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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Засоби захисту корпоративних інформаційних ресурсів»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Іван ОБРЕЖА
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
ОБРЕЖА Іван
(прізвище, ім'я)

Керівник к. держ.упр. СКИБУН Олександр
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент д.е.н., проф. ЛЕГОМІНОВА Світлана
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ВСТУП

Актуальність дослідження.

Перехід до цифровізації, став поштовхом до збільшення кіберзлоченів, які впливають на виконання всіх бізнес-процесів в організаціях. Складність і масштабованість таких кіберзлоченів, на основі нових методів та інструментів для викрадення даних, шантажу, саботажу та шпигунства полягають у застосуванні фішингових атак, програми-вимагачів (ransomware), DDoS-атак, інсайдерських атаки можуть вимагають від організацій вживають належних заходів безпеки, щоб не стати легкою мішенню для таких загроз.

Корпоративні інформаційні ресурси є одним з найцінніших активів для організацій. Це можуть бути фінансові дані, конфіденційна інформація про клієнтів, інтелектуальна власність, комерційна таємниця, особисті дані співробітників тощо. Витік або втрата таких даних може мