру, щоб вони знали, де вони повинні бути і в який час;

– координація діяльності в режимі реального часу для забезпечення належного охоплення агентом;

– підготовка звітів, щоб показати загальну ефективність роботи контакт-центру;

– також аналітик може виконувати такі обов'язки, як:

– управління прямими звітами

– проведення щоденних, тижневих та щомісячних зустрічей з планування з оперативними керівниками;

– постійно інформувати всіх про майбутні плани, виклики чи ризики щодо рівня обслуговування;

– ходьба по підлозі, щоб переконатися, що люди перебувають у потрібному місці і роблять те, що їм задумано.

Аналітик з якості

Мета та обов'язки

Аналітик якості телефонного центру здійснює моніторинг та оцінку якості розмов із клієнтами за всіма каналами контактного центру. Це включає телефонні дзвінки (як вхідні, так і вихідні), електронні листи, розмови в чаті тощо.

Роблячи це, перед якісним аналітиком покладена ширша мета - підтримка радників для поліпшення взаємодії з клієнтами.

Повсякденна діяльність аналітика з якості включатє:

– моніторинг та оцінка роботи агента за набором критеріїв;

– надання відгуку агентам про те, як вони можуть покращитися;

– розробка програм оцінки для агентів;

– розробка метрики для оцінки якості для відстеження індивідуальної та командної діяльності;

– спостереження за тенденціями кол-центру;

– підготовка звітів для керівництва про те, де контактний центр покращився і де він міг би покращитися;

– впровадження тренінгів та тренінгів для агентів.

Також від аналітика можуть чекати такі обов'язки, як:

– проведення аналізу першопричин для виявлення прогалин у знаннях;

– забезпечення зворотного зв'язку із клієнтами та внутрішнього зворотного зв’язку з керівництвом;

– визначення та допомога у впровадженні інструментів, які покращать ефективність роботи радника;

Інші ролі в кол-центрі.

Ось ще декілька, коротших вступів до деяких інших ролей контактного центру, які ми виділили на початку цієї статті.

Керівник кол-центру.

Начальники контактних центрів керують операціями контактних центрів різного розміру. Зазвичай це швидка сфера бізнесу, яка є складною і постійно змінюється.

Очікується, що хтось на цій посаді визначатиме майбутнє роботи контактного центру, щоб покращувати взаємодію з клієнтами через кожен доступний канал.

Як правило, керівник кол-центру підпорядковується директору служби обслуговування клієнтів або керуючому директору і несе відповідальність за результати роботи всіх груп кол-центру.

Однак у ролі є набагато більше, як це зазначено у перелічених нижче обов’язках.

Основні обов'язки включають:

– бюджет / управління збитками;

– прийняття рішень щодо людей, процесів, технологій та майбутнього;

– розробка планів використання нових інструментів та технологій;

– координація роботи команди контакт-центру на всіх рівнях;

– забезпечення дотримання або перевищення kpi;

– нагляд за процесами набору та планування роботи;

– перегляд та чітке визначення всіх ролей контактного центру.

Директор з цифрових контактів

Ця роль головним чином відповідає за використання цифрових каналів та ефективність контактів із клієнтами через цифрові лінії обслуговування.

Крім того, відповідальність директора з цифрових контактів полягає у наданні послуги, яка не загрожує існуючим доходам, послугам та розміру націнки.

Крім того, особа, яка виконує цю роль, повинна керувати створенням / розробкою стратегії цифрового контакту, досліджуючи, пропонуючи та розробляючи правильні цифрові канали, що відповідають іміджу та амбіціям бренду.

Основні обов'язки включають:

– поглиблення розуміння тенденцій та можливостей цифрового ринку, що мають відношення до контакт-центру;

– забезпечення послідовного надання послуг електронною поштою, в інтернеті, в чаті, відео, соціальній та іншій кореспонденції;

– розробка та впровадження способів розвитку різних каналів;

– виявлення та дослідження сторонніх постачальників.

Спеціаліст з кібербезпеки

Спеціаліз з кібербезпеки – це фахівець, який відповідає за провильну роботу інформаційної безпеки.

Основні обов'язки, як правило, включають:

– Адміністрування та підтримка кібербезпеки

– Створення корпоративних політик і процедур

– Підтримка, постійний моніторинг і поліпшення існуючої системи управління інформаційною безпекою та політикою захисту персональних даних.

– Контроль виконання всіх операцій компанії щодо ІБ

– Проведення навчання з IT-безпеки для співробітників

Системний адміністратор

Системний адміністратор – це фахівець, який підтримує правильну роботу комп'ютерної техніки і програмного забезпечення, а також відповідає за інформаційну безпеку організації.

Основні обов'язки, як правило, включають:

– підготовка й збереження резервних копій даних, їх періодична перевірка й знищення;

– встановлення й конфігурування оновлень операційної системи і прикладного програмного забезпечення;

– встановлення й конфігурування нового апаратного й програмного забезпечення;

– створення й підтримка в актуальному стані файлу облікових записів користувачів;

– підтримання інформаційної безпеки в організації;

– документування своєї роботи;

– усунення неполадок у комп'ютерній системі;

– монтаж комп'ютерної техніки та визначення необхідності ремонту;

– участь у проектуванні та монтажі локальної мережі;

– участь у плануванні комп'ютерних систем та придбанні нової комп'ютерної техніки.

Менеджер операцій

Як допоміжну роль у більших центрах, керівник операцій, як правило, буде доглядати за оперативними елементами контактного центру.

Очікується, що людина, яка виконує цю функцію, підтримує зв’язок із керівниками команд та менеджером кол-центру щодо інформації про ефективність роботи, і, як правило, вони є ланкою з IT-відділом або постачальниками технологій.

Отже, менеджер з операцій повинен добре володіти статистикою та мати технічний підхід, спілкуючись із усіма рівнями контактного центру.

Основні обов'язки включають:

- Провідні операції для забезпечення досягнення цілей KPI;
- Планування та реалізація стратегії контактного центру;
- Спільна робота з тренінгами, підбором персоналу та персоналом для планування ресурсних кампаній;
- Розробка постійних удосконалень процесів;
- Підтримка взаємодії з ключовими контактами клієнта;
- Встановлення та перегляд стандартів якості.

Менеджер з персоналу

Повинні бути тісні стосунки між менеджером з персоналу та кол-центром через постійні заходи персоналу, такі як набір та навчання.

Залежно від компанії, у кол-центрі можуть бути кадрові ресурси.

HR відповідають за забезпечення того, щоб умови роботи та посадові інструкції були на місці, а також за організацію набору персоналу.

Зазвичай кадровий персонал відповідає за забезпечення того, щоб умови роботи та посадові інструкції були на місці, а також за організацію набору та, можливо, навчання для кол-центру. Вони також займаються проблемами, які можуть бути у людей особисто чи професійно.

Тренер

Деякі центри мають тренерів як частину загальної команди через великий обсяг вступних та постійних тренувань, які необхідні.

Вони відповідають за підготовку та проведення тренінгів для агентів у центрі.

1.2 Принцип роботи оператора кол-центру

Принцип роботи оператора кол-центру наведено на рис.1.3.

1.3 Інформаційня, яка цикрулює

1. Персональні дані клієнтів
2. Робочі матеріали call -центру.
3. Послуги, що надані клієнту
4. Інформація про послуги

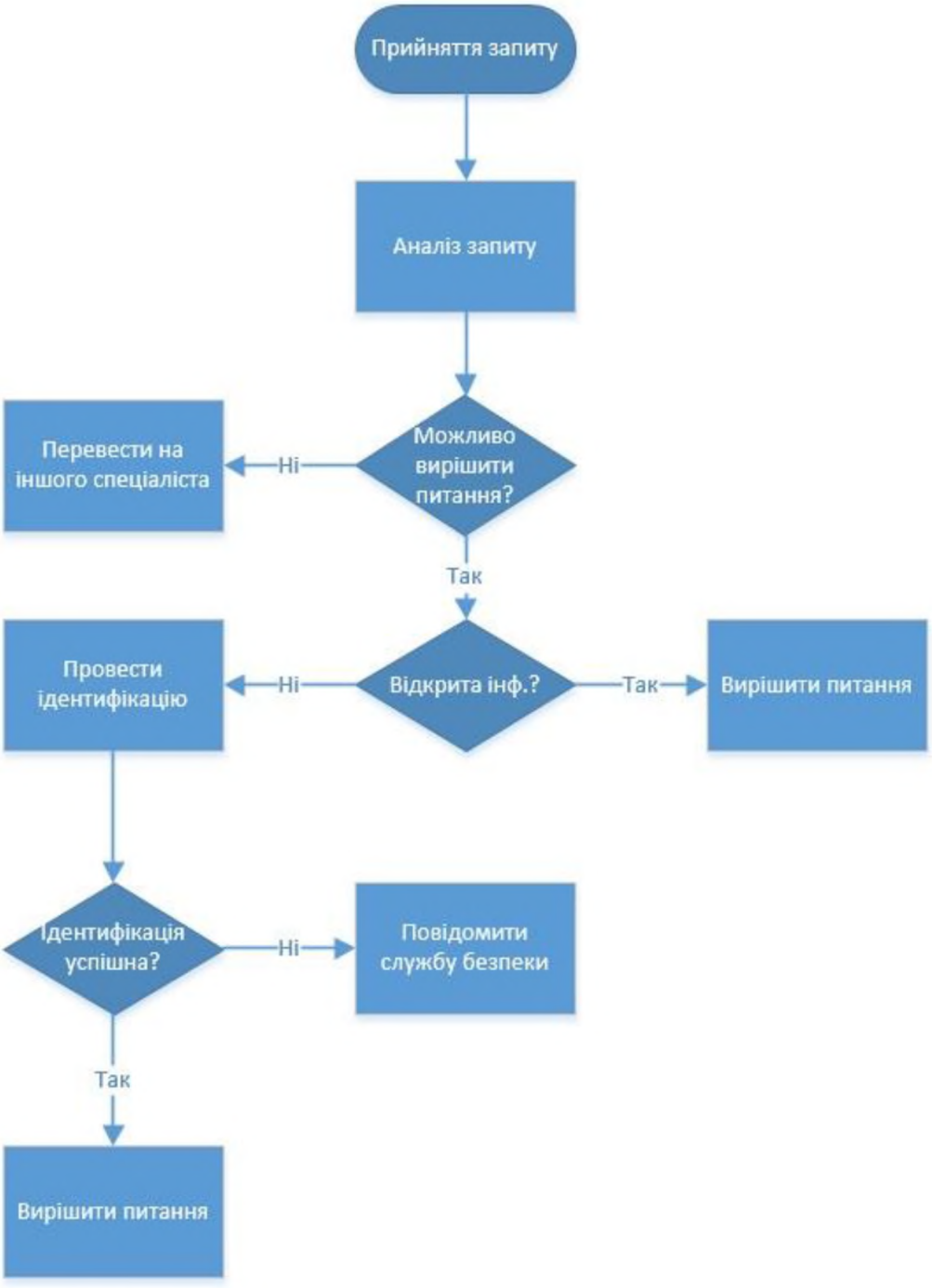


Рисунок 1.3 – Принцип роботи оператора кол-центра

Перелік інформаційних,яка циркулює наданий у табл. 1.1

Таблиця 1.1 – нформаційня, яка цикрулює

Номер (№)	Інформація	Режим доступу	Особи, що використовують інформацію	Вимоги до окремих атрибутів захисту
1	Інформація про послуги	Відкритий доступ	Оператор call-центру	Цілісніть,доступність
2	Персональні дані клієнта	Обмежений доступ	Оператор call -центру	Конфіденційність
3	Робочі матеріали кол-центру		Працівники call -центру	Конфіденційність
4	Послуги, що надані клієнтам		Працівники call -центру	Конфіденційність, цілісність доступність

1.4 Системи контролю оператора кол-центру

Завдання будь-якого call-центру - забезпечити клієнту відповіді на всі запитання. При цьому потрібно дотримати норми ввічливості, такту і при необхідності - ще й індивідуальну корпоративну стилістику бесіди.

Сучасний рівень комп'ютерних програм дозволяє проводити контроль роботи співробітників за комп'ютером точно і прицільно. Їх різноманітність дає можливість роботодавцю підібрати оптимальний за своїми параметрами інструмент контролю і обліку робочого часу і ефективності.

Перелік систем контролю оператора call -центру:

1. SL-IP: система запису IP телефонії

SL-IP забезпечує запис і зберігання всієї мовної та службової інформації в режимі реального часу при переговорах з використанням IP-телефонії (або VoIP - Voice over Internet Protocol)

Функції модуля моніторингу:

– Відтворення і аналіз архівної інформації, синхронне відтворення архівних аудіо- і відео- записів користувачів /, відтворення всього процесу з клієнтом в рамках однієї записи, включаючи IVR-дзвінки, переведення виклику, виклик і конференц-зв'язку.

– Формування вибірок для складання та оцінки циклів взаємодії Клієнт - Співробітник по заданих параметрах: ID клієнта, користувач, група, філія, тривалості дзвінка, день тижня, час.

– Оперативне підключення до прослуховування дзвінка в режимі реального часу, перемикання виклику в режим конференції (підключення до розмови), запис розмови на вимогу.

– Коментування та маркування фонограм для спрощення роботи з накопиченою інформацією.

– Наскрізний пошук фонограм за параметрами виклику.

2. Yaware.TimeTracker

Yaware.TimeTracker - це програмне забезпечення для управління проектами з автоматичною програмою відстеження часу, яка допомагає користувачам управляти своїм часом та підвищувати свою продуктивність. Програмне забезпечення дозволяє користувачам відстежувати час, витрачений на проекти та використання веб-сайтів / програмного забезпечення, керувати ресурсами, аналізувати продуктивність та підвищувати ефективність роботи. Це дозволяє клієнтам відстежувати використання програмного забезпечення та Інтернету, контролювати час роботи та понад нормові роботи, оцінювати та вшановувати досягнення, а також робити знімки та скріншоти.

Особливості:

– автоматичне фіксація часу;

– рахунки, що виставляються та не підлягають оплаті;

– виставлення рахунків;

- база даних співробітників;
- відстеження витрат;
- мобільне відстеження часу;
- багато ставок виставлення рахунків;
- відстеження часу в автономному режимі;
- інтернет-відстеження часу;
- розрахунок понаднормової роботи;
- час на звітність проекту;
- відстеження відпусток / відпусток;

3. Speech-to-text

Google Cloud Speech-to-Text - це послуга, яка дозволяє конвертувати аудіо в текст, застосовуючи моделі нейронних мереж в простому у використанні API, він розпізнає понад 80 мов та варіантів, підтримує глобальну базу користувачів і може транскрибувати текст користувачів продиктувати мікрофон програми, увімкнути командний контроль за допомогою голосу або транскрибувати аудіофайли, серед багатьох інших випадків використання.

Всі функції:

- Глобальна лексика

Підтримує глобальну базу користувачів за допомогою широкої мовної підтримки, понад 125 мов.

- Потокове розпізнавання мови

Дає змогу отримати результати розпізнавання мовлення в режимі реального часу, коли API обробляє аудіовхід, переданий з мікрофона програми або надісланий із попередньо записаного аудіофайлу.

- Мовна адаптація

Налаштовує розпізнавання мови, щоб транскрибувати специфічні для домену терміни та рідкісні слова, надаючи підказки та підвищуючи точність

транскрипції певних слів або фраз. Автоматично перетворює розмовні числа в адреси, роки, валюти та інше за допомогою класів.

– Мовлення в текст On-Prem

Надає повний контроль над своєю інфраструктурою та захищеними мовними даними, одночасно використовує технологію розпізнавання мови Google, яка працює безпосередньо у приватних центрах обробки даних.

– Багатоканальне розпізнавання

Функція перетворення мови в текст може розпізнавати різні канали в багатоканальних ситуаціях (наприклад, відеоконференція) та анотувати транскрипти.

– Міцність шуму

Мова в текст може обробляти шумний звук у багатьох середовищах, не вимагаючи додаткового шумопоглинання.

– Домен-специфічні моделі

Вибір навчених моделей для голосового управління та телефонних дзвінків та транскрипції відео, оптимізованих для вимог до якості для конкретного домену.

– Фільтрування вмісту

Фільтр нецензурної лексики допомагає виявити невідповідний або непрофесійний вміст у аудіоданих та відфільтрувати нецензурні слова в текстових результатах.

– Автоматичне визначення мови (бета-версія)

Вибір до чотирьох мовних кодів, функція перетворення мови в текст визначить правильну мову, якою розмовляють у багатомовних сценаріях.

– Автоматична пунктуація (бета-версія)

Функція точно ставить розділові знаки (наприклад, коми, знаки запитання та крапки).

– Діаризація спікера (бета-версія)

Допомагає дізнатись, хто що сказав, отримуючи автоматичні прогнози щодо того, хто з доповідачів говорив у кожному висловлюванні.

1.5 DLP системи для call-центрів

1.5.1 Методи аналізу даних

DLP-систему використовують, коли необхідно забезпечити захист конфіденційних даних від внутрішніх загроз. І якщо фахівці з інформаційної безпеки в достатній мірі освоїли і застосовують інструменти захисту від зовнішніх порушників, то з внутрішніми справа йде не так гладко.

Використання в структурі інформаційної безпеки DLP-системи передбачає, що ІБ-фахівець розуміє:

– як співробітники компанії можуть організувати витік конфіденційних даних;

– яку інформацію слід захищати від загрози порушення конфіденційності.

Всебічні знання допоможуть фахівцеві краще зрозуміти принципи роботи технології DLP і налаштувати захист від витоків коректним чином.

DLP-система повинна вміти відрізняти конфіденційну інформацію від неконфіденційної. Якщо аналізувати всі дані всередині інформаційної системи організації, виникає проблема надмірного навантаження на IT-ресурси і персонал. DLP працює в основному «в зв'язці» з відповідальним фахівцем, який не тільки «вчить» систему коректно працювати, вносить нові і видаляє неактуальні правила, а й проводить моніторинг поточних, заблокованих або підозрілих подій в інформаційній системі.

Функціональність DLP-системи будується навколо «ядра» - програмного алгоритму, який відповідає за виявлення і категоризацію інформації, яка потребує захисту від витоків. В ядрі більшості DLP-рішень закладені дві технології: лінгвістичного аналізу і технологія, заснована на статистичних методах. Також в ядрі можуть використовуватися менш поширені техніки, наприклад, застосування міток або формальні методи аналізу.

Розробники систем протидії витокам доповнюють унікальний програмний алгоритм системними агентами, механізмами управління інцидентами, парсером, аналізаторами протоколів, перехоплювачами та іншими інструментами.

Ранні DLP-системи базувалися на одному методі в ядрі: або лінгвістичному, або статистичному аналізі. На практиці недоліки двох технологій компенсувалися сильними сторонами один одного, і еволюція DLP привела до створення систем, універсальних у плані «ядра».

Лінгвістичний метод аналізу працює безпосередньо з вмістом файлу і документа. Це дозволяє ігнорувати такі параметри, як ім'я файлу, наявність або відсутність в документі грифа, хто і коли створив документа. Технологія лінгвістичної аналітики включає:

– морфологічний аналіз - пошук по всіх можливих словоформам інформації, яку необхідно захистити від витоку;

– семантичний аналіз - пошук входжень важливою (ключовий) інформації по змісту файлу, вплив входжень на якісні характеристики файлу, оцінка контексту використання.

Лінгвістичний аналіз показує високу якість роботи з великим об'ємом інформації. Для об'ємного тексту DLP-система з алгоритмом лінгвістичного аналізу більш точно вибере коректний клас, віднесе до потрібної категорії і запустить налаштоване правило. Для документів невеликого обсягу краще використовувати методику стоп-слів, яка ефективно зарекомендувала себе в боротьбі зі спамом.

Учитися в системах з лінгвістичним алгоритмом аналізу реалізована на високому рівні. У ранніх DLP-комплексів були складності з завданням категорій і іншими етапами «навчання», проте в сучасних системах закладені налагоджені алгоритми самонавчання: виявлення ознак категорій, можливості самостійно формувати і змінювати правила реагування. Для настройки в інформаційних системах подібних програмних комплексів захисту даних вже не потрібно залучати лінгвістів.

До недоліків лінгвістичного аналізу зараховують прив'язку до конкретної мови, коли не можна використовувати DLP-систему з «англійським» ядром для аналізу українськомовних потоків інформації і навпаки. Інший недолік пов'язаний зі складністю чіткої категоризації з використанням імовірнісного підходу, що утримує точність спрацьовування в межах 95%, тоді як для компанії критичною може виявитися витік будь-якого обсягу конфіденційної інформації.

Статистичні методи аналізу, навпаки, демонструють точність, близьку до 100-відсотковою. Недолік статистичного ядра пов'язаний з алгоритмом самого аналізу.

На першому етапі документ (текст) ділиться на фрагменти прийнятною величини (НЕ посимвольний, але досить, щоб забезпечити точність спрацьовування). З фрагментів знімається хеш (в DLP-системах зустрічається як термін Digital Fingerprint - «цифровий відбиток»). Потім хеш порівнюється з хешем еталонного фрагмента, взятого з документа. При збігу система позначає документ як конфіденційний і діє відповідно до політиками безпеки.

Недолік статистичного методу в тому, що алгоритм не здатний самостійно навчатися, формувати категорії і типізувати. Як наслідок - залежність від компетенцій фахівця і ймовірність завдання хешу такого розміру, при якому аналіз буде давати надмірну кількість помилкових спрацьовувань. Усунути недолік нескладно, якщо дотримуватися рекомендацій розробника з налаштування системи.

З формуванням хешів пов'язаний і інший недолік. У розвинених IT-системах, які генерують великі обсяги даних, база відбитків може досягати такого розміру, що перевірка трафіку на збіги з еталоном серйозно сповільнить роботу всієї інформаційної системи.

Перевага рішень полягає в тому, що результативність статистичного аналізу не залежить від мови та наявності в документі нетекстової інформації. Хеш однаково добре знімається і з англійської фрази, і з зображення, і з відеофрагменту.

Лінгвістичні та статистичні методи не підходять для виявлення даних певного формату для будь-якого документа, наприклад, номери рахунків або паспорта. Для виявлення в масиві інформації подібних типових структур в ядро DLP-системи впроваджують технології аналізу формальних структур.

У якісному DLP-рішення використовуються всі засоби аналізу, які працюють послідовно, доповнюючи один одного.

Засоби аналізу DLP систем наведено у рис. 1.4

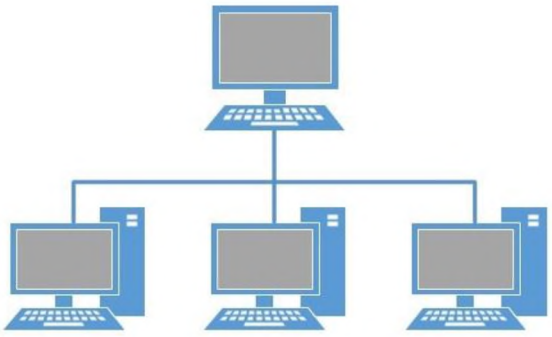
Рисунок 1.4 – засоби аналізу DLP систем

Визначити, які технології присутні в ядрі, можна за описом можливостей конкретного DLP-комплексу.

У таблиці 1.2 представлені рівні контролю.

Не менше значення, ніж функціональність ядра, мають рівні контролю, на яких працює DLP-система. Їх два:

Таблиця 1.2 – Рівні контролю

	• рівень мережі, коли контролюється мережевий трафік в інформаційній системі;

	• рівень хоста, коли контролюється інформація на робочих станціях.

Розробники сучасних DLP-продуктів відмовилися від відокремленої реалізації захисту рівнів, оскільки від витоку потрібно захищати і кінцеві пристрої, і мережу.

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

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

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

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

Принцип поділу технологій в DLP-системах залишився в минулому. Сучасні програмні рішення для запобігання витоків задіють методи, які компенсують недоліки один одного. Завдяки комплексному підходу конфіденційні дані всередині периметра інформаційної безпеки стає більш стійкими до погроз.

1.5.2 Типи DLP систем

Типи DLP систем представлені на рисунку 1.5.

Традиційна класифікація передбачає дві групи DLP-систем:

– активні, здатні блокувати конфіденційну інформацію при виявленні порушень;

– пасивні, здатні тільки «спостерігати» за потоками даних без можливості втрутитися і вплинути на процеси.

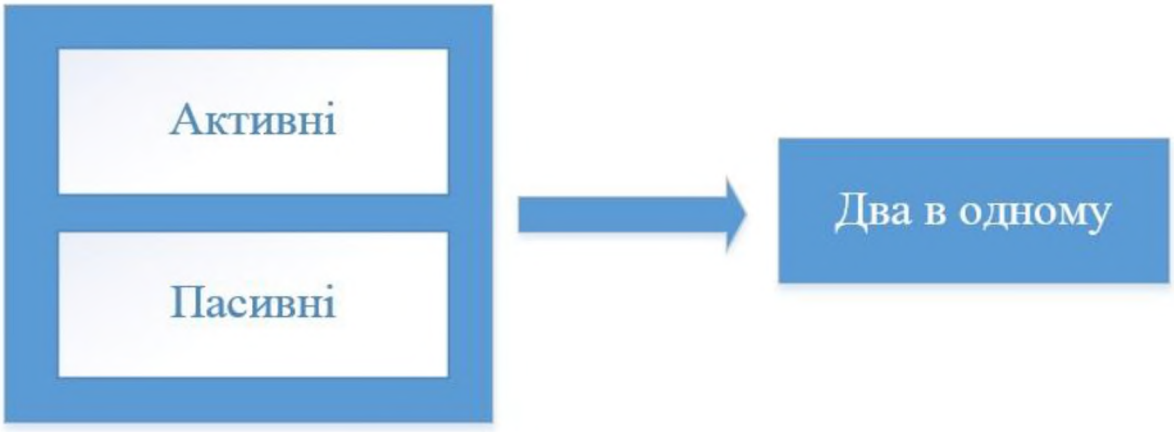


Рисунок 1.5 –Типи DLP систем

Сучасні рішення для запобігання витоків - це комплекси «два в одному», здатні працювати і в активному, і в пасивному режимі.

Поєднання двох режимів в DLP-системі дає перевагу вже на етапі тестування. Впровадження DLP активного типу супроводжується ризиком припинення налагоджених бізнес-процесів через некоректні налаштування або несправність реакції на події. Установка DLP-комплексу в пасивному тестовому режимі дає можливість спокійно переконатися, що правила моніторингу і реакції налаштовані коректно, канали руху інформації - під постійним наглядом, а системи логування та архівування не перевантажувати мережеву інфраструктуру.

Інший критерій класифікації DLP-рішень - за методами архітектурної реалізації.

Методи архітектурної реалізації DLP систем представлені на рисунку 1.6

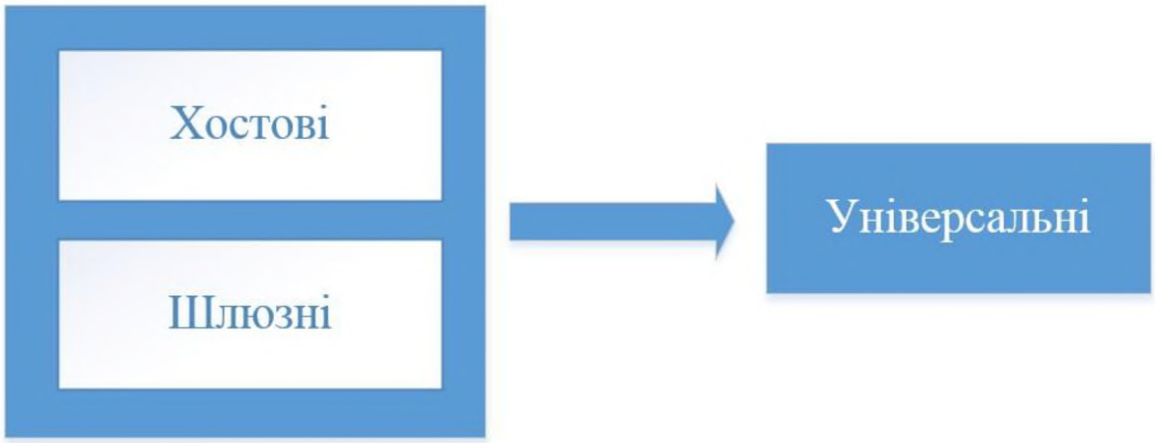


Рисунок 1.6 – Методи архітектурної реалізації DLP

Хостові DLP припускають установку програм-«агентів» на комп'ютери користувачів. Агенти стежать за дотриманням політик безпеки і не дають здійснювати потенційно небезпечні дії, наприклад, запускати ПО зі знімних пристроїв. Одночасно агенти реєструє всі дії користувачів і передають інформацію в єдину базу. Таким чином ІБ-фахівець отримує повне уявлення про те, що відбувається в корпоративній мережі.

Основна перевага хостових рішень полягає в більш повному контролі каналів передачі інформації і дій користувача на робочому місці. Агенти фіксують всі операції за комп'ютером, плюс DLP-рішення нового покоління дозволяють записувати переговори співробітників або, наприклад, підключаються до веб-камері. Недолік хостових систем в тому, що контроль поширюється тільки на пристрої, які підключаються безпосередньо і безпосередньо взаємодіють з робочою станцією.

При виборі хостових DLP-систем слід звернути увагу, яким способом встановлюються агенти на комп'ютери користувачів. Функція віддаленої установки і адміністрування позбавить ІБ-фахівців від необхідності вручну ставити агента на кожну робочу станцію.

Інша важлива вимога до агентських компонентів хостових DLP - прихований режим роботи і захист від видалення. Якщо у користувача є права локального адміністратора і рівень IT-грамотності вище середнього, він потенційно може зупинити роботу агентів і вивести комп'ютер з-під «поля зору» DLP-системи.

Мережеві DLP засновані на застосуванні централізованих серверів, куди перенаправляється копія вхідного і вихідного трафіку для перевірки на відповідність політикам безпеки. Мережеві рішення забезпечують високий рівень захисту від несанкціонованого впливу, так як дозволяють обмежити доступ до виділеного шлюзу і надати права адміністрування вузькому колу співробітників.

Область застосування мережевих DLP-систем обмежена, відповідно, мережевими протоколами і каналами: SMTP, POP3, HTTP (S), IMAP, MAPI, NNTP, ICQ, XMPP, MMP, MSN, SIP, FTP і т.д. Вагомим аргументом на користь мережевого DLP-рішення буде, відповідно, здатність контролювати всі протоколи передачі даних, затребувані в компанії. З точки зору адміністратора безпеки привабливості мережевого DLP-комплексу додасть легкість впровадження і настройки.

Хостової і мережеві DLP-системи контролюють різні канали передачі інформації, і логічним кроком розробників стала інтеграція можливостей різнотипних рішень. Практично всі сучасні інструменти запобігання витоків на ІБ-ринку - універсальні комплекси.

Крім архітектурних слід враховувати також особливості адміністрування DLP-систем. У порівнянні потрібно врахувати алгоритми розгортання компонентів системи, методи розподілу ролей, реалізацію консолі управління. Адміністратору безпеки треба попередньо оцінити інформативність інтерфейсу, складність настройки правил і інші параметри, від яких залежить зручність управління комплексом захисту інформації.

Аналітичні можливості DLP-систем

Визначити, чи відповідає DLP-рішення завданням компанії, допоможуть чотири параметри(наведені у рис. 1.7).

Рисунок 1.7 – Параметри DLP систем

Формування звітності залежить від можливостей DLP-системи не тільки вести моніторинг, а й архівувати перехоплену інформацію. Тіньова копія може включати різні типи даних: веб-трафік; поштові відправлення; активність на принтерах; файли, що записуються на USB-носії; інформацію, що проходить по мережевим протоколам. Тіньове копіювання є ефективним засобом розслідування інцидентів, проте можливість зберігати «резервну копію» закладена не у всіх

DLP-системах. Причина - додаткове навантаження на мережеві ресурси і робочі станції кінцевих користувачів.

1.5.3 DLP системи для call-центру

Cloud DLP

Cloud DLP – це DLP система, яка допомогає класифікувати дані в хмарі та поза нею, надаючи необхідну інформацію для забезпечення належного управління, контролю та відповідності.

Cloud DLP забезпечує доступ до потужної платформи перевірки, класифікації та деідентифікації конфіденційних даних.

– Взаємодія з Cloud DLP через інтерфейс забезпечує багато функцій та переваг API. Наприклад:

– Перевірка сховища Cloud Storage, BigQuery та Cloud Datastore на наявність конфіденційних даних, використовуючи одноразові завдання, або створіть тригер завдання для автоматизації та моніторингу ресурсів за визначеним графіком.

– Виявлення та класифікація загальних типів інформації (детектори типів конфіденційних даних, такі як адреси електронної пошти або номери кредитних карток) або власні типи інформації, які визначаються для захисту внутрішніх ідентифікаторів або секретів компанії.

– Створення шаблонів перевірки даних, щоб повторно використовувати параметри конфігурації для кількох завдань сканування або тригерів роботи.

Cloud DLP включає:

– Понад 120 вбудованих детекторів інформаційного типу (або "infoType").

– Можливість визначати власні детектори infoType за допомогою словників, регулярних виразів та контекстних елементів.

– Методи де-ідентифікації, включаючи редагування, маскування, шифрування, що зберігає формат, зміщення дати тощо.

– Можливість виявлення конфіденційних даних у потоках даних, структурованому тексті, файлах у сховищах сховищ, таких як Cloud Storage та BigQuery, і навіть у зображеннях.

– Аналіз структурованих даних, щоб допомогти зрозуміти ризик їхньої повторної ідентифікації, включаючи обчислення таких показників, як k-анонімність, l-різноманітність тощо.

Всі функції

– Гнучка класифікація

Більше 120 попередньо визначених детекторів з акцентом на якість, швидкість та масштаб. Детектори постійно вдосконалюються та розширюються.

– Проста і потужна редакція

Зніміть ідентифікацію ваших даних: редагуйте, маскуйте, маркуйте та перетворюйте текст і зображення, щоб забезпечити конфіденційність даних.

– Безсерверний

Cloud DLP готовий до роботи, не потрібно керувати обладнанням, віртуальними машинами або масштабувати. Просто надішліть трохи або багато даних і ваги Cloud DLP для вас.

– Детальні висновки

Результати класифікації можна надсилати безпосередньо у BigQuery для детального аналізу або експорту в інші системи. Спеціальні звіти можна легко створювати в Data Studio.

– Безпечна обробка даних

Cloud DLP безпечно обробляє ваші дані та проходить кілька незалежних незалежних перевірок для перевірки безпеки, конфіденційності та безпеки даних.

– Ціни, що платять по мірі

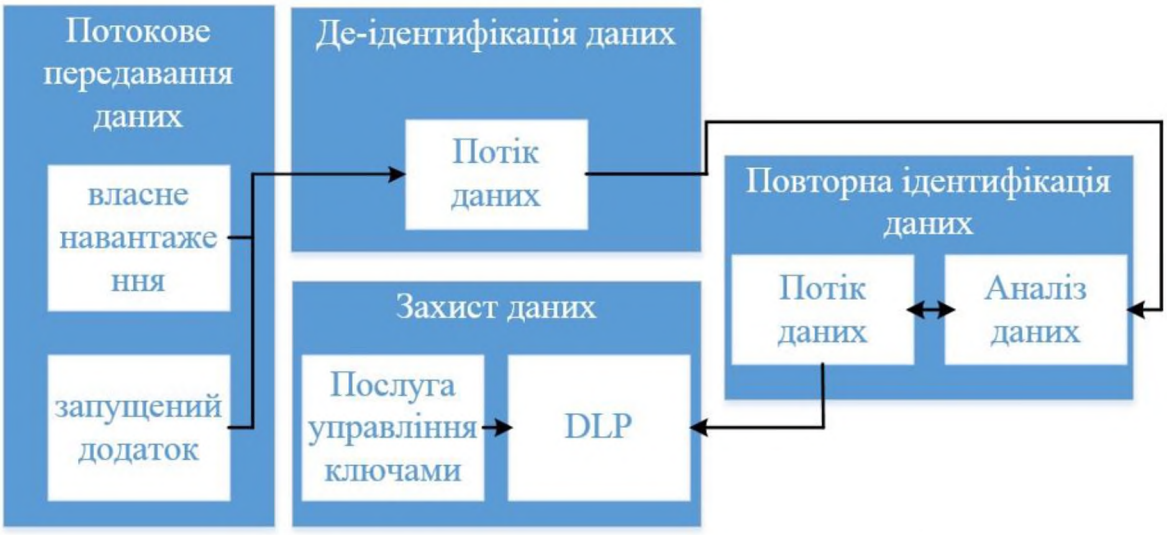


Рисунок 1.8 – Архітектура Google Cloud DLP

Хмарний DLP стягується з урахуванням обсягу оброблених даних, а не на основі підписки або пристрою. Це зручне для споживачів ціноутворення дозволяє платити по ходу, а не заздалегідь до попиту.

– Проста інтеграція робочого навантаження

– Ефективно розгортається Cloud DLP із багаторазовими шаблонами, відстежуйте дані за допомогою періодичного сканування та інтегруйте в безсерверну архітектуру за допомогою сповіщень Pub / Sub.

– Спеціальні правила

Можливість додавати свої власні типи, налаштовувати пороги виявлення та створювати правила виявлення відповідно до потреб та зменшіть рівень шуму.

На рис. 1.8 наведено архітектуру Google Cloud DLP

Forcepoint DLP

Forcepoint DLP – це система, яка захищає організації від витоків інформації та втрати даних по периметру та всередині організації, а також у певній інфраструктурі як сервісні платформи.

– Система включає механізм аналітики, який визначає та класифікує інциденти з високим ризиком. Інциденти, генеровані політикою DLP для всіх

основних компонентів DLP Forcepoint, оцінюються для звітування про тих, у кого найбільший показник ризику втрати даних або крадіжки даних.

– Він може працювати як окремо в мережі, так і бути в парі з Forcepoint Web Security або Forcepoint Email Security, щоб забезпечити всебічне рішення безпеки. Forcepoint DLP Network запобігає втраті даних через електронну пошту та через веб-канали, такі як HTTP, HTTPS та FTP.

– Включає шлюз електронної пошти Forcepoint DLP, який розгортається в Microsoft Azure для забезпечення дотримання політики DLP для Microsoft Exchange Online

– Підтримує сканування вмісту, наданого сторонніми рішеннями, такими як Citrix FileShare, за протоколом ICAP

Кінцева точка Forcepoint DLP запобігає втраті даних через канали кінцевих точок, таких як знімні пристрої зберігання даних, мобільні пристрої, завантаження браузера, поштові клієнти та додатки - наприклад, IM та клієнти спільного використання файлів.

– Він також може виявляти та обробляти конфіденційні дані, що зберігаються на портативних та настільних системах.

– Агент кінцевої точки дозволяє адміністраторам аналізувати вміст у робочому середовищі користувача та блокувати або контролювати порушення політики, як визначено профілями кінцевої точки.

Forcepoint DLP захищає організації від втрати даних шляхом:

– моніторинг даних під час переміщення всередині або поза організацією

– захист даних під час маніпулювання ними в офісних програмах за допомогою елементів керування на основі політик, які відповідають бізнес-процесам

– виявлення та ранжування інцидентів високого ризику для запобігання або запобігання втраті даних та крадіжка даних

Forcepoint DLP має такі основні компоненти:

– Сервер управління - це машина на базі Windows, на якій розміщено програмне забезпечення Forcepoint Security Manager та програмне забезпечення Forcepoint DLP.

Сервер управління забезпечує основну технологію втрати інформації, збір відбитків пальців, застосування політик та зберігання криміналістики. Розгортання може включати кілька серверів DLP Forcepoint для спільного використання навантаження аналізу, але існує лише один сервер управління.

– Механізм політики знаходиться на всіх серверах Forcepoint DLP, серверах шлюзу веб-вмісту та пристроях захисту електронної пошти Forcepoint. Політичні механізми також інтегровані з кінцевими точками Windows, Mac OS X та Linux, на яких запущено Forcepoint DLP Endpoint.

Механізм політики відповідає за аналіз даних та використання аналітики для порівняння їх із правилами у політиках.

– Механізм аналітики розміщений на 64-розрядному комп'ютері Linux.

Він використовується для виявлення потенційно ризикованих інцидентів, ранжування їх за подібною діяльністю та присвоєння оцінки ризику.

– База даних політик є сховищем для політик DLP Forcepoint. Для оптимальної роботи він зберігається локально на кожному сервері (як база даних відбитків пальців).

На рис. 1.9 наведено архітектуру Forcepoint DLP

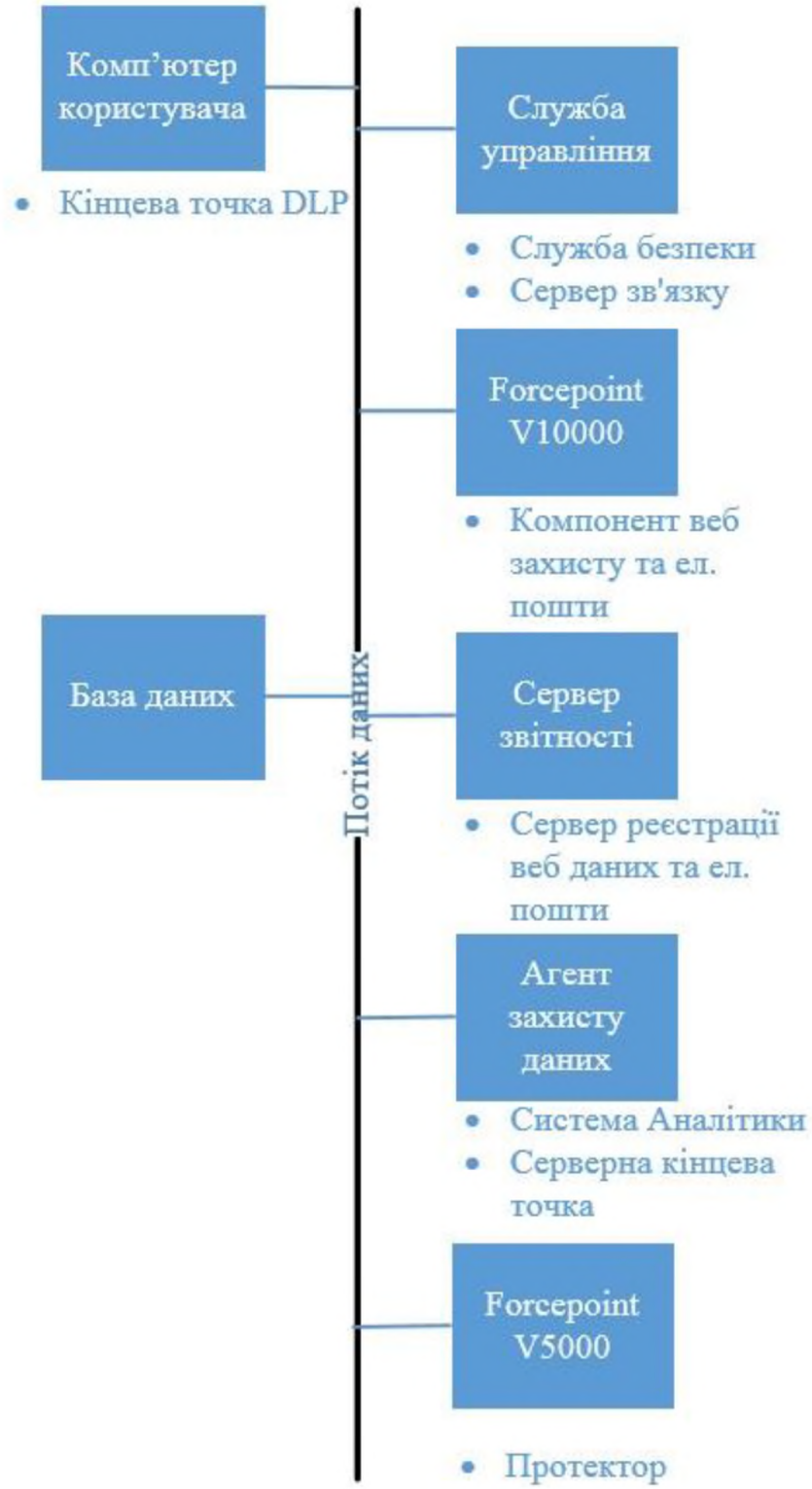


Рисунок 1.9 – Архітектура Forcepoind DLP

1.6 Висновок

Було розглянуто архітектуру call-центру,а саме ключові пункти для побудови і організації роботи, системи контролю оператора call-центру та принципи роботи і архітектуру DLP систем, які можуть буду впроваджені в

систему call-центру для відстеження і запобігання витоку інформації з обмеженим доступом. Але для відстеження інформації, яка циркулює між оператором і клієнтом call-центру цього не достатньо.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Модель загроз

Загрози природного походження

Загрози природного характеру представлені в таблиці 2.1

Таблиця 2.1 – Загрози природного харатеру

Загроза	Джерело загрози	Спосіб реалізації	Наслідки	Спосіб захисту
Стихійне лихо	Зовнішнє середовище	Пожежа, повінь, землетрус, техногенні аварії	Ц, д	Планування відновлювальних робіт

Загрози штучного походження

Загрози штучного походження представлені в таблиці 2.2.

Таблиця 2.2 – Загрози штучного характеру

Загроза	Джерело загрози	Спосіб реалізації	Наслідки	Спосіб захисту
Порушення роботи серверу баз даних	Зловмисник	Виведення з ладу серверу баз даних на рівні операційної системи	Ц, Д	Використання антивірусних комплексів
Порушення роботи серверу баз даних	Зловмисник	Виведення з ладу серверу баз даних на рівні апаратної частини	Ц, Д	Контроль доступу до серверу баз даних
Помилки в ПЗ	Розробник, зловмисник	Помилки в програмному забезпечені системи ІБ	К, Ц, Д	Використання ліцензованого ПЗ
Імітація	Персонал, зловмисник	Неправомірне отримання персональних даних клієнтів з подальшим маскуванням під дійсного клієнта	К, Ц, Д	Ідентифікація та перевірка справжності користувача
Погана навчанність	Персонал	Помилкові дії персоналу	К, Ц, Д	Покращення методів навчання та контролю
Пошкодження	Зловмисник, персонал	Виведення з ладу інформаційно-телекомунікаційної системи	Д	Планування відновлювальних робіт та фізичних захист
Знищення інформації	Персонал, зловмисник	Знищення носіїв інформації	Ц, Д	Контроль доступу до носіїв інформації

Продовження таблиці 2.2

Загроза	Джерело загрози	Спосіб реалізації	Наслідки	Спосіб захисту
Старіння	Носій інформації	Старіння носіїв інформації и засобів обробки інформації	Ц, Д	Періодичне оновлення апаратна частини ІС
Підміна	Персонал	Підміна інформації за допомогою ПЗ	Ц	Розмежування та контроль доступу до ПЗ
Знищення ПЗ	Персонал, зловмисник	Знищення ПЗ	Ц, Д	Розмежування та контроль доступу до ПЗ

2.2 Модель порушника

Модель внутрішнього порушника

Модель внутрішнього порушника представлена в таблиці 2.3.

Таблица 2.3 – Модель внутрішнього порушника

Порушник	Мета порушника	Рівень можливостей	Порушення	Наслідки порушення
Системний адміністратор	Корисливий інтерес	Конфігурація ПЗ, фізичний доступ до носіїв інформації	Знищення носіїв інформації	Д, Ц
Системний адміністратор	Корисливий інтерес	Конфігурація ПЗ, фізичний доступ до носіїв інформації	Модифікація ПЗ	К, Ц, Д
Системний адміністратор	Корисливий інтерес	Конфігурація ПЗ, фізичний доступ до носіїв інформації	Крадіжка інформації або носія інформації	К, Ц, Д
Спеціаліст з кібербезпеки	Завдання збитків	Кофігурація комплексів засобів захисту	Порушення нормальної роботи комплексу засобів захисту	Д
Спеціаліст з кібербезпеки	Недбалість	Кофігурація комплексів засобів захисту	Помилки при конфігурації/ адмініструванні систем/політик безпеки	К, Ц, Д
Користувач ІС	Корисливий інтерес	Запуск фіксованого набору програм	Порушення політики ІБ	К, Ц, Д
Користувач ІС (оператор call-	Корисливий інтерес	Запуск фіксованого наб	Крадіжка інформації	К, Ц, Д

Продовження таблиці 2.3

центру)		набору програм		
Порушник	Мета порушника	Рівень можливостей	Порушення	Наслідки порушення
Користувач ІС (оператор call-центру)	Завдання збитків	Запуск фіксованого набору програм	Модифікація Інформації клієнта	Ц
Користувач ІС (оператор call-центру)	Завдання збитків	Запуск фіксованого набору програм	Знищення інформації	Ц,Д

Модель зовнішнього порушника

Модель зовнішнього порушника представлена в таблиці 2.4.

Таблиця 2.4 – Модель зовнішнього порушника

№	Порушник	Мета порушника	Рівень знань про ІС	Спосіб здійснення порушення	Наслідки порушення
1.	Зловмисник	Отримання необхідної інформації	Базові знання про методи захисту ІС	Маскування під зареєстрованого користувача	К
2.	Зловмисник	Завдання збитків	Базові знання про систему електро-живлення ІС	Порушення нормальної роботи електроживлення технічних засобів	Д
3.	Клієнт	Корисливий інтерес	Базові знання про методи захисту ІС	Порушення клієнтами умов використання ІС	Ц

2.3 Профіль захищеності

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

КД-2 – базова довірча конфіденційність;

КО-1 – повторне використання об'єктів;

КВ-1 – мінімальна конфіденційність при обміні;

ЦД-1 – мінімальна довірча цілісність;

ЦО-1 – обмежений відкат;

ЦВ-1 – мінімальна цілісність при обміні;

ДР-1 – квоти;

ДВ-1 – ручне відновлення;

НР-2 – захищений журнал;

НИ-2 – одиночна ідентифікація і автентифікація;

НК-1 – однонаправлений достовірний канал;

НО-2 – розподіл обов'язків адміністраторів;

НЦ-2 – КЗЗ з гарантованою цілісністю;

НТ-2 – самотестування при старті;

НВ-1 – автентифікація вузла.

1.Критерії конфіденційності

1.1 Довірча конфіденційність

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

КД-2 – базова довірча конфіденційність

Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта

КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процесс

Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту

НЕОБХІДНІ УМОВИ: НИ-1

Найбільше розповсюдження отримав механізм, коли у вигляді атрибутів доступу використовуються мітки, що визначають рівень конфіденційності інформації (об'єкта) і рівень допуску користувача. Таким чином КЗЗ на підставі порівняння міток об'єкта і користувача може визначити, чи є користувач, що здійснює запит на доступ до інформації, авторизованим користувачем.

Реалізується за допомогою Active Directory операційної системи Windows.

1.2 Повторне використання об’єктів

КО-1. Повторне використання об'єктів

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною

Після того як об'єкт (напр. виділена область оперативної пам’яті, де зберігалися тимчасові файли під час роботи з текстовим документом) виділяється процесу або користувачеві, то інформація в об'єкті від

попереднього процесу неповинна містити інформацію від процесу попереднього користувача.

Повторне використання об'єкта може бути реалізовано також шляхом шифрування інформації, що міститься в об'єктах, і використання керування криптографічними ключами замість знищення інформації.

1.3 Конфіденційність при обміні

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

КВ-1. Мінімальна конфіденційність при обміні

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності

КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається

НЕОБХІДНІ УМОВИ: НО-1

Послуга реалізується за допомогою служби криптографії операційної системи Windows.

2. Критерії цілісності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

2.1 Довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування

ЦД-1. Мінімальна довірча цілісність

Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту

НЕОБХІДНІ УМОВИ: НИ-1

Послуга реалізується за механізмів служби криптографії та Active Directory операційної системи Windows.

2.2 Відкат

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

ЦО-1. Обмежений відкат

Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу

НЕОБХІДНІ УМОВИ: НИ-1

Послуга реалізується за допомогою функції “Відновлення системи” операційної системи Microsoft Windows 10 Pro.

2.3 Цілісність при обміні

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

ЦВ-1: Мінімальна цілісність при обміні

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається

НЕОБХІДНІ УМОВИ: НЕМАЄ

Послуга реалізується за допомогою механізмів служби криптографії операційної системи Windows.

3. Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

3.1 Використання ресурсів

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

ДР-1. Квоти

Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься

Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження

НЕОБХІДНІ УМОВИ: НО-1

Реалізується за допомогою Active Directory операційної системи Windows

3.2 Відновлення після збоїв

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

ДВ-1. Ручне відновлення

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС

Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження

Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування

НЕОБХІДНІ УМОВИ: НО-1

Реалізується за допомогою Windows Task Manager операційної системи Microsoft

4. Критерії спостереженості

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям спостереженості, КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача

4.1 Реєстрація

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

НР-2. Захищений журнал

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються

КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації

НЕОБХІДНІ УМОВИ: НИ-1, НО-1

Реалізується за допомогою служби журналів подій операційної системи Microsoft Windows

4.2 Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ран жируються залежно від числа задіяних механізмів автентифікації.

НИ-2. Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування

НЕОБХІДНІ УМОВИ: НК-1

Реалізується за допомогою компоненту Winlogon операційної системи Microsoft.

4.3 Достовірний канал

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

НК-1. Однонаправлений достовірний канал

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем

НЕОБХІДНІ УМОВИ: НЕМАЄ

Реалізується за допомогою компоненту Winlogon операційної системи Microsoft

4.4 Розподіл обов'язків

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

НО-2. Розподіл обов'язків адміністраторів

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі

НЕОБХІДНІ УМОВИ: НИ-1

Реалізується за допомогою функції створення ролей DLP системи Forcepoint DLP.

4.5 Цілісність комплексу засобів захисту

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

НЦ-2. КЗЗ з гарантованою цілісністю

Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів

КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ

НЕОБХІДНІ УМОВИ: НЕМАЄ

Реалізується забороною завантаження операційної системи з сторонніх носіїв. Таким чином всі можливі запити до захищених об’єктів (запис, модифікування, видалення) контролюються комплексом засобів захисту.

4.6 Самотестування

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

НТ-2. Самотестування при старті

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ

НЕОБХІДНІ УМОВИ: НО-1

Реалізується за допомогою Процедура POST операційної системи Windows.

4.7 Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість

ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ран жируються на підставі повноти реалізації.

НВ-1: Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму

Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації

НЕОБХІДНІ УМОВИ: НЕМАЄ

Реалізується за допомогою вбудованої аутентифікації Windows .

2.4 Політики безпеки

Навчання ІБ

Всі співробітники call-центру повинні проходити періодичну підготовку в області політики і процедур ІБ, прийнятих в організації.

Використання ресурсів локальної мережі

Для виконання своїх службових обов'язків кожен співробітник забезпечується доступом до відповідних інформаційних ресурсів. Інформаційними ресурсами є каталоги і файли, що зберігаються на дисках серверів організації, бази даних, електронної пошти.

Основними робочими каталогами є особисті каталоги співробітників і каталоги підрозділів, створені відповідно до особливостей їх роботи. Доступ співробітників до ресурсів мережі здійснюється відповідно до матриці доступу. Тимчасове розширення прав доступу здійснюється відділом ІС СМТ Установи відповідно до Порядку надання (Зміни) повноважень користувача.

Політика використання інформаційних ресурсів

Загальні обов’язки користувача ПЗ call-центру :

– При роботі з ПЗ керуватися нормативною документацією (керівництво користувача).

– Звертатися до спеціалістів, назначених відповідальними за системне адміністрування та інформаційну безпеку по всіх технічних питаннях щодо роботи в корпоративній ІС, а також за необхідною консультацією з питань застосування технічних і програмних середовищ корпоративної ІС.

– Мінімізувати вивід на печатку оброблюваної інформації.

Обробка конфіденційної інформації

При обробці конфіденційної інформації співробітник call-центру зобов'язаний:

– знати і виконувати вимоги по роботі з конфіденційною інформацією;

– розташовувати екран монітора таким чином, щоб виключити перегляд конфіденційної інформації сторонніми людьми;

– обов'язково перевіряти адресу одержувача електронної пошти на правильність набору;

– не запускати виконувані файли на зовнішніх накопичувачах, отриманих від неперевіреного джерела;

– не передавати конфіденційну інформації по відкритим каналам зв'язку, крім мереж корпоративної інформаційної системи.

Використання ПЗ

На АРМ call-центру допускається використання тільки ліцензійного програмного забезпечення, затвердженого в переліку дозволеного програмного забезпечення.

Користувачі АРМ не мають права видаляти, змінювати, доповнювати, оновлювати програмну конфігурацію на АРМ call-центру. Зазначені роботи, а так само роботи по установці, реєстрації та активації придбаного ліцензійного ПЗ можуть бути виконані тільки системним адміністратором.

Використання електронної пошти

Електронна пошта використовується для обміну в рамках ІС call-центру та загальнодоступних мереж інформацією у вигляді повідомлень і документів в електронному вигляді.

При роботі з корпоративною електронною поштою call-центру користувач повинен враховувати:

– електронна пошта не являє собою засіб, який гарантовано доставляє відправлене повідомлення до адресата;

– електронна пошта не є засобом передачі інформації, який гарантує;

– електронна пошта не є засобом передачі інформації, яка гарантовано ідентифікує відправника повідомлення;

– електронна пошта призначена виключно для використання у службових цілях;

– будь-які повідомлення корпоративної електронна пошти можуть бути прочитані, використані в інтересах організації або видалені уповноваженими співробітниками організації;

– для забезпечення функціонування електронної пошти допускається застосування ПЗ, що входить до реєстру дозволеного до використання ПЗ.

Робота в мережі

Доступ до мережі Інтернет надається співробітникам call-центру з метою виконання ними своїх службових обов'язків, що вимагають безпосереднього підключення до зовнішніх інформаційних ресурсів.

Для доступу співробітників Установи до мережі Інтернет допускається застосування ПЗ, що входить до реєстру дозволеного до використання ПЗ.

При використанні мережі Інтернет необхідно:

– дотримуватися вимог цієї політики;

– використовувати мережу Інтернет виключно для виконання своїх службових обов'язків;

– при використанні мережі Інтернет заборонено:

– використовувати наданий організацією доступ в мережу Інтернет в особистих цілях;

– використовувати несанкціоновані апаратні і програмні засоби, що дозволяють отримати несанкціонований доступ до мережі Інтернет;

– Опублікувати, завантажувати і поширювати матеріали, які містять:

1. Конфіденційну інформацію
2. Службову таємницю
3. Шкідливе ПЗ

Політика роботи оператора call-центру з клієнтом

При роботі оператор call-центру повинен:

– приймати вхідні дзвінки;

– робити вихідних інформаційні дзвінки;

– надавати клієнтам інформацію;

– проводити ідентифікацію клієнта, якщо клієнт запитує конфіденційну інформацію;

– реєструвати дані в ІС;

– виконувати вимоги політики обробки конфіденційної інформації;

– виконувати вимоги політики використання інформаційних ресурсів;

– виконувати вимоги політики використання електронної пошти;

– виконувати вимоги політики використання ПЗ;

– виконувати вимоги політики використання ресурсів локальної мережі;

Політика відповідальності оператора

Оператор call-центру несе відповідальність:

– За невиконання (неналежне виконання) своїх посадових обов'язків, передбачених цією посадовою інструкцією, в межах, визначених чинним законодавством України.

– За вчинені в процесі здійснення своєї діяльності правопорушення, - в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.

– За завдання матеріальної шкоди - в межах, визначених чинним цивільним законодавством та законодавством України.

– Оператор call-центру має право:

– запитувати і отримувати необхідні матеріали і документи, що відносяться до питань своєї діяльності;

– своєї компетенції повідомляти керівництву підприємства про всі недоліки обговоренні питань, що стосуються виконання його обов'язків;

– знайомитися з проектами рішень керівництва підприємства, що стосуються діяльності Підрозділи;

– Вносити на розгляд керівництва пропозиції щодо вдосконалення роботи, пов'язаної з передбаченими цією інструкцією;

– доповідати керівництву підприємства про всі виявлені порушення і недоліки в зв'язку з виконуваної роботою.

Політика роботи спеціаліста з кібербезпеки

При роботі спеціаліст з кібербезпеки повинен:

– адмініструвати та підтримувати кібербезпеку;

– створювати корпоративні політики і процедури;

– кідтримувати,проводити постійний моніторинг і поліпшення існуючої системи управління інформаційною безпекою та політикою захисту персональних даних;

– контролювати виконання всіх операцій компанії щодо ІБ;

– кроводити навчання з ІТ-безпеки для співробітників;

Політика відповідальності спеціаліста з кібербезпеки

– Спеціаліст з кібербезпеки несе відповідальність:

– За невиконання (неналежне виконання) своїх посадових обов'язків, передбачених цією посадовою інструкцією, в межах, визначених чинним законодавством України.

– За вчинені в процесі здійснення своєї діяльності правопорушення, - в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.

– За завдання матеріальної шкоди - в межах, визначених чинним цивільним законодавством та законодавством України.

Управління інцидентами інформаційної безпеки

В Установі повинна бути розроблена і затверджена формальна процедура повідомлення про події в області ІБ, а також процедура реагування на такі події, що включає в себе дії, які повинні виконуватися під час вступу повідомлень про подію.

Всі співробітники повинні бути ознайомлені з процедурою повідомлення, а в їх обов'язки повинна входити максимально швидка передача інформації про події.

На додаток до повідомлення про події ІБ і недоліки безпеки повинен використовуватися моніторинг систем, повідомлень і вразливостей для виявлення інцидентів ІБ.

Цілі управління інцидентами ІБ повинні бути узгоджені з керівництвом для обліку пріоритетів Установи при поводженні з інцидентами.

Необхідно створити механізми, що дозволяють оцінювати і відслідковувати типи інцидентів, їх масштаб і пов'язані з ними витрати.

2.5 Архітектура системи

На рисунку 1.1 зображено архітектуру системи до впровадження методики.

На рисунку 2.1 зображено архітектуру системи після впровадження методики.

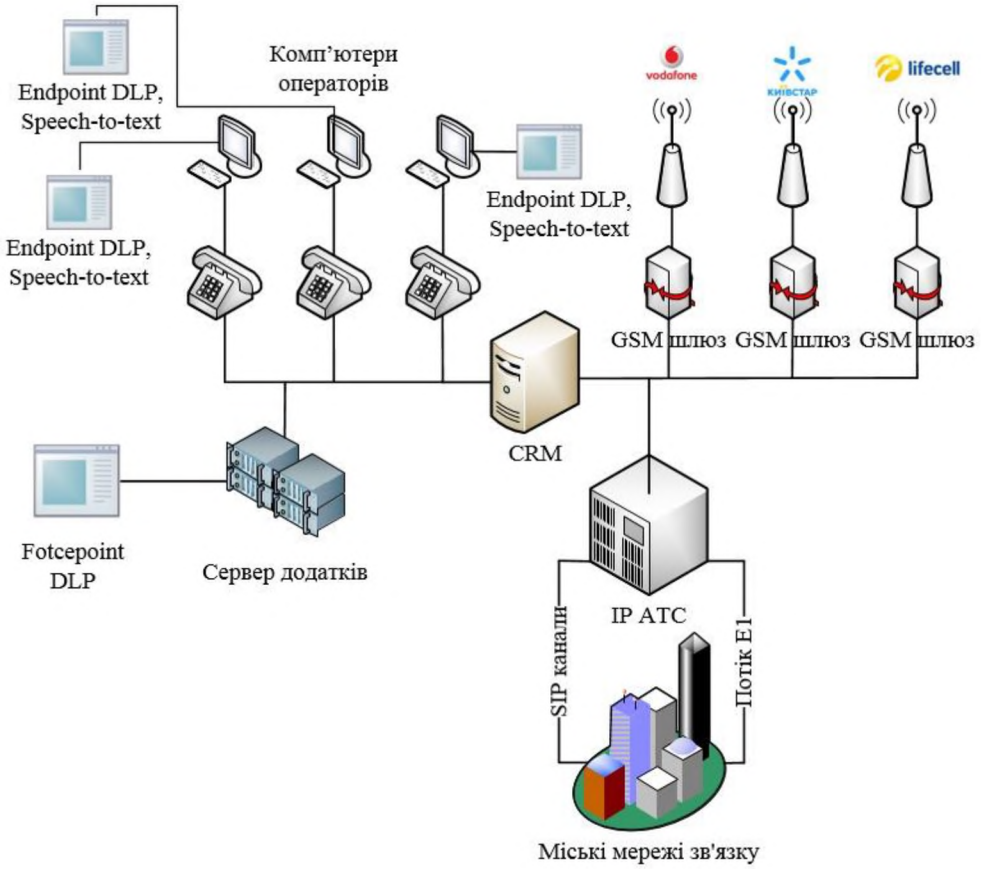


Рисунок 2.1 – Архітектура системи після впровадження методики

2.6 Конфігурація системи

Перед початком роботи Forcepoint DLP треба пройти два етапи:

1. Підготовчий етап
2. Етап налаштування

Етап налаштування включає:

1. Створення політики
2. Створення класифікаторів інформації
3. Визначення ресурсів
4. Створення політики виявлення
5. Створення ролей

2.6.1 Підготовчий етап

Підготовчий етап наведений в ДОДАТКУ Б

2.6.2 Етап налаштування

2.6.2.1 Щоб створити власну політику DLP у модулі захисту даних диспетчера Forcepoint Security:

1. Перейти на сторінку Головне> Керування політикою> Політики DLP.
2. Натиснути Створити власну політику.

Відкриється загальна сторінка майстра спеціальної політики.

3. Заповнити кожну сторінку майстра, а потім натиснути кнопку Далі.

Щоб отримати докладні вказівки щодо будь-якої сторінки,потрібно натиснути Довідка> Пояснити цю сторінку.

4. Переглянувши інформацію на кінцевій сторінці майстра, натиснути кнопку Готово.

За допомогою вкладки Загальне майстра настроюваної політики визначити назву та опис політики, вибрати одного або кількох власників політики та визначити, чи слід надавати правилу на основі політики те саме ім’я, що й сама політика:

1. Ввести унікальну назву політики .
2. Вказати, чи ввімкнено правило для цієї політики. Якщо цей параметр не вибрано, правило присутнє, але не використовується.
3. Ввести Опис політики.
4. Щоб визначити одного або кількох власників для цієї політики:

a. Натиснути Редагувати.

b. Вибрати одного або кількох власників, як описано у Вибір елементів для включення або виключення в політику.

c. Натиснути OK.

5. Кожна політика має одне або кілька правил. Коли це правило буде створено, правило буде автоматично додано на основі властивостей, встановлених у майстрі. Вказати, як назвати правило, пов’язане з цією політикою:

– Вибрати Використовувати назву політики для назви правила, щоб надати правилу для цієї політики таку саму назву, що і політика.

6. Натиснути «Далі», а потім перейти до майстра спеціальних політик для визначення логіки

Щоб визначити логіку правила:

1. За допомогою спадного вікна поруч із Монітори цього правила вибрати один із наступних параметрів:

– Щоб застосувати правило щодо будь-якого вмісту без аналізу, вибрати Усі дії. Це може призвести до великої кількості інцидентів.

– Щоб відстежувати один або декілька конкретних класифікаторів, вибрати «Конкретні дані», а потім у спадному списку вкажіть, коли запускати інциденти.

Вибрати усі частини транзакції в цілому, щоб викликати інцидент, якщо сума всіх збігів у транзакції перевищує налаштований поріг. Наприклад, якщо порогове значення дорівнює 3, тоді транзакція з 2 збігами в тілі повідомлення та одним збігом у рядку теми викликає інцидент.

Вибрати кожну частину транзакції окремо, щоб викликати інцидент

спрацьовує лише тоді, коли поріг досягнуто в якійсь одній частині

транзакція. Наприклад, у тілі повинні бути 3 сірники або

3 у рядку теми або іншій частині повідомлення для ініціювання інциденту.

2. Натиснути Додати, а потім за допомогою розкривного списку:

– Вибрати Шаблони та фрази, щоб додати регулярний вираз, ключову фразу, сценарій або класифікатор словника.

– Вибрати Властивості файлу, щоб додати до файлу назву, тип або класифікатор розміру файлу.

– Вибрати «Відбиток пальця», щоб додати до умови класифікатор відбитків пальців файлу або бази даних.

– Вибрати машинне навчання, щоб додати до стану класифікатор машинного навчання. Машинне навчання дозволяє адміністраторам наводити приклади даних, які слід захистити, щоб система могла вчитися у них та визначати предмети подібного характеру.

– Вибрати розмір транзакції, щоб виявляти транзакції вказаного розміру або більше.

– Визначити кількість вкладень електронної пошти (лише транзакції електронної пошти), щоб виявляти повідомлення електронної пошти з певною кількістю вкладень або більше.

– Визначити кількість адрес електронної пошти (лише транзакції електронною поштою), щоб виявляти повідомлення, надіслані на вказану кількість доменів або більше.

Щоб видалити умову з правила,потрібно вибрати умову та натисніть Видалити.

Щоб відредагувати поріг умови (кількість збігів, що викликають інцидент), потрібно натиснути гіперпосилання у стовпці Властивості.

У класифікаторах словників ваги фраз словника враховуються при визначенні, чи досягнуто порогового значення.

На вкладці Загальне у вікні Вибір класифікатора вмісту перелічені доступні класифікатори вмісту. Сортування або фільтрування стовпців для пошуку конкретних класифікаторів.

Для пошуку класифікатора потрібно ввести ключовий термін (наприклад, «кредитна картка») і натиснути лупу, щоб знайти відповідний класифікатор вмісту. Необов'язково включати символи підстановки, такі як „кредит *”.

Натиснути Створити, щоб додати до правила один або кілька нових класифікаторів вмісту. Адміністратори можуть додати стільки, скільки потрібно. Вибрати з наступних типів класифікаторів:

– Регулярний вираз - це рядок, який використовується для опису або відповідності набору рядків відповідно до певних правил синтаксису. Коли сканований текст транзакції сканується, система використовує регулярні вирази, щоб знайти в тексті рядки, що відповідають шаблонам конфіденційної інформації.

– Ключова фраза - це точне ключове слово або фраза (наприклад, "цілком таємно" або "Конфіденційна"), яка може бути знайдена у вмісті,

призначеному для зовнішнього одержувача, і, можливо, вказує на розповсюдження секретної інформації. Система може заблокувати розповсюдження цієї інформації.

– Словник - це контейнер для слів та виразів, що належать одній мові. Багато словників вбудовано в DLP Forcepoint, включаючи списки медичних станів, фінансових умов, юридичних умов та умов кредитних карток. Ви також можете створити або налаштувати список словників, а потім використовувати його у своїх політиках. Кожному терміну в словнику може бути присвоєна вага, тому, коли один термін виявляється, до порогового значення відводиться більше балів, ніж коли виявляється інший термін.

2.6.2.2 Створення класифікатора вмісту

Створення регулярного виразу для Visa

Використати сторінку "Шаблони та фрази> Властивості регулярного виразу" в модулі захисту даних диспетчера Forcepoint Security, щоб створити класифікатор шаблону або з нуля, або на основі існуючого класифікатора.

Щоб створити візерунок з нуля:

1. Перейти на сторінку Класифікатори вмісту> Шаблони та фрази.
2. За допомогою панелі інструментів у верхній частині панелі вмісту вибрати Нове> Регулярний вираз.
3. Ввести ім'я для виразу – “Visa”.
4. Ввести опис цього шаблону –“Регулярний вираз для Visa”
5. Використати поле Значення, щоб ввести регулярний вираз – “\b(4\d{3}[\-\\]\d{4}[\-\\]\d{4} [\-\\]\d{4})\b”
6. Натиснути OK.

Створення регулярного виразу для Mastercard

Використати сторінку "Шаблони та фрази> Властивості регулярного виразу" в модулі захисту даних диспетчера Forcepoint Security, щоб створити класифікатор шаблону або з нуля, або на основі існуючого класифікатора.

Щоб створити візерунок з нуля:

1. Перейти на сторінку Класифікатори вмісту> Шаблони та фрази.
2. За допомогою панелі інструментів у верхній частині панелі вмісту вибрати Нове> Регулярний вираз.
3. Ввести ім'я для виразу – “Mastercard”.
4. Ввести опис цього шаблону –“ Регулярний вираз для Mastercard”.
5. Використати поле Значення, щоб ввести регулярний вираз – “\b(([51-55]\d{3}[\-\\]\d{4}[\-\\]\d{4} [\-\\]\d{4})\b”.
6. Натиснути OK.

Створення регулярного виразу для електронної пошти

Використати сторінку "Шаблони та фрази> Властивості регулярного виразу" в модулі захисту даних диспетчера Forcepoint Security, щоб створити класифікатор шаблону або з нуля, або на основі існуючого класифікатора.

Щоб створити візерунок з нуля:

1. Перейти на сторінку Класифікатори вмісту> Шаблони та фрази.
2. За допомогою панелі інструментів у верхній частині панелі вмісту вибрати Нове> Регулярний вираз.
3. Ввести ім'я для виразу – “Електронна пошта”.
4. Ввести опис цього шаблону –“ Регулярний вираз для електронної пошти”.
5. Використати поле Значення, щоб ввести регулярний вираз – “\b[a-zA-Z1-9\-\._]+@[a-z1-9]+(.[a-z1-9]+){1,}\b”.
6. Натиснути OK.

Створення регулярного виразу для ПІБ

Використати сторінку "Шаблони та фрази> Властивості регулярного виразу" в модулі захисту даних диспетчера Forcepoint Security, щоб створити класифікатор шаблону або з нуля, або на основі існуючого класифікатора.

Щоб створити візерунок з нуля:

1. Перейти на сторінку Класифікатори вмісту> Шаблони та фрази.

2. За допомогою панелі інструментів у верхній частині панелі вмісту вибрати Нове> Регулярний вираз.

3. Ввести ім'я для виразу – “ПІБ”.

4. Ввести опис цього шаблону –“ Регулярний вираз для ПІБ”.

5. Використати поле Значення, щоб ввести регулярний вираз – “\b([А-ЯЁ][а-яё]+[\-\s]?){3,}\b”.

6. Натиснути OK.

Створення регулярного виразу для номеру мобільного телефона

Використати сторінку "Шаблони та фрази> Властивості регулярного виразу" в модулі захисту даних диспетчера Forcepoint Security, щоб створити класифікатор шаблону або з нуля, або на основі існуючого класифікатора.

Щоб створити візерунок з нуля:

1. Перейти на сторінку Класифікатори вмісту> Шаблони та фрази.

2. За допомогою панелі інструментів у верхній частині панелі вмісту вибрати Нове> Регулярний вираз.

3. Ввести ім'я для виразу – “Номер мобільного телефона”.

4. Ввести опис цього шаблону –“ Регулярний вираз для номера мобільного телефона”.

5. Використати поле Значення, щоб ввести регулярний вираз – “\b\+?\d+([\(\s\-]?\d+[\)\s\-]?[\d\s\-]+)?\b”

6. Натиснути OK.

Створення регулярного виразу для серії та номера паспорта

Використати сторінку "Шаблони та фрази> Властивості регулярного виразу" в модулі захисту даних диспетчера Forcepoint Security, щоб створити класифікатор шаблону або з нуля, або на основі існуючого класифікатора.

Щоб створити візерунок з нуля:

1. Перейти на сторінку Класифікатори вмісту> Шаблони та фрази.

2. За допомогою панелі інструментів у верхній частині панелі вмісту вибрати Нове> Регулярний вираз.

3. Ввести ім'я для виразу – “ Серія та номера паспорта ”.

4. Ввести опис цього шаблону –“ Регулярний вираз для серії та номера паспорта ”.

5. Використати поле Значення, щоб ввести регулярний вираз – “ \b^[А-ГҐДЕЄЖЗИІЇЙК-Я]{2}\d{6}\b ”

6. Натиснути OK.

Створення ключового виразу

Для створення або редагування класифікатора ключових фраз потрібно використати сторінку Шаблони та фрази> Властивості ключових фраз у модулі Захист даних менеджера безпеки Forcepoint.

Наявність ключового слова або фрази (наприклад, "цілком секретно" або "Проект X") у вмісті, призначеному для зовнішнього одержувача, може свідчити про те, що секретна інформація просочується. Forcepoint DLP дозволяє блокувати розповсюдження цієї інформації, визначаючи класифікатор ключових фраз.

Щоб отримати доступ до сторінки Властивості ключових фраз:

– Щоб створити нову ключову фразу,потрібно натиснути кнопку Нова> Ключова фраза на панелі інструментів сторінки "Шаблони та фрази".

Щоб визначити ключову фразу:

1. Ввести назву класифікатора ключових фраз.

2. Ввести опис цієї ключової фрази.

3. Ввести ключове слово або фразу – “Картка”, “Номер картки”, “Паспорт”, “Серія та номер паспорта”, “Адреса проживання”…

4. Натиснути OK.

Машинне навчання

Класифікатори машинного навчання - це вдосконалений інструмент, який дозволяє адміністраторам наводити приклади типу даних для захисту та не для захисту. Це дозволяє Forcepoint DLP навчитися ідентифікувати конфіденційні дані в трафіку.

– Приклади того, що захищати, називаються позитивними навчальними наборами.

– Приклади того, що не слід захищати, називаються негативними тренувальними наборами.

Ці приклади разом виховують систему.

На відміну від відбитків пальців, файли не повинні містити частини фактичних файлів для захисту, але натомість вони можуть виглядати подібними або охоплювати подібну тему. Система вивчає та розпізнає складні моделі та взаємозв'язки та приймає рішення без точного включення / виключення критеріїв, зазначених у класифікаторах відбитків пальців. Машинне навчання може навіть таким чином захистити нові документи нульового дня.

Оскільки класифікатори машинного навчання не шукають точного збігу, вони можуть обробляти більшу кількість файлів, ніж класифікатори відбитків пальців.

Використати сторінку Скановані папки майстра машинного навчання, щоб визначити документи, які будуть скановані та використані для пошуку подібних документів або частин документів у майбутньому.

1. У розділі Позитивні приклади визначти Шлях до папки, яка містить приклади типу текстових даних, які ви потрібно захистити, щоб система могла вчитися на них та визначати подібні дані в трафіку.

Наприклад, для захисту власного вихідного коду, написаного на Java, вказати шлях до розташування власного вихідного коду.

– Для досягнення найкращих результатів у цій папці має бути принаймні 50 прикладів.

2. За допомогою спадного списку Тип вмісту виберати тип, який найкраще описує вміст, який потрібно захистити. Це має відповідати типу вмісту в папці позитивних прикладів.

3. У розділі Негативні приклади встановити прапорець, щоб вказати, чи доступні негативні приклади.

4. У розділі Усі документи встановити прапорець, якщо немає спеціальної папки з негативними документами. Потім визначити Шлях до папки, що містить усі типи документів у мережі та трафік кінцевих точок, і система визначить хороші негативні приклади.

– Папка може містити як позитивні, так і негативні приклади.

– Система порівнює позитивні приклади з документами в цій папці та вирішує, які файли представляють негативні приклади.

– Виберати цей параметр і навести негативні приклади для покращення швидкості та точності класифікатора.

5. Натиснвти Далі, щоб продовжити.

Створення правила з класифікатора вмісту

Використати Створити правило для класифікатора вмісту, щоб створити правило з обраного класифікатора.

1. Щоб отримати доступ до цієї сторінки:
2. Перейти на сторінку Класифікатори вмісту.
3. Вибрати підтримуваний тип класифікатора.
4. Вибрати класифікатор зі списку.
5. натиснути Створити правило з класифікатора на панелі інструментів у верхній частині області вмісту.

Якщо ця опція не відображається,потрібно натиснути Інші дії, а потім вибрати Створити правило з класифікатора.

На сторінці Створення правила для класифікатора вмісту вгорі сторінки відображається назва вибраного класифікатора вмісту та тип політики (шаблон, ключова фраза тощо). Цю інформацію не можна редагувати.

Заповніть поля на сторінці наступним чином:

1. Ввести нову назву правила – “Правило виявлення для call-центру”.
2. Вибрати Додати це правило до існуючої політики, а потім вибрати назву політики
3. Натиснути OK, щоб зберегти зміни.

2.6.2.3 Визначення ресурсів

У політиці адміністратори можуть визначати:

– Джерела даних та пункти призначення

– Пристрій кінцевої точки або програма, яка може використовуватися

– Виправні дії, які слід вжити при виявленні порушення (наприклад, заблокувати або повідомити)

У Forcepoint DLP вони сукупно називаються ресурсами.

Додавання користувацьких комп'ютерів

Скористайтеся сторінкою Головне> Управління політикою> Ресурси> Спеціальні комп'ютери в модулі захисту даних диспетчера безпеки Forcepoint, щоб переглянути та налаштувати список локальних комп'ютерів, які є можливими джерелами або напрямками інформації у вашій організації, крім комп'ютерів у каталог користувача.

Щоб додати новий комп'ютер до системи,потрібно натиснути Створити, а потім:

1. Ввести IP-адресу або ім'я хосту для комп'ютера.
2. Ввести повне доменне ім'я для комп'ютера.
3. Ввести опис цього комп'ютера.
4. Натиснути OK.

Додатки кінцевих точок

Forcepoint надає довгий перелік вбудованих програм, які можна вибрати для моніторингу в кінцевій точці під час налаштування політики щодо кінцевих точок.

Скористайтеся сторінкою Головне> Управління політикою> Ресурси> Кінцеві програми, щоб переглянути вбудовані програми та визначити власні програми.

Щоб додати програму, натисніть Створити> Програма або Створити> Хмарне додаток на панелі інструментів у верхній частині сторінки, а потім:

1. Ввести ім'я для цієї програми, наприклад, Microsoft Word.

2. У полі Ініціював:

– Для настільних програм Windows ввести ім'я виконуваного файлу (наприклад, winword.exe).

– Для програм Mac або Windows Store ввести назву програми (наприклад, Microsoft.SkypeApp * для програми Windows Store Camera).

– Для хмарних додатків ввести URL-адресу.

4. Ввести Опис для цієї програми.

5. Щоб пов’язати програму з існуючою групою програм,потрібно позначити Належить до, а потім вибирати групу, що цікавить.

6. Якщо примусове виконання програми не потрібне,потрібно позначити Довірену програму. Довіреним програмам дозволяється записувати будь-який тип інформації на знімний носій інформації, наприклад, на USB-накопичувач. Їм також дозволено копіювати будь-який тип даних на віддалений спільний диск у мережі.

7. У розділі «Захоплення екрану» за допомогою розкривного списку «Дія» вибрати дію, яку потрібно виконати, коли кінцеві користувачі намагаються захопити екрани з цієї програми. (Копіювання / вирізання, доступ до файлів, вставка, завантаження)

Знімки екрану не аналізуються на вміст. Вони заблоковані та перевірені, дозволені та перевірені або дозволені, як зазначено тут.

6. Натиснути OK.

Імпорт додатків

Вибравши Головне> Ресурси> Програми> Нова програма / Інтернет-програма.

Коли додаються програми за допомогою цього екрана, вони ідентифікуються за назвою виконуваного файлу. Іноді користувачі намагаються обійти спостереження, змінюючи ім'я виконуваного файлу. Наприклад, якщо відстежується "winword.exe" на пристроях кінцевих точок користувачів, вони

можуть змінити ім'я виконуваного файлу на "win-word.exe", щоб уникнути моніторингу.

Додавання власних груп додатків

Використати Керування політикою> Ресурси> Групи додатків кінцевої точки> Група програм або сторінка Групи хмарних додатків, щоб визначити групи програм, яких немає у списку, визначеному Forcepoint. Щоб отримати доступ до цієї сторінки, натиснути Створити на панелі інструментів у верхній частині області вмісту на сторінці Групи програм кінцевої точки.

– Спеціальна група програм може містити заздалегідь визначені та / або власні програми кінцевої точки.

– До програм належать локально встановлені програмні пакети, такі як Microsoft Word та Excel, а також спеціальні програми.

– Хмарні програми - це програми, доступ до яких здійснюється через Інтернет.

Щоб налаштувати спеціальну групу програм:

1. Вести ім'я для групи програм, наприклад Desktop Publishing.
2. Вести Опис групи заявок.
3. У полі Учасники натиснути Редагувати, щоб вибрати програми для включення до цієї групи.
4. У розділі Операції з кінцевими точками вибрати операції, які повинні ініціювати аналіз вмісту для програм цієї групи.

Оскільки знімки екрану не аналізуються на вміст, налаштуйте параметри захоплення екрана для окремих програм кінцевих точок (не груп програм).

5. Натиснути OK.

Додавання плану дій

Скористайтися сторінкою «Управління політикою»> «Ресурси»> «Плани дій»> «Інформація про план дій», щоб створити план дій.

Щоб отримати доступ до цієї сторінки, потрібно визначити одну з таких дій:

– Натиснути Створити на панелі інструментів у верхній частині області вмісту на сторінці Плани дій.

– Натиснути назву плану дій у списку на сторінці Плани дій.

Щоб створити план дій:

1. Ввести Ім'я та Опис для плану дій.

Додавання нового сценарію виправлення

Використати сторінку Керування політикою> Ресурси> Сценарії виправлення> Деталі сценарію виправлення, щоб визначити нову кінцеву точку, управління інцидентами або сценарій політики.

– Щоб отримати доступ до цієї сторінки, потрібно натиснути кнопку Створити на сторінці Ресурси> Сценарії виправлення, а потім вибрати тип сценарію.

Щоб додати сценарій виправлення:

1. Ввести назву цього сценарію виправлення.

2. Ввести опис цього сценарію.

3. Сторінка містить вкладку для кожної операційної системи, що підтримується для вибраного типу сценарію. Вкладок може бути до 3: Windows, Linux та Mac. Визначити сценарій для кожної доступної операційної системи. Коли виявляється порушення в кінцевій точці, система знає, яку версію запускати.

Використовуйте сторінку Керування політикою> Ресурси> Плани дій у модулі Захист даних у диспетчері Forcepoint Security, щоб визначити, як система реагує на виявлення різних порушень.

Наступні плани дій надаються за замовчуванням.

1. Перевірити та повідомити

Аудируйте випадки з усіх каналів, і якщо вони налаштовані, генеруйте сповіщення.

2. Лише аудит

(За замовчуванням) Дозволити всі дії на всіх каналах та реєструвати випадки в журналі аудиту. Якщо налаштовано, він також генерує сповіщення. Цей план дій розроблений для легких порушень.

3. Аудит без криміналістики

Те саме, що лише аудит, але не зберігає криміналістичних даних щодо події.

4. Заблокувати все

Блокуйте всі випадки на всіх каналах, перевіряйте їх і, якщо це налаштовано, генеруйте сповіщення. Цей план дій розроблений для серйозних порушень.

5. Блок без криміналістики

Те саме, що і "Блокувати всі", але не зберігає криміналістичних даних щодо інциденту.

6. Відкинути вкладення електронної пошти

Видаліть вкладення електронної пошти, що порушують політику.

Додавання або редагування плану дій

Скористатися сторінкою «Управління політикою»> «Ресурси»> «Плани дій»> «Інформація про план дій», щоб створити або змінити план дій.

Щоб отримати доступ до цієї сторінки,потрібно виконати одну з таких дій:

– Натиснути Створити на панелі інструментів у верхній частині області вмісту на сторінці Плани дій.

– Натиснути назву плану дій у списку на сторінці Плани дій.

Щоб створити або відредагувати план дій:

1. Ввести або оновіть Ім'я та Опис для плану дій.

2.Вибрати дії

Сценарії виправлення

Сценарії виправлення розширюють функціональність виявлення та запобігання втраті даних.

Сценарій виправлення - це виконуваний файл, який запускається механізмом політики або агентом кінцевої точки, коли спрацьовує інцидент.

Сценарій виправлення вважається ресурсом. Налаштуйте сценарії виправлення на сторінці Ресурси> Сценарії виправлення в модулі захисту даних диспетчера безпеки Forcepoint. Використовуйте цю сторінку для ідентифікації та управління зовнішніми сценаріями, які запускаються, коли виявляються різні порушення.

Види сценаріїв виправлення

Існує 3 типи сценаріїв виправлення:

– Сценарій кінцевої точки запускається автоматично, коли ініціюються інциденти з кінцевими точками. Оскільки сценарій виконується на пристрої кінцевої точки, він повинен мати мінімальні вимоги до процесора та дискового простору. Крім того, сценарій не повинен передбачати, що кінцевий комп'ютер є частиною мережі, і він повинен бути меншим ніж 5 МБ.

– Сценарій управління аваріями працює на інцидентах, вибраних у звіті про інциденти. Щоб активувати цей сценарій:

1. Відкрити інцидент на сторінці Головна> Звітування> Запобігання втраті даних> Інциденти.

2. Натиснути «Виправити»> «Запустити сценарій виправлення» на панелі інструментів у верхній частині області вмісту.

3. Вибрати скрипт для запуску.

Сценарій можна використовувати для автоматизації таких завдань, як відкриття справи CRM. Він не виконується автоматично.

– Сценарій політики запускається автоматично, коли спрацьовують випадки запобігання втраті даних та виявлення. Наприклад, сценарій може зашифрувати дані, виявлені при виявленні порушень, або виконати дію в системі DRM. Оскільки сценарій пов'язаний із мережевим сервером, він може бути більшим і вимогливішим до ресурсів центрального процесора, а також може використовувати інші інструменти в мережі.

Додавання нового сценарію виправлення

Використати Керування політикою> Ресурси> Сценарії виправлення> Сторінка подробиць сценарію виправлення, щоб визначити нову кінцеву точку, управління інцидентами або сценарій політики.

– Щоб отримати доступ до цієї сторінки, потрібно натиснути Створити на сторінці Ресурси> Сценарії виправлення, а потім вибрати тип сценарію.

Щоб додати сценарій виправлення:

1. Ввести назву цього сценарію виправлення.
2. Ввести опис цього сценарію.
3. Сторінка містить вкладку для кожної операційної системи, що підтримується для вибраного типу сценарію. Вкладок може бути до 3: Windows, Linux та Mac.

Визначте сценарій для кожної доступної операційної системи. Коли виявляється порушення в кінцевій точці, система знає, яку версію запускати.

Заповніть поля на кожній вкладці наступним чином:

- виконуваний файл

Перейти до виконуваного файлу, який потрібно запустити, коли виявлено певний інцидент.

- Аргументи (за бажанням)

За бажанням Ввести будь-які аргументи, які ви потрібно включити в команду. Якщо аргументи укладено у лапки, розділіть аргументи пробілом. Наприклад:

“-E” “-o”

- Додаткові файли

Якщо для сценарію потрібні додаткові файли, такі як файл ресурсу або інші скрипти, які він викликає, натиснути Додаткові файли, а потім перейти до zip-файлу, що містить додаткові файли для запуску.

4. Натиснути OK. Рядок виконання показує хід кожного файлу під час завантаження. Є можливість будь-коли скасувати процес. Коли завантаження завершиться, нова зовнішня команда з’явиться на панелі деталей.

Параметри виявлення даних Forcepoint

На вкладці Відкриття:

1. Щоб система запустила сценарій виправлення для випадків виявлення мережі, вибрати Запустити сценарій виправлення, а потім вибрати сценарій зі спадного списку.

2. У розділі "Розпізнавання кінцевої точки", якщо для розгортання ввімкнено класифікаційне позначення, позначте Додати класифікаційний тег, щоб вказати тег або теги, які застосовуватимуться до файлів.

– Теги додаватимуться лише до файлів, які відповідають умовам, встановленим на сторінці Налаштування> Загальне> Послуги> Класифікація.

– Класифікаційне позначення повинно бути ввімкнене, щоб ця опція відображалася у плані дій.

3. Якщо в плані дій увімкнено класифікаційне позначення, ввести до двох пар Мітка тегу та Значення.

Кожна мітка та значення повинні вже існувати в системі класифікації тегів, щоб Forcepoint Data Discovery міг додати тег до файлів.

4. Щоб система запустила сценарій виправлення кінцевої точки для випадків виявлення кінцевої точки, вибрати Запустити сценарій виправлення кінцевої точки, а потім вибрати сценарій зі спадного списку.

Сценарії виправлення можна додати на сторінку Головне> Управління політикою> Ресурси> Сценарії виправлення. Вибрати Створити> Сценарій кінцевої точки.

5. Натиснути OK, щоб зберегти зміни.

2.6.2.4 Створення політики виявлення

Створити нові політики на сторінці Головне> Управління політиками> Політики виявлення> Керування політиками виявлення в модулі захисту даних диспетчера безпеки Forcepoint.

1. Натиснути Додати на панелі інструментів у верхній частині області вмісту, а потім виберати Заздалегідь визначену політику або Спеціальну політику.

2. З'явиться майстер. Параметри у майстрі різні, залежно від вибраного типу політики.

Спеціальні політики

У майстрі спеціальних політик:

1. На вкладці Загальні ввести унікальне ім’я політики та Опис політики.

2. Позначити Увімкнено, щоб активувати політику.

3. За замовчуванням жоден власник політики не включається до політики. Щоб визначити власників політики, натиснути Редагувати, а потім:

a. Вибрати тип облікових записів для відображення (адміністратор з кібербезпеки).

b. Вибрати обліковий запис зі списку ліворуч, а потім натиснути стрілку вправо, щоб перемістити його до вибраного списку. Облікові записи в цьому списку вважаються власниками політик і отримують повідомлення про них у разі порушення політики.

c. Натиснути ОК.

4. Вказати, що слід використовувати ім'я політики для імені правила.

5. Натиснути Далі.

6. На вкладці Умова вказати, чи контролює це правило конкретні дані чи всі дії та чи відстежуються дані у всіх частинах транзакції в цілому або в кожній частині транзакції окремо.

7. Натиснути Додати, щоб додати класифікатор вмісту або атрибут до умови, яку потрібно створити:

– Шаблони та фрази: “Visa”, “Mastercard”, “Електронна пошта”, “Номер мобільного телефона”, “ПІБ”, “Серія та номер паспорта”… і натиснути кнопку ОК.

– Властивості файлу: виберати властивості файлу, які потрібно додати до цієї політики. Натиснути ОК.

8. Вибрати відповідь на запитання: Коли запускати правило?

– Усі умови відповідають

– Принаймні одна умова відповідає

– Користувацькі умови

Вибравши користувацькі умови,потрібно використати параметри праворуч, щоб заповнити опис стану.

9. Натиснути «Далі», щоб визначити ступінь серйозності та дії щодо інцидентів, які відповідають цьому правилу, та вказати план дій, який слід вжити. Натиснути Додатково, щоб додатково вказати ступінь тяжкості відповідно до кількості відповідних умов.

10. Натиснути Далі, щоб завершити роботу майстра.

11. Натиснути Готово, щоб створити нове правило та додати його до політики.

2.6.2.5 Створення ролей

Додавання ролі адміністратораа з безпеки

Щоб визначити нову роль:

1. Перейти на сторінку Налаштування> Авторизація> Ролі в модулі Захист даних Менеджера безпеки.

2. Натиснути Створити на панелі інструментів у верхній частині області вмісту.

3. Ввести ім’я нової ролі – “Адміністратор з безпеки”.

4. Ввести Опис ролі.

У розділі "Дозволи" вибрати наступне:

– Вибрати «Налаштований», щоб визначити охоплення цієї ролі, а потім продовжити користувацькі права доступу:

1. У розділі Статус вибрати звіти про стан, до яких ця роль повинна мати доступ:

– на інформаційній панелі відображаються системні сповіщення, статистика та підсумок подій за останні 24 години.

– екран "Здоров'я системи" дозволяє контролювати продуктивність серверів і захисників Forcepoint DLP.

– на екрані стану кінцевої точки узагальнено результати тестів підключення кінцевих точок.

2. У розділі „Звітування” Вибрати функції „Запобігання втраті даних та мобільні події” та функції звітування, до яких ця роль повинна мати доступ.

– Вибрати Детальні звіти, щоб надати адміністраторам із цією роллю доступ до детальних звітів про запобігання втраті даних.

– Вибрати звіти про рейтинг ризиків інцидентів, щоб дозволити адміністраторам із цією роллю отримувати доступ до рейтингу ризиків інцидентів та звітів про випадки.

3. Вибрати інцидент Discovery та функції звітування для цієї ролі.

– Детальні звіти - Вибрати цей параметр, щоб надати адміністраторам із цією роллю доступ до звітів про деталі виявлення.

4. Позначити Надіслати сповіщення електронною поштою, якщо адміністратори з цією роллю повинні отримувати сповіщення про призначення інциденту.

5. У розділі Керування політикою Вибрати функції управління політикою, яку ця роль повинна виконувати.

– Політики запобігання втраті даних - Може конфігурувати політики DLP для всіх каналів, а також класифікаторів вмісту та ресурсів.

– Політики виявлення - може налаштовувати політики виявлення, завдання, класифікатори вмісту та ресурси.

6. У розділі Журнали Вибрати журнали, до яких ця роль повинна мати доступ.

– Журнал трафіку містить детальну інформацію про трафік, що контролюється Forcepoint DLP протягом певних періодів, наприклад дані, що порушують політику, та вжиті дії.

– Системний журнал відображає системні події, надіслані від різних компонентів Forcepoint, наприклад серверів Forcepoint DLP, захисників або механізмів політики.

– Журнал аудиту відображає дії, що виконуються адміністраторами в системі.

7. У розділі Налаштування Вибрати, до яких параметрів загальних налаштувань повинні мати доступ адміністратори з цією роллю.

– Послуги - адміністратори можуть налаштовувати локальні та зовнішні служби, такі як служба зв'язку та Microsoft RMS.

– Архівувати розділи - адміністратори можуть вибирати розділи випадків, а потім архівувати, відновлювати або видаляти їх.

– Оновлення політики - адміністратори можуть оновити заздалегідь визначені політики до останньої версії. Усі інші загальні налаштування

– Аналітика - адміністратори можуть налаштовувати параметри, що використовуються для розрахунку оцінок ризику у звіті про рейтинг ризиків інцидентів.

– Усі інші загальні налаштування - адміністратори можуть налаштувати всі інші параметри в меню Налаштування> Загальні.

8. Вкажіть, чи можуть адміністратори цієї ролі налаштувати параметри авторизації модуля захисту даних.

9. У розділі Розгортання Вибрати, які функції повинні виконувати адміністратори з цією роллю.

– Керувати системними модулями - надайте цій ролі можливість реєструвати модулі на сервері управління.

– Керувати профілями кінцевих точок - надайте цій ролі можливість перегляду та редагування профілей кінцевих точок. Адміністратори можуть

додавати нові профілі кінцевих точок, видаляти профілі та переставляти порядок.

– Параметри розгортання - надайте цій ролі можливість розгорнути параметри конфігурації на всіх системних модулях.

10. Натиснути OK, щоб зберегти зміни.

Додавання ролі системного адміністратора

Щоб визначити нову роль:

1. Перейти на сторінку Налаштування> Авторизація> Ролі в модулі Захист даних Менеджера безпеки.

2. Натиснути Створити на панелі інструментів у верхній частині області вмісту.

3. Ввести ім’я нової ролі – “Системний адміністратор”.

4. Ввести Опис ролі.

5. У розділі "Дозволи" вибрати наступне:

– вибрати «Налаштований», щоб визначити охоплення цієї ролі, а потім продовжити користувацькі права доступу:

1. У розділі Статус вибрати звіти про стан, до яких ця роль повинна мати доступ:

– на інформаційній панелі відображаються системні сповіщення, статистика та підсумок подій за останні 24 години.

– екран "Здоров'я системи" дозволяє контролювати продуктивність серверів і захисників Forcepoint DLP.

– на екрані стану кінцевої точки узагальнено результати тестів підключення кінцевих точок.

2. У розділі „Звітування” Вибрати функції „Запобігання втраті даних та мобільні події” та функції звітування, до яких ця роль повинна мати доступ.

– вибрати Підсумкові звіти, щоб надати адміністраторам з цією роллю доступ до підсумкових звітів про запобігання втраті даних.

3. Вибрати інцидент Відкриття та функції звітування для цієї ролі.

– підсумкові звіти - Вибрати цей параметр, щоб надати адміністраторам з цією роллю доступ до зведених звітів про виявлення.

4. Позначте Надіслати сповіщення електронною поштою, якщо адміністратори з цією роллю повинні отримувати сповіщення про призначення інциденту.

5. У розділі Журнали Вибрати журнали, до яких ця роль повинна мати доступ.

– журнал трафіку містить детальну інформацію про трафік, що контролюється Forcepoint DLP протягом певних періодів, наприклад дані, що порушують політику, та вжиті дії.

– системний журнал відображає системні події, надіслані від різних компонентів Forcepoint, наприклад серверів Forcepoint DLP, захисників або механізмів політики.

– журнал аудиту відображає дії, що виконуються адміністраторами в системі.

6. У розділі Налаштування Вибрати, до яких параметрів загальних налаштувань повинен мати доступ адміністратор з цією роллю.

– послуги - адміністратори можуть налаштовувати локальні та зовнішні служби, такі як служба зв'язку та Microsoft RMS.

– архівувати розділи - адміністратори можуть вибирати розділи випадків, а потім архівувати, відновлювати або видаляти їх.

– оновлення політики - адміністратори можуть оновити заздалегідь визначені політики до останньої версії. Усі інші загальні налаштування

– усі інші загальні налаштування - адміністратори можуть налаштувати всі інші параметри в меню Налаштування> Загальні.

7. Вказати, чи можуть адміністратори цієї ролі налаштувати параметри авторизації модуля захисту даних.

8. У розділі Розгортання вибрати, які функції повинен виконувати адміністратор з цією роллю.

– керувати системними модулями - надайте цій ролі можливість реєструвати модулі на сервері управління.

– керувати профілями кінцевих точок - надайте цій ролі можливість перегляду та редагування профілі кінцевих точок. Адміністратори можуть додавати нові профілі кінцевих точок, видаляти профілі та переставляти порядок. (Не входить до Forcepoint Web Security або Forcepoint Email Security.)

9. Натиснути OK, щоб зберегти зміни.

2.7 Висновок

Була розглянута модель загроз і порушника, наведена методика роботи DLP та Speech-to-text систем, яка дозволя аналізувати інформацію та дії між оператором call-центру та клієнтом на наявність порушень політики безпеки у діях оператора та у разі потреби блокувати доступ до тієї чи іншої інформації або блокувати дії.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою цього розділу є обґрунтування економічної доцільності застосування методика виявлення порушень політики безпеки оператора call-центру. Для досягнення поставленої мети необхідно здійснити наступні розрахунки:

– капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект від засобів резервування даних на комерційному підприємстві;

– показники економічної ефективності застосування засобів резервування даних на комерційному підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

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

3.1.1. Визначення витрат на створення методики захисту інформації

3.1.1.1 Визначення трудомісткості розробки та опрацювання засобів резервування даних на підприємстві

Визначення трудомісткості розробки та опрацювання засобів резервування даних на підприємстві здійснюється, виходячи з тривалості кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації:

$$t= t_{тз} + t_{п} + t_{з} + t_{озб} + t_{овр} + t_{пб} + t_{д} \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку методики, $t_{тз}$ = 16 год. ;

$t_п$ – тривалість процесу аналізу моделі порушника, $t_п$ = 16 год.;

$t_з$ – тривалість процесу аналізу моделі загроз, $t_з$ = 16 год. ;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення роботи методики, $t_{озб}$ = 12 год.;

$t_{овр}$ – тривалість впровадження методики, $t_{овр}$ = 24 год.;

$t_{пб}$ – тривалість складання політик безпеки, $t_{пб}$ = 16;

$t_д$ – тривалість документального оформлення політики безпеки, $t_д$ = 8 год..

Отже, t=16+16+16+12+24+16+8= 108 годин,

3.1.1.2 Розрахунок витрат на створення методики

Витрати на створення методики ***Кпз*** складаються з витрат на заробітну плату виконавця програмного забезпечення ***Ззп*** і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК ***Змч***:

$$K_{пз} = З_{зп} + З_{мч} . \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування) і визначається за формулою:

$$З_{ЗП} = t \cdot З_{пр}, \text{ грн.}, \quad (3.3)$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата програміста з нарахуваннями, грн./годину.

За формулою (3.3) визначається заробітна плата виконавця з урахуванням середньогодинної заробітної плати з нарахуваннями у розмірі 150,5 грн./годину.

$$З_{зп} = 108 \cdot 150{,}5 = 16254 \text{ грн.},$$

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot C_{мч} + t_{д} \cdot C_{мч} \text{ , грн.,} \quad (3.4)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_{д}$ – трудомісткість підготовки документації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./годину.

Вартість машинного часу для налагодження програмного комплексу на ПК визначається за формулою (3.4):

$$З_{мч} = 6 \cdot 3{,}9 + 2 \cdot 3{,}9 = 31{,}2 \quad \text{грн.}$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot C_{е} + \frac{Ф_{зал} \cdot Н_{а}}{F_{р}} + \frac{К_{лпз} \cdot Н_{апз}}{F_{р}}, \text{ грн.,} \quad (3.5)$$

де P – встановлена потужність ПК (P = 0,8 кВт);

$t_{нал}$ – час налагодження програмного комплексу;

$C_{е}$ – тариф на електричну енергію ($C_{е}$ = 1,68 грн./кВт за годину);

$Ф_{зал}$ – залишкова вартість ПК на поточний рік ($Ф_{зал}$ = 5345 грн.);

$Н_{а}$ – річна норма амортизації на ПК ($Н_{а}$ = 0,1 частки одиниці);

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення ($Н_{апз}$ = 0,2 частки одиниці);

$К_{лпз}$ – вартість ліцензійного програмного забезпечення ($К_{лпз}$ = 1827 грн.);

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня ($F_р$ = 1920 годин).

Вартість 1 години машинного часу ПК визначається за формулою (3.5):

$$Смч = 0,8 \cdot 2 \cdot 1,68 + \frac{5345 \cdot 0,1}{1920} + \frac{2650 \cdot 0,2}{1920} = 3,9 \text{грн.}$$

Витрати на створення програмного продукту $К_{пз}$ визначаються за формулою (3.2)

$$К_{пз} = 16254+31,2=16285,2 \text{ грн.}$$

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

Визначена таким чином вартість створення методики *Кпз* є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

Вартість безстрокової ліцензії Forcepoint Endpoint DLP для юридичних осіб при закупівлі її на 2-15 ПК складає 1625 грн. Програмне забезпечення встановлюється на 14 ПК.

Вартість безстрокової ліцензії Forcepoint DLP для юридичних складає 2000 грн. Програмне забезпечення встановлюється на 1 ПК.

Вартість безстрокової ліцензії Speech-to-text складає 1000 грн. Програмне забезпечення встановлюється на 15 ПК.

Таким чином, капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \quad (3.6)$$

де $К_{пр}$ – вартість розробки методики ($К_{пр}$=17329,68 грн.);

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), ($К_{зпз}$ = 39 750 грн.);

Капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки визначаються за формулою (3.6):

$$К = 17329,68+ 39\ 750+16285,2 + = 57079,68 \text{ грн.}$$

3.1.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \text{ грн.} \quad (3.7)$$

де $С_в$ - вартість відновлення й модернізації системи ($С_в$ = 0);

$С_к$ - витрати на керування системою в цілому обчислюються за формулою (3.8);

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

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

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.} \quad (3.8)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_н$ = 0 грн.).

Річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій.

Амортизації підлягає програмне забезпечення Forcepoint DLP та Speech-to-text API загальною вартістю 39 750 грн. з припустимим строком дії

користування 2 роки. Таким чином, річні амортизаційні відрахування за прямолінійним методом нарахування складуть:

$$С_а = 39\ 750 / 2 = 19875 \text{ грн.}$$

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

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.15)$$

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

Основна заробітна плата одного системного адміністратора на місяць складає 16000 грн. Додаткова заробітна плата –8% від основної заробітної плати. Отже,

$$С_з = 16000*12 + 16000*12*0,08= 207\ 360 \text{ грн.}$$

З 01.01.2016 року ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 207360*0,22 = 45619,2 \text{ грн.}$$

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.16)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р = 0,8 кВт);

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

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

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, визначається за формулою (3.16):

$$С_{ел} = 0,8*1920*1,68 = 2580,48 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат -1% ($С_{тос}$ = 57079,68 *0,01=570,79 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються за формулою (3.8):

$$С_к = 570,79 + 207360 + 45619,2 + 2580,48 + 19875= 276005,47 \text{ грн.}$$

Річні поточні витрати на функціонування системи інформаційної безпеки визначаються за формулою (3.9):

$$С = 276005,47 \text{ грн.}$$

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості збитку застосовуємо спрощену модель оцінки.

Необхідні вхідні дані для розрахунку:

де $t_п$ – час простою вузла внаслідок атаки ($t_п$ = 12 годин);

$t_в$ – час відновлення після атаки персоналом ($t_в$ = 8 годин);

$t_{ві}$ – час повторного введення загубленої інформації співробітниками атакованого сегменту мережі ($t_{ві}$ = 7 годин);

$З_о$ – заробітна плата обслуговуючого персоналу ($З_о$ = 16000 грн. на місяць);

$З_с$ – заробітна плата співробітників атакованого вузла ($З_с$ = 10000 грн. на місяць);

$Ч_о$ – чисельність обслуговуючого персоналу ($Ч_о$ = 2 особи);

$Ч_с$ – чисельність співробітників атакованого сегменту мережі ($Ч_с$ = 15 особи);

О – обсяг продажів атакованого сегменту мережі, (О = 310000 грн. на рік);

$П_{зч}$ – вартість заміни устаткування або запасних частин, ($П_{зч}$ = 0 грн.);

I – число атакованих вузлів (I = 15);

N – середнє число атак на рік (N = 28).

Упущена вигода від простою атакованого вузла становить:

$$U = П_п + П_в + V, \qquad (3.10)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн.;

$П_в$ – вартість відновлення працездатності сегмента мережі, грн.;

V – втрати від зниження обсягу продажів за час простою атакованого вузла, грн.

Упущена вигода від простою атакованого вузла визначається за формулою (3.10):

$$U = 3409{,}09 + 6829{,}53 + 1490{,}38 = 11729 \text{ грн.},$$

Втрати від зниження продуктивності співробітників атакованого сегмента мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_п = \frac{\sum Зс}{F} \cdot t_п \quad , \qquad (3.11)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить F = 176 годин).

Втрати від зниження продуктивності співробітників атакованого сегмента мережі визначаються за формулою (3.18):

$$П_п = \frac{10000}{176} \cdot 15 \cdot 4 = 3409{,}09 \text{ грн.},$$

Витрати на відновлення працездатності сегмента мережі включають кілька складових:

$$П_в = П_{ві} + П_{пв} + П_{зч}, \qquad (3.12)$$

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

$П_{пв}$ – витрати на відновлення сегмента мережі, грн.;

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

Витрати на відновлення працездатності сегмента мережі визначаються за формулою (3.12):

$$П_в = 2556{,}81 + 272{,}72 + 4000 = 6829{,}53 \text{ грн.},$$

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

$$П_{ві} = \frac{\sum Зс}{F} \cdot t_{ві} \ . \qquad (3.13)$$

Витрати на повторне введення інформації визначаються за формулою (3.13):

$$П_{вi} = \frac{10000}{176} \cdot 15 \cdot 3 = 2556{,}81 \text{ грн.}$$

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

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в \ . \qquad (3.14)$$

Витрати на відновлення сегмента мережі визначаються за формулою (3.14):

$$П_{пв} = \frac{16000}{176} \cdot 3 = 272{,}72 \text{ грн.}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого сегмента мережі визначаються виходячи із середньогодинного обсягу продажів типового підприємства і сумарного часу простою атаковано сегмента мережі:

$$V = \frac{O}{Fp} \cdot (t_п + t_в + t_{вi}) \text{ , грн.} \qquad (3.15)$$

де $F_р$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько ($F_р$ = 2080 годин).

Втрати від зниження очікуваного обсягу продажів типового підприємства визначаються за формулою (3.15):

$$V = \frac{310000}{2080} \cdot (4 + 3 + 3) = 1490{,}38 \text{ грн.},$$

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

$$B = \sum_i \sum_n U = 3*30*11711{,}96 = 1054076{,}4 \text{ грн.} \qquad (3.16)$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.}, \qquad (3.17)$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (60%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і визначається за формулою (3.17):

E = 1054076,4*0,60 – 276005,47= 356440,37 грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \tag{3.18}$$

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

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

Коефіцієнт повернення інвестицій ROSI визначається за формулою (3.18):

$$ROSI = \frac{356440,37}{57079,68} = 6,24, \quad \text{частки одиниці,}$$

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

$$\text{ROSI} > (N_{деп} - N_{інф})/100), \tag{3.19}$$

де $N_{деп}$ – річна депозитна ставка, (13 %);

$N_{інф}$ – річний рівень інфляції, (4%).

Розрахункове значення коефіцієнта повернення інвестицій визначається за формулою (3.19):

$$6,24 > (13 - 4)/100 = 6,24 > 0,09.$$

Термін окупності капітальних інвестицій T_o визначається за формулою (3.20) та показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{6{,}24} = 0{,}16, \quad \text{років.} \qquad (3.20)$$

3.4 Висновок

Результатом проведеної роботи в даному розділі є обґрунтування економічної доцільності застосування методики виявлення порушень політики безпеки оператора call-центру.

Розраховані капітальні витрати, які складають 57079,68 грн., поточні витрати на експлуатацію системи інформаційної безпеки, що становлять 276005,47 грн. Визначена величина економічного ефекту складає 356440,37 грн. Коефіцієнт повернення інвестицій складає 6,24 та швидкість повернення 0,16 року(біля 2 місяців).

Аналіз проведених розрахунків дозоляє зробити висновок про економічну доцільність застосування методики виявлення порушень політики безпеки оператора call-центру.

ВИСНОВКИ

У ході роботи було розглянуто: архітектура call-центру, системи контролю оператора call-центру, DLP системи та принципи їх роботи. Також була розроблена модель загроз і порушника. Була розроблена методика конфігурації DLP системи Forcepoint DLP та системи Speech-to-text для виявлення порушень політики безпеки оператора call-центру при обробці запитів клієнта.

Використання методики надає організації можливість зменшити вірогідність витоку інформації з обмеженим доступом, наприклад, з call-центру не зможе безперешкодно статися витік баз кредитних карт і персональних даних клієнтів. За результатами переміщень конфіденційних даних повинна вестися докладна статистика з можливістю відстеження відповідності вимогам діючих стандартів безпеки. Для підвищення ефективності роботи системи слід поєднати використання в єдиному програмному комплексі, методів DLP, методів роботи з мовною інформацією, а також адаптувати методи навчання системи.

Навчання системи здійснюється:

- введенням зразків конфіденційної інформації;
- введенням машинного навчання;
- включенням політик безпеки
- включенням політик виявлення;
- введенням власних слів і виразів, характерних для конфіденційних даних;
- введенням винятків.

Об'єднання методів роботи в мовною інформацією і DLP-систем дозволяє контролювати інформацію, яка залишала межі корпоративної мережі, захистити серверні сховища і знімні носії, які фізично можуть потрапити до рук сторонніх осіб. Таким чином, методи роботи в мовною інформацією можуть істотно

розширити можливості DLP-систем і знизити ризики витоку конфіденційних даних.

ПЕРЛІК ПОСИЛАНЬ

1. Jackson D. Typical Roles in a Call Centre – With Job Descriptions [Електронний ресурс] / Douglas Jackson – Режим доступу до ресурсу: https://www.callcentrehelper.com/typical-roles-in-a-call-centre-51389.htm.

2. Организация Call-центра (колл-центра) с нуля [Електронний ресурс] – Режим доступу до ресурсу: https://skomplekt.com/organizatciya-call-centra-s-nulya/

3. Что такое DLP и как они работают? [Електронний ресурс] – Режим доступу до ресурсу: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/.

4. ПРИНЦИП РАБОТЫ DLP-СИСТЕМЫ [Електронний ресурс] – Режим доступу до ресурсу: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/printsip-raboty-dlp-sistemy/

5. Cloud Data Loss Prevention [Електронний ресурс] – Режим доступу до ресурсу: https://cloud.google.com/dlp#section-5.

6. Forcepoint DLP Administration Help [Електронний ресурс] – Режим доступу до ресурсу: https://www.websense.com/content/support/library/data/v84/help/dlp_help.pdf.

7. Speech-to-Text [Електронний ресурс] – Режим доступу до ресурсу: https://cloud.google.com/speech-to-text.

8. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

9. НД ТЗІ 2.5-005-99. «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

10. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. – К.: ДСТСЗІ СБ України, 1999.

11. Aussprache und Intonation üben [Електронний ресурс] – Режим доступу до ресурсу: https://www.sprachenzentrum.fuberlin.de/slz/lernen_zu_lernen/bilder_und_pdf/pdf/Aussprache_Intonation2.pdf.

12. What Is DLP? [Електронний ресурс] – Режим доступу до ресурсу:https://www.fortinet.com/resources/cyberglossary/data-loss-prevention.

13. What is DLP and how to implement it in your organization? [Електронний ресурс] – Режим доступу до ресурсу: https://www.exabeam.com/dlp/data-loss-prevention-policies-best-practices-and-evaluating-dlp-software/.

14. Обзор функции защиты от потери данных [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/ru-ru/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	35	
6	А4	2 Розділ	44	
7	А4	3 Розділ	13	
8	А4	Висновки	2	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	26	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	2	

ДОДАТОК Б. ПІДГОТОВЧИЙ ЕТАП

Підготовчий етап включає:

1. Установка серверної частини Forcepoint DLP
2. Установка клієнтської частини Forcepoint Endpoint DLP
3. Визначення модулів DLP системи, які будуть працювати
4. Установка Speech-to-text на кінцеві пристрої

1. Установка сервера управління

1. Увійти на інсталяційну машину з обліковим записом, який має привілеї як домену, так і місцевого адміністратора.

2. Двічі натиснути Forcepoint85Setup.exe, щоб запустити програму налаштування.

3. На екрані привітання натиснути кнопку Пуск.

4. На екрані Угоди про підписку вибрати Я приймаю цю угоду, а потім натиснути Далі.

5. На екрані «Тип інсталяції» вибрати «Диспетчер безпеки Forcepoint», а потім «DLP Forcepoint».

Натиснути Далі.

6. Якщо на екрані «Тип інсталяції» не встановлено SQL Server, вибрати «Установити SQL Server 2016 Express SP1» на цій машині.

7. Дотримуватись інструкцій майстра, щоб встановити Microsoft SQL Server 2016 Express SP1 для використання Forcepoint Security Manager.

8. На екрані Підсумок перед установкою натиснути Далі, щоб продовжити встановлення.

9. На екрані Підсумок натиснути Готово.

Установка інфраструктури управління Forcepoint

1. На екрані привітання програми налаштування інфраструктури Forcepoint Натиснути кнопку Далі.

2. На екрані каталогу встановлення прийміть шлях встановлення за замовчуванням (рекомендується) або вказати власний шлях встановлення та Натиснути Далі.

3. На екрані SQL Server вказати розташування механізму баз даних.

4. Вказати метод автентифікації та інформацію про обліковий запис для підключення до бази даних SQL Server:

a. Вибрати автентифікацію SQL Server, щоб використовувати обліковий запис SQL Server, або автентифікацію Windows, щоб використовувати надійне з'єднання Windows.

b. Ввести ім'я користувача або акаунт та його пароль.

Для SQL Server Express автоматично визначається sa (обліковий запис системного адміністратора за замовчуванням).

c. Forcepoint DLP може використовувати SSL для шифрування зв'язку з базою даних. Якщо шифрування вже налаштовано в Microsoft SQL Server, вибрати Шифрувати з'єднання, щоб увімкнути шифрування SSL.

d. Натиснути Далі.

5. На екрані Сервер та облікові дані Ввести таку інформацію:

a. Вибрати IP-адресу для цього пристрою. Якщо апарат має одну мережеву карту інтерфейсу (NIC), буде вказана лише одна адреса.

Адміністратори використовуватимуть обрану адресу IPv4 для доступу до Менеджера безпеки через веб-браузер. Це також IP-адреса, яку віддалені компоненти Forcepoint використовуватимуть для підключення до сервера управління.

b. Вказати Сервер або домен облікового запису служби, який буде використовуватися компонентами Forcepoint Management Infrastructure та Security Manager.

Ім'я хосту не може перевищувати 15 символів.

c. Вказати ім'я користувача та пароль для облікового запису служби.

d. Натиснути Далі.

6. На екрані Обліковий запис адміністратора ввести адресу електронної пошти та пароль для облікового запису адміністратора Security Manager за замовчуванням: admin. Цей обліковий запис має повний доступ до всіх функцій і функцій диспетчера безпеки для всіх продуктів.

7. На екрані Налаштування електронної пошти налаштуйте SMTP-сервер для використання для системних сповіщень, а потім натиснути кнопку Далі. Параметри SMTP також можна налаштувати після встановлення.

a. Ввести IP-адресу або ім'я хосту SMTP-сервера, через який слід надсилати сповіщення електронною поштою. У більшості випадків слід використовувати порт за замовчуванням.

b. Ввести адресу електронної пошти відправника, яка з'явиться в повідомленнях електронної пошти із сповіщеннями.

c. Ввести описове ім'я відправника, яке використовуватиметься в повідомленнях електронної пошти. Це може допомогти одержувачам визначити, що повідомлення походить від диспетчера безпеки.

8. На екрані Підсумок перед установкою перевірте інформацію, а потім Натиснути Далі, щоб розпочати встановлення

9. Якщо ви вирішили встановити SQL Server Express, PowerShell 1.0 та Windows Installe 4.5 будуть встановлені, якщо їх ще немає.

10. Якщо для інсталяції обрано SQL Server Express, запускається інсталяція SQL Server 2016 SP1 Express.

11. З'явиться екран встановлення

12. На екрані Установка завершена Натиснути Готово.

Установка компонентів управління DLP Forcepoint

1. Коли запущено інсталятор Forcepoint DLP, з'являється екран привітання. Натиснути Далі, щоб розпочати встановлення DLP Forcepoint.

2. На екрані Цільова папка прийміть каталог встановлення за замовчуванням (C: \ Program Files (x86) \ Websense \ Data Security) або Натиснути кнопку Огляд, щоб вибрати інше місце.

Щоб продовжити, Натиснути Далі.

3. На екрані Локальний адміністратор Вказати Ім'я користувача та Пароль для облікового запису локального адміністратора з повним доступом до всіх серверів, що включають компоненти Forcepoint DLP.

4. Якщо база даних SQL Server знаходиться на віддаленій машині, використовуйте екран Тимчасове розташування файлів, щоб увімкнути архівування інцидентів та резервне копіювання системи, а потім Вказати, де система зберігає тимчасові файли під час обробки архівів та резервного копіювання та відновлення системи

5. На екрані бази даних відбитків пальців прийміть каталог баз даних за замовчуванням (C: \ Program Files (x86) \ Websense \ Data Security \ PreciseID DB \) або Натиснути кнопку Огляд, щоб вибрати інший локальний шлях.

Щоб продовжити, Натиснути Далі.

6. На екрані Підтвердження встановлення спочатку перевірте правильність поточного часу та даних, а потім Натиснути кнопку Встановити, щоб розпочати встановлення компонентів DLP Forcepoint.

7. Відобразиться екран Прогрес встановлення.

Під час встановлення програма налаштування може відображати запит на:

- встановити необхідні сторонні служби.
- порт 80.
- порт 443.

Натиснути Так, щоб продовжити встановлення (Ні скасовує встановлення).

8. Коли з’явиться екран Установка завершена, натиснути Готово, щоб закрити інсталятор Forcepoint DLP.

Установка віртуального пристрою механізму аналітики

1. У майстрі першого завантаження ввести так, щоб встановити образ механізму аналітики, а потім прочитайте та прийміть угоду про підписку.

2. На першому запиті Вибрати режим захисту. Єдиний доступний варіант - 1, для Forcepoint DLP Analytics Engine. ввести так, щоб продовжити.

3. Ввести ім'я хосту для пристрою.

Приклад: appliance.domain.com

4. Є можливість налаштувати сервер NTP; Вибрати так, щоб увімкнути NTP та Ввести NTP-сервер, розділяючи URL-адреси комами.

5. Вибрати відповідний часовий пояс.

6. Ввести пароль адміністратора для входу в прилад.

7. Вибрана конфігурація відображається для перегляду. Якщо вас влаштовує поточна конфігурація, Ввести так, щоб продовжити налаштування мережі приладу.

8. У вас є можливість налаштувати мережу приладів за допомогою сервера DHCP або вручну. Вибрати ні для ручної конфігурації; DHCP не підтримується.

9. Якщо ви вибрали ручну конфігурацію, Ввести маску підмережі, шлюз за замовчуванням та DNS, коли буде запропоновано.

10. Вибрана конфігурація відображається для перегляду. Якщо вас влаштовує поточна конфігурація, Ввести так, щоб продовжити налаштування двигуна приладу.

11. Ввести IP-адресу диспетчера Forcepoint Security.

12. Ввести ім’я користувача та пароль для Forcepoint Security Manager.

13. Вибрана конфігурація відображається для перегляду. Якщо вас влаштовує поточна конфігурація, Ввести так.

14. Повні налаштування конфігурації для аналізу механізму аналізу для огляду. Якщо ви задоволені готовою конфігурацією, Ввести так.

Якщо ви введете ні, майстер конфігурації перезапуститься, і вам потрібно буде повторно ввести всю інформацію.

15. Після завершення роботи майстра віртуальний пристрій механізму аналітики встановлюється та відображається на сторінці Налаштування> Розгортання> Системні модулі. Щоб розгорнути механізм аналітики, Натиснути Розгорнути.

Встановлення агента інтеграції

Коли ви вставляєте агент інтеграції в інсталятор продукту, 3 компоненти DLP Forcepoint встановлюються на машині кінцевого користувача:

– PEInterface.dll взаємодіє з механізмом політики Forcepoint DLP на сервері управління.

– ConnectorsAPIClient.exe підключає API сторонніх продуктів до Forcepoint DLP.

– registerAgent.bat (або .vbs) виконує реєстрацію на сервері управління. У Windows інсталяційний пакет агента інтеграції надається у вигляді файлу MSI. Майстер встановлення MSI представляє 4 інтерактивні діалоги:

– Installation-dir, щоб вибрати каталог встановлення

– зареєстровані канали для вибору каналів DLP для використання: HTTP, SMTP, принтер, виявлення

– локальна IP-адреса, щоб вибрати, яку із статичних IP-адрес, призначених на даний момент пристрою, слід використовувати для реєстрації

– деталі сервера управління, щоб вказати IP-адресу або ім'я хосту, ім'я користувача та пароль сервера управління

Реєстрація агента інтеграції

Кожен екземпляр агента інтеграції повинен бути зареєстрований після встановлення. Іншими словами, кожного разу, коли сторонній продукт встановлюється на машині кінцевого користувача, цей екземпляр агента потрібно реєструвати.

Операцію реєстрації можна виконати під час встановлення установчиком або за допомогою утиліти командного рядка, що постачається разом із агентом.

Утиліта командного рядка отримує такі вхідні аргументи:

– протоколи - непорожній список підтримуваних протоколів (поза HTTP, SMTP, Printer, Discovery).

– пані сервера управління - IP-адреса або ім’я хосту, ім’я користувача, пароль.

– локальна IP-адреса (необов’язково) - Якщо вона не надана, використати будь-яку зі статичних адрес апарата та роздрукуйте її на стандартний вихід.

– шукати IP-адресу (необов’язково) - використовується для перереєстрації після зміни IP. Якщо цього не вказано, використати адресу у файлі “registerAgent.conf”. Якщо цей файл не існує, використати вказану локальну IP-адресу.

Успішна операція реєструє машину на сервері управління та визначає, що вона має відповідні протоколи. Він також генерує файли сертифікатів у тому самому каталозі, де знаходиться інструмент. Інструмент також зберігав файл конфігурації (registerAgent.conf) з IP-адресою, яка використовується для реєстрації.

У разі невдачі сценарій повертає значущий код виходу і друкує повідомлення про помилку стандартний вихід

Встановлення агента сканера

Сканер - це назва агента для виявлення та відбитків пальців. Він вибирається за замовчуванням, коли ви встановлюєте сервер управління або додаткові сервери DLP Forcepoint.

1. Завантажити інсталятор Forcepoint Security (Forcepoint85Setup.exe) зі сторінки «Мій обліковий запис> Завантаження» за адресою support.forcepoint.com.
2. Запустити програму встановлення.
3. Прийняти ліцензійну угоду.
4. Вибрати Власний.
5. Натиснути на посилання встановити для Forcepoint DLP.
6. На екрані привітання натиснути Далі, щоб розпочати встановлення.

7. На екрані Папка призначення вказати папку, в яку слід встановити агент.

8. На екрані «Вибір компонентів» вибрати «Гусеничний агент», а потім на локальному жорсткому диску буде встановлена ціла функція. Якщо це автономна установка, скасуйте вибір усіх інших параметрів, включаючи Forcepoint DLP Server.

9. На екрані Доступ до сервера вибрати IP-адресу, щоб ідентифікувати цей апарат до інших компонентів Forcepoint.

10. На екрані Реєстрація з сервером Forcepoint DLP Вказати шлях та ввійти в облікові дані для сервера Forcepoint DLP, до якого цей агент буде підключатися. Це може бути сервер управління або додатковий сервер DLP Forcepoint. FQDN - це повноцінне доменне ім'я машини.

11. На екрані локального адміністратора ввести ім’я користувача та пароль відповідно до інструкцій на екрані. Частина імені сервера / хоста імені користувача не може перевищувати 15 символів.

12. Якщо був встановений на цьому комп'ютері клієнт Lotus Notes, щоб була можливість виконувати “відбитки пальців” та виявлення на сервері Lotus Domino, з’явиться екран Lotus Domino Connections.

13. Якщо на екрані Підтвердження встановлення вся введена інформація правильна, Натиснути кнопку Встановити, щоб розпочати встановлення.

14. Після завершення інсталяції з’являється екран «Інсталяція завершений», який повідомляє про те, що ваша установка завершена. Натиснути Готово.

15. Після завершення встановлення з’являється екран «Успішне встановлення» з повідомленням про те, що встановлення завершено.

Встановлення протектора

КРОК 1: Прийняти ліцензійну угоду

Щоразу, коли відкривається майстер встановлення, з’являється ліцензійна угода з кінцевим користувачем. Використати клавіші "вниз",

прокручування або пробіл, щоб прочитати до кінця угоди. Уважно прочитати ліцензійну угоду і, коли з’явиться відповідний запит, Ввести yes, щоб прийняти її.

КРОК 2: Вибрати обладнання для встановлення та підтвердити вимоги до обладнання Система перевіряє, чи відповідає ваше обладнання наступним вимогам:

- 2 ГБ оперативної пам'яті
- 4 процесора
- Процесор з кеш-пам'яттю більше 2 Мб
- Швидкість процесора 8000
- Розділ “/ opt / websense / data” повинен мати принаймні 45 ГБ
- 2 мережеві адаптери

Якщо машина не відповідає вимогам, майстер запитує, продовжувати чи ні.

КРОК 3: Встановити адміністраторський і root пароль

1. Ввести і підтвердити новий пароль для облікового запису “адміністратор”. З міркувань безпеки найкраще змінити пароль за замовчуванням.

2. Ввести і підтвердити новий пароль користувача (обов’язково). Кореневий обліковий запис забезпечує повний доступ до пристрою і ним слід користуватися обережно

КРОК 4: Встановити мережеву карту для сервера управління та SSH зв'язку

З'явиться список доступних мережевих інтерфейсів (NIC). На цьому кроці вибрати мережеву карту для використання сервером управління, з'єднаннями SSH та входом до захисника (за замовчуванням eth0). Усі інші мережеві карти будуть використовуватися для перехоплення трафіку.

Щоб допомогти визначити, який мережевий адаптер використовувати, майстер може імітувати трафік протягом 0-60 секунд і змусити світлодіоди

блимати на вибраному інтерфейсі. Це працює не для всього обладнання та драйверів.

1. Коли з’явиться відповідний запит, вибрати номер індексу NIC керуючої NIC або прийміть інтерфейс за замовчуванням.

2. Ввести число 0-60, щоб вказати, як довго (у секундах) імітувати дорожній рух, або Натиснути Enter, щоб пропустити цей крок.

3. Ввести IP-адресу мережевої карти, яку потрібно використовувати. За замовчуванням 192.168.1.1.

4. Ввести префікс IP цього мережевого адаптера. Це маска підмережі у скороченому форматі (кількість бітів у масці підмережі). Типовим значенням є 24 (255.255.255.0).

5. Ввести адресу трансляції для NIC. Майстер встановлення надасть обчислене значення, яке зазвичай є правильним.

6. Ввести IP-адресу шлюзу за замовчуванням, який буде використовуватися для доступу до мережі. Якщо IP-адреса сервера Forcepoint DLP не знаходиться в тій самій підмережі, що і протектор, потрібен шлюз за замовчуванням, щоб повідомити захиснику, як взаємодіяти з сервером Forcepoint DLP.

КРОК 5: Визначити ім'я хоста та ім'я домену

1. Ввести унікальне ім’я хосту для пристрою-протектора.

2. За бажанням ввести доменне ім’я мережі, до якої було додано захисник. Встановлене тут доменне ім'я буде використано сервером Forcepoint DLP при визначенні параметрів захисника.

КРОК 6: Визначити сервер доменних імен

Необов’язково Ввести IP-адресу сервера доменних імен (DNS) для цього захисника. DNS надає доступ до інших мережевих ресурсів, використовуючи їхні імена замість IP-адрес.

КРОК 7: Встановити дату, час та часовий пояс

1. Ввести поточний часовий пояс.

2. Ввести поточну дату у такому форматі: дд-ммм-рррр

3. Ввести поточний час у 24-годинному форматі HH: MM: SS.

КРОК 8: Зареєструватись на сервері Forcepoint DLP

На цьому кроці буде створено захищений канал, що з'єднує захисник із сервером Forcepoint DLP. Це може бути або сервер управління, або додатковий сервер.

1. Ввести IP-адресу або повне доменне ім’я сервера DLP Forcepoint. Звернути увагу, що це повинна бути IP-адреса, визначена під час встановлення серверного комп'ютера. Це не може бути вторинна IP-адреса.

2. Ввести ім'я користувача та пароль адміністратора Forcepoint DLP, який має привілеї для управління системними модулями.

Заключний крок: Перевірити встановлення протектора

У модулі захисту даних диспетчера безпеки переконайтися, що статус захисника більше не очікується, а піктограма відображає його активний статус. Оновити браузер.

Натиснути Розгорнути.

Налаштування протектора

Щоб розпочати моніторинг мережі на предмет втрати конфіденційної інформації,потрібно налаштувати захист у модулі захисту даних диспетчера безпеки Forcepoint на сторінці Параметри> Розгортання> Системні модулі.

Основними кроками є:

1. Вибрати екземпляр протектора.

2. Визначити канали для контролю протектора.

3. Надати додаткові параметри конфігурації, необхідні серверу Forcepoint DLP для визначення політик щодо несанкціонованого трафіку.

4. Натиснути на розгортання.

2. Встановлення клієнтської частини Forcepoint Endpoint DLP

Процес розгортання програмного забезпечення кінцевої точки включає такі основні кроки:

1. Встановити сервер управління DLP Forcepoint.

2. Створити пакет для клієнта кінцевої точки та розгорнути його на комп'ютерах користувачів (настільні та портативні машини), як описано в документації до кінцевої точки.

3. Додати профіль кінцевої точки до модуля захисту даних диспетчера Forcepoint Security або використати профіль за замовчуванням, встановлений разом із клієнтським пакетом.

Профілі кінцевих точок - це шаблони, які встановлюють дозволи на службу. Профіль описує необхідну поведінку клієнта кінцевої точки: як він підключається до серверів кінцевих точок, які варіанти користувацького інтерфейсу доступні на клієнті та як він використовує шифрування для захисту конфіденційних даних. Кожен профіль розгортається до вибраних клієнтів кінцевих точок.

4. Налаштувати параметри кінцевої точки.

5. Створити ресурси кінцевої точки.

6. Створити або змінити правило для каналів кінцевих точок.

7. Визначити тип машин кінцевих точок для моніторингу та налаштувати поведінку в мережі та поза мережею.

Додавання профілю кінцевої точки

Профіль кінцевої точки за замовчуванням автоматично встановлюється на клієнт кінцевої точки. Він застосовується до всіх клієнтів кінцевих точок, яким не призначено інший профіль. Профіль за замовчуванням не можна видалити, але його частини можна редагувати.

За потреби визначити додаткові профілі.

– Щоб створити новий профіль, потрібно натиснути Новий на панелі інструментів у верхній частині сторінки Кінцевої точки.

– Щоб відредагувати існуючий профіль, Натиснути ім'я профілю у списку профілів кінцевих точок.

Майстер профілю кінцевої точки відкриється на вкладці Загальне.

1. Ввести ім'я та опис для профілю.

2. Вибрати або зніміть Доступний, щоб увімкнути або вимкнути профіль у списку профілів кінцевих точок.

Якщо профіль вимкнено, він не розгортається на жодному хості кінцевої точки.

3. За замовчуванням профіль застосовується до всіх кінцевих точок. Щоб включити або виключити певні кінцеві точки у профілі, натисніть Редагувати.

4. Вибрати категорію кінцевої точки зі спадного списку Дисплей. Доступний список оновлюється, щоб показати доступні кінцеві точки в цій категорії.

5. Щоб відфільтрувати доступні кінцеві точки, потрібно ввести текст у поле Фільтрувати за або Знайти.

– натиснути піктограму Застосувати фільтр (послідовність), щоб увімкнути фільтр.

– натиснути піктограму Очистити фільтр (X), щоб видалити поточний фільтр.

Підтримуються символи підстановки: знак запитання (?) Для позначення одного символу та зірочка (*) для кількох символів. Якщо на екрані забагато елементів, перегляньте список за допомогою кнопок «Далі», «Попередній», «Перший» та «Останній».

6. Щоб включити конкретну кінцеву точку до цього профілю:

a. У Вибраному списку вибрати вкладку Включити.

b. У списку Доступні вибрати кінцеву точку.

c. Натиснути>, щоб перемістити кінцеву точку до Вибраного списку.

7. Натиснути OK.

8. Щоб виключити певну кінцеву точку в цьому профілі кінцевої точки:

a. У Вибраному списку вибрати вкладку Виключити.

b. У списку Доступні вибрати кінцеву точку.

c. Натиснути>, щоб перемістити кінцеву точку до Вибраного списку.

9. Натиснути OK.

Налаштування параметрів кінцевої точки

Використати вкладки сторінки «Налаштування»> «Загальне»> «Кінцева точка» в модулі «Захист даних» у диспетчері Forcepoint Security, щоб налаштувати параметри програмного забезпечення кінцевої точки, наприклад, як часто перевіряти зв'язок та перевіряти наявність оновлень.

Сторінка відкриється на вкладці Загальні. Налаштувати параметри на вкладці Загальні таким чином:

1. У розділі Підключення використати поле Тестувати зв'язок у кожному полі, щоб вказати, як часто за хвилини (від 1 до 60) клієнти кінцевих точок перевіряють зв'язок (за замовчуванням 5 хвилин).

2. За допомогою випадаючого списку Перевіряти наявність оновлень вибрати, як часто (від 30 секунд до 24 годин) клієнти кінцевих точок перевіряють наявність оновлень конфігурації (1 година за замовчуванням).

3. Використати поле Кінцева точка відключена..., щоб визначити, через який час (від 1 до 60 годин) клієнт кінцевої точки визначається для відключення (48 годин, за замовчуванням).

4. У розділі Адміністрування встановити, яку дію (Дозвіл чи блокування) виконувати, коли користувачі не відповідають на запит на підтвердження після спроби виконати операцію, яка порушує політику (Блокувати за замовчуванням)

5. Якщо не потрібно, щоб користувачі кінцевих точок мали змогу деінсталювати клієнтське програмне забезпечення кінцевої точки або вимкнути блокування або захист від фальсифікацій, Вибрати Увімкнути пароль адміністратора кінцевої точки, а потім Ввести і підтвердіть пароль. Він повинен відповідати всім наступним умовам:

- Майте принаймні 8 символів
- Містити великі регістри
- Містити малі літери
- Містити цифри
- Містити нелітерально-цифрові символи

Пароль не потрібен для адміністрування клієнтів кінцевих точок.

6. У розділі Оптичний носій вказати, чи дозволяти стороннім CD / DVD записування в Windows.

– Система контролює програми для запису CD / DVD, що не є власними, блокуючи або дозволяючи операції, не виконуючи класифікацію вмісту.

– Неприродне блокування CD / DVD застосовується до пристроїв читання та запису CD, DVD та Blue-ray у кінцевих точках Windows 7, Windows 8, Windows Server 2008 R2 та Windows Server 2012.

Кінцева точка Linux не підтримує записи CD / DVD.

7. Натиснути Зберегти.

Створення ресурсів кінцевої точки

Forcepoint надає довгий перелік вбудованих програм, які можна вибрати для моніторингу в кінцевій точці під час налаштування політики щодо кінцевих точок. Ці програми, включаючи веб-програми та програми SaaS, включені до програми Endpoint.

Скористайтися сторінкою Головне> Керування політикою> Ресурси> Кінцеві програми, щоб переглянути вбудовані програми та визначити власні програми.

Щоб додати програму, натиснути Створити> Програма або Створити> Хмарне додаток на панелі інструментів угорі сторінки, а потім:

1. Ввести ім'я для цієї програми, наприклад, Microsoft Word.

2. У полі Initiated by:

– Для настільних програм Windows ввести ім'я виконуваного файлу (для

наприклад, winword.exe).

– Для програм Mac або Windows Store Ввести назву програми (наприклад,

Microsoft.SkypeApp * для програми Windows Store Camera).

– Для хмарних додатків Ввести URL-адресу.

3. Ввести Опис для цієї програми.

4. Щоб пов’язати програму з існуючою групою програм, позначити Належить до, потім Вибрати групу, що цікавить.

5. Якщо примусове виконання програми не потрібне, позначити Довірену програму

Довіреним програмам дозволяється записувати будь-який тип інформації на знімний носій інформації, наприклад, на USB-накопичувач. Їм також дозволено копіювати будь-який тип даних на віддалений спільний диск у мережі.

6. У розділі Захоплення екрана за допомогою розкривного списку Дія вибрати дію, яку потрібно виконати, коли кінцеві користувачі намагаються захопити екрани з цієї програми.

7. Натиснути OK.

Дані кінцевих точок, що надсилаються на цільові канали, такі як знімні носії (включаючи USB-накопичувачі, CD / DVD та інші зовнішні накопичувачі), Інтернет, принтери та програмні програми, можна контролювати та аналізувати.

Для націлювання на певний пристрій спочатку треба додати пристрій у список ресурсів:

1. Перейти на сторінку Головне> Керування політикою> Ресурси в модулі Захист даних Менеджера безпеки.

2. Натиснути «Пристрої кінцевих точок», потім натисніть «Створити».

Щоб вибрати кінцеві точки призначення для моніторингу в політиці:

1. Перейти на сторінку Головне> Керування політикою> Політики DLP в модулі Захист даних Менеджера безпеки.

2. Натиснути Керувати політиками.

3. Виконати одне з наступного:

– Натиснути політику та вибрати Додати> Правило

– Натиснути правило та вибрати Редагувати

4. Перейти до розділу "Призначення" для правила.

5. Вибрати із наведеного нижче:

– Вибрати Кінцева точка електронної пошти, щоб відстежувати вихідні або внутрішні повідомлення електронної пошти, надіслані на вказані адреси. За замовчуванням ця опція охоплює всі кінцеві точки призначення. Щоб вибрати пункти призначення, натисніть Редагувати.

– Вибрати Кінцева точка HTTP / HTTPS зі спадного списку Канали, щоб відстежувати пристрої кінцевих точок, таких як ноутбуки, та захищати їх від розміщення конфіденційних даних у Мережі. Цей трафік можна контролювати, коли машини кінцевих точок знаходяться поза мережею.

Кінцеве програмне забезпечення перехоплює повідомлення HTTP (S) під час їх завантаження в браузер. (Він не відстежує запити на завантаження.)

– Вибрати Друк кінцевої точки, щоб відстежувати дані, які надсилаються з машини кінцевої точки на локальний або мережевий принтер. Система підтримує драйвери, які друкують на фізичному пристрої, а не ті, що друкують у файл або PDF.

– Вибрати програму Кінцева точка, щоб контролювати або запобігати копіюванню та вставці конфіденційних даних із такої програми, як Microsoft Word або веб-браузер. Це бажано, оскільки клієнти кінцевих точок часто відключаються від корпоративної мережі і можуть становити загрозу безпеці.

– Вибрати знімний носій кінцевої точки, щоб контролювати або запобігати передачі конфіденційних даних на знімний носій. У плані дій ви визначаєте, блокувати це, дозволяти, просити користувачів підтвердити свою дію, шифрувати його ключем профілю, налаштованим адміністраторами, або шифрувати паролем, наданим користувачами кінцевих точок. Тут визначте пристрої для аналізу.

– Вибрати локальну мережу Endpoint, щоб відстежувати чи запобігати передачі конфіденційних даних через підключення до локальної

мережі на мережевий диск або спільний доступ на іншому комп'ютері. Адміністратори DLP Forcepoint можуть:

– Вказати список IP-адрес, імен хостів або мереж, дозволених як джерело або місце призначення для копіювання в локальну мережу.

– Встановити іншу поведінку відповідно до типу кінцевої точки (ноутбук чи інший) та розташування (підключено чи не підключено).

Контроль локальної мережі кінцевої точки застосовується лише до спільного використання корпорації Майкрософт.

3. Налаштування системного модуля DLP Forcepoint

Щоб налаштувати системний модуль DLP Forcepoint:

1. Перейти на сторінку Налаштування> Розгортання> Системні модулі в модулі захисту даних диспетчера безпеки Forcepoint.

2. Натиснути Модуль.

3. Вибрати поля, як показано у відповідному розділі нижче.

– Налаштування сервера управління DLP Forcepoint
– Налаштування сховища "відбитків пальців"
– Налаштування додаткового сервера DLP Forcepoint
– Налаштування сервера кінцевої точки
– Налаштування сканера
– Налаштування механізму політики
– Налаштування сервера OCR
– Налаштування протектора
– Налаштування ICAP
– Налаштування агента інтеграції
– Налаштування служб захисту
– Налаштування механізму аналітики
– Налаштування модуля Web Content Gateway
– Налаштування модуля захисту електронної пошти Forcepoint

Налаштування сховища "відбитків пальців"

Основне сховище “відбитків пальців” Forcepoint DLP зберігається на сервері управління. Первинний репозиторій створює вторинні сховища на екземплярах сервера Protector, Content Gate та Forcepoint DLP, а також на будь-якому іншому модулі із механізмом політики. Вони містять структуровані (бази даних) “відбитків пальців” і часто оновлюються, щоб залишатися актуальними. “Відбитків пальців” у файлі не зберігаються у вторинному сховищі, оскільки вони передаються в режимі реального часу.

Щоб налаштувати вибране сховище:

1. Ввести назву модуля.

2. Ввести Опис модуля (до 4000 символів).

3. Продовжити одне з наступного:

– Основне сховище відбитків пальців

– Вторинне сховище відбитків пальців

Основне сховище “відбитків пальців”

Під налаштування продуктивності:

1. Вибрати Максимальний простір на диску, виділений для використання сховищем відбитків пальців, у мегабайтах (50 000 МБ за замовчуванням).

2. Вибрати Максимальний розмір кешу для сховища відбитків пальців, який використовуватиметься для кешування відбитків пальців у пам'яті, у мегабайтах (512 МБ за замовчуванням).

3. Натиснути OK, щоб зберегти зміни та повернутися до сторінки Системні модулі.

Вторинне сховище “відбитків пальців"

Вторинні сховища “відбитків пальців" містять лише структуровані дані (відбитки в базі даних).

“Відбитки пальців” у файлі передаються в режимі реального часу, тому їх не потрібно зберігати в системних модулях, відмінних від сервера управління.

1. У розділі «Вибір сховища» використовуйте параметри в розділі «Виявити відбитки пальців», щоб вказати, де слід проводити виявлення “відбитків пальців”:

– Вибрати сховище, встановлене, щоб виконувати виявлення на пульті дистанційного керування сховище, а потім вибрати сервер, де знаходиться сховище. Зазвичай це основне сховище на сервері управління, але це може бути будь-яке сховище. Forcepoint рекомендує вибрати сховище в тій самій локальній мережі, що і ця. Коли вибрано основне сховище, адміністраторам ніколи не доведеться виконувати синхронізацію. Первинне сховище завжди в курсі останніх відбитків пальців.

– Вибрати це локальне сховище, щоб виявлення виконувалось локально. Якщо вибрано цей параметр, параметри налаштування продуктивності вмикаються.

Синхронізація відбувається лише тоді, коли це сховище не має найсвіжіших відбитків пальців.

2. Якщо вибрано локальне сховище, у розділі Налаштування продуктивності вибрати Максимальний розмір кешу (максимальний обсяг пам'яті), виділений для сховища “відбитків пальців”, у мегабайтах.

3. Вказати, чи існують періоди, коли вторинне сховище не слід оновлювати.

– За замовчуванням вторинні сховища постійно перевіряють наявність оновлень з основного (кожні 30 секунд). Це гарантує, що машина вторинного сховища завжди має найновіші відбитки пальців.

– Щоб виключити певний проміжок часу з цієї операції вводу-виводу, Вибрати Постійно, за винятком між, і вкажіть період відключення, наприклад: піковий робочий час.

Протягом цього періоду вторинне сховище не перевірятиме оновлення у первинного сховища. (Часи передбачаються в зоні сховища бази даних.

Налаштування модуля захисту електронної пошти DLP Forcepoint

Модуль захисту електронної пошти Forcepoint розміщений на приладі серії V. Він фільтрує вхідні, вихідні та внутрішні повідомлення електронної пошти щодо спаму та вірусів і використовує Forcepoint DLP для аналізу вмісту.

Модулі захисту електронної пошти включають механізм політики та вторинне сховище відбитків пальців. Щоб налаштувати ці компоненти, розгорнути модуль захисту електронної пошти на сторінці Системні модулі та Натиснути компонент.

Налаштування додаткового сервера DLP Forcepoint

Додаткові сервери DLP Forcepoint включають вторинне сховище відбитків пальців, сервер кінцевої точки, сканер, механізм політики та сервер OCR.

Щоб оновити модуль, відредагуйте такі поля:

1. За бажанням Ввести нове ім'я сервера DLP Forcepoint (до 128 символів).
2. Ввести новий Опис для сервера Forcepoint DLP (до 4000 символів).
3. Натиснути OK, щоб зберегти зміни та повернутися до сторінки Системні модулі.

Налаштування сервера кінцевої точки

Сервер кінцевої точки - це серверний компонент кінцевої точки Forcepoint DLP. Сервери кінцевих точок отримують інциденти від клієнтів кінцевих точок та надсилають параметри конфігурації.

Щоб налаштувати сервер кінцевої точки, Вибрати його на сторінці Системні модулі та заповніть поля наступним чином:

Вибрати або зніміть параметр Увімкнено, щоб увімкнути або вимкнути модуль.

1. За бажанням Ввести нову описову назву модуля (до 128 символів).
2. За бажанням Ввести корисний Опис модуля (до 4000 символів).

3. Ввести повне доменне ім’я модуля. Це потрібно, коли модуль розгортається поза мережею компанії.

4. Натиснути OK, щоб зберегти зміни та повернутися до сторінки Системні модулі.

На сторінці також відображаються тип модуля та ім’я хосту, які не можна змінити.

Налаштування сканера

Сканер - це агент, який виконує сканування виявленнь. У розгортанні DLP Forcepoint може бути кілька сканерів.

Щоб налаштувати сканер, вибрати його на екрані Системні модулі та заповніть поля наступним чином:

1. Ввести назву модуля (до 128 символів).

2. Ввести Опис модуля (до 4000 символів).

3. Натиснути OK, щоб зберегти зміни та повернутися до сторінки Системні модулі.

На сторінці також відображається тип модуля та повне доменне ім’я, які не можна змінити.

Налаштування механізму політики

Механізм політики відповідає за аналіз даних та використання аналітики для порівняння їх із правилами у політиках DLP Forcepoint. У розгортанні може бути кілька механізмів політики для управління великими обсягами транзакцій.

Щоб налаштувати екземпляри механізму політики, Вибрати його на екрані Системні модулі, а потім за допомогою сторінки редагування оновити наступні поля:

1. Вибрати або зніміть значення Доступний, щоб увімкнути модуль.

2. Ввести Опис модуля (до 4000 символів).

3. Додаткові сервери DLP Forcepoint включають сервер OCR, здатний перехоплювати текстові зображення багатьма мовами.

Вибрати Увімкнути OCR за допомогою, щоб увімкнути оптичне розпізнавання символів, а потім вибрати сервер OCR із розкривного списку.

– OCR за замовчуванням вимкнено.

– Для найкращої роботи Вибрати сервер OCR, який знаходиться найближче до механізму політики.

– Якщо сервер не встановлено, цей параметр не можна налаштувати.

4. Натиснути OK, щоб зберегти зміни та повернутися до сторінки Системні модулі.

Налаштування сервера OCR

Сервер OCR дозволяє системі аналізувати файли зображень, що надсилаються через мережеві канали, такі як вкладення електронної пошти та веб-повідомлення. Сервер визначає, чи є зображення текстовими, і якщо так, витягує та аналізує текст на делікатний вміст. Немає спеціального атрибута політики для налаштування оптичного розпізнавання символів (OCR). Якщо знайдено чутливий текст, зображення блокується або дозволяється відповідно до активних політик.

Щоб використовувати OCR, встановіть додатковий сервер Forcepoint DLP; сервер OCR автоматично включається в додаткові установки сервера DLP Forcepoint.

Щоб увімкнути аналіз OCR у вашій мережі:

1. Перейти на сторінку Налаштування> Розгортання> Системні модулі в модулі Захист даних Менеджера безпеки та відредагувати механізм політики на кожному сервері або агенті, який буде отримувати трафік, який потрібно проаналізувати.

2. У кожному вікні редагування вибрати Доступний OCR та вказати, який OCR-сервер (додатковий сервер Forcepoint DLP) використовувати для вилучення тексту із зображень.

Додавання OCR-сервера

Щоб додати OCR-сервер:

1. Ввести Опис модуля (до 4000 символів).

2. У розділі Точність вкажіть свій допуск на швидкість проти точності.

– вибрати Швидко, якщо у вас велика кількість зображень (рівень навантаження на ваш OCR-сервер буде великим), і ви стурбовані продуктивністю. Тільки великі зображення з інтенсивним текстом надсилаються для вилучення; невеликі зображення та документи, які не містять багато тексту, взагалі не витягуються. Цей параметр покращує продуктивність, але може погіршити точність.

– вибрати Точний, якщо у вас невелика кількість зображень (рівень навантаження на ваш OCR-сервер буде невеликим). Кожне текстове зображення у вашій мережі надсилається на сервер для вилучення. Це впливає на продуктивність, але забезпечує найточніші результати. Якщо відповідь неадекватна - наприклад, браузери очікують тайм-ауту на каналі HTTP - змініть це налаштування на Швидкий або Збалансований.

– вибрати Збалансований (за замовчуванням), щоб збалансувати точність та швидкість.

3. У розділі Мови вибрати мови, які можуть відображатися в текстових зображеннях. Деякі мови входять до складу Forcepoint DLP. Інші мови потребують окремого мовного пакету на сервері OCR.

Налаштування протектора: вкладка Локальні мережі

Вказати трафік, який захисник буде контролювати на вкладці «Локальні мережі». Вибрати:

– Включити усі мережі, підключені до мережі захисту.

– Включити певні мережі (за замовчуванням). Після вибору цієї опції:

1. Натиснути Додати, щоб визначити мережі.

2. Ввести мережеву адресу та маску підмережі.

Додані мережі відображаються в таблиці і можуть бути видалені або відредаговані за допомогою відповідних кнопок.

За замовчуванням вибрано "Включити певні мережі", і включені загальні списки IP-адрес, що не підлягають рухомості (відповідно до RFC1918): 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

– використовуючи цю опцію, переконайтесь, що всі внутрішні IP-адреси організації включені до цього списку.

– цей список дозволяє захиснику дізнатися, які зв'язки є вхідними, а які вихідними.

– ці мережі називаються "моїми мережами" при розгляді вхідних / вихідних / внутрішніх директив для різних каналів.

Якщо використовуються HTTP та SMTP у режимі моніторингу або SMTP у режимі MTA, обов'язково вибрати Включити певні мережі.

– додати всі внутрішні мережі для всіх сайтів.

– розглядати поштові сервери та поштові ретранслятори частиною внутрішньої мережі; цей список використовується для визначення напрямку руху.

Натиснути OK, щоб застосувати налаштування.

Налаштування механізму аналітики

Механізм аналітики використовується для розрахунку ризику інциденту, ранжування його за подібною діяльністю та присвоєння оцінки ризику. Щоб скористатися цією функцією, спочатку потрібно встановити механізм аналітики на 64-розрядному комп'ютері Linux.

Щоб налаштувати агент, вибрати його вузол на сторінці «Налаштування»> «Розгортання»> «Системні модулі» в модулі «Захист даних» Менеджера безпеки.

За бажанням оновити ім'я та опис модуля.

На сторінці конфігурації також відображається така інформація, яку неможливо змінити:

– Тип модуля

– FQDN (повне доменне ім'я) машини, на якій був встановлений модуль

– Версія модуля

Налаштування агента інтеграції

Агент інтеграції дозволяє стороннім продуктам надсилати дані до Forcepoint DLP для аналізу. Він вбудований у сторонні інсталятори та взаємодіє з Forcepoint DLP через API на основі C. (Агент інтеграції не підтримує виявлення транзакцій.)

Щоб змінити назву та опис модуля, вибрати вузол модуля на сторінці «Налаштування»> «Розгортання»> «Системні модулі» в модулі захисту даних диспетчера безпеки Forcepoint.

На сторінці конфігурації також відображається така інформація, яку неможливо змінити:

– Тип модуля

– FQDN (повне доменне ім'я) машини, на якій був встановлений модуль

– Версія модуля

4. Установка та налаштування Speech-to-text

1. Встановити Cloud Console на комп’ютер за допомогою GoogleCloudSDKInstaller.exe
2. Відкрити Cloud Console та в бібліотеці вибрати Speech-to-text
3. Перейти до меню налаштувань Speech-to-text
4. В пункті Шлях до вхідних даних вибрати папку де знаходяться файли,які потрібно конвертувати в текст
5. В пункті Шлях збереження даних вибрати папку куди зберігати конвертовані данні
6. В пункті Час перевірки встановити “Кожні 10 секунд”
7. Натиснути Готово

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

16 Додаток Д.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу магістра на тему:
“Методика виявлення порушень політики безпеки оператора call-центру при обробці запитів клієнта”

студента групи 125м-19-1
Ковриги Данила Андрійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __джерела та __ додатка.

Актуальність теми полягає в необхідності підвищення захищеності інформації з обмеженим доступом від витоку через порушення політики безпеки оператора call-центру.

Зміст та структура дипломної роботи дозволяють розкрити поставлену тему повністю.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. У роботі було розглянуто архітектуру call-центру, принципи роботи оператора call-центру, системи контролю оператора call-центру, архітектуру та принципи роботи DLP систем, виконано аналіз інформації, яка циркелює в call-центрі, аналіз загроз, визначений профіль захищеності та методи його реалізації, розроблена методика виявлення порушень політики безпеки оператора call-центру при обробці запитів від клієнта.

Це підтверджує самостійність обробки даних, практичні рекомендації та висновки.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому кваліфікаційна робота задовольняє усім вимогам і може бути допущена до захисту, а його автор ***Коврига Данило Андрійович*** заслуговує на оцінку «_____».

Керівник кваліфікаційної роботи,
к.т.н., доц. Флоров С.В.

Керівник спец. част.
ст. викл. Мєшков В.І.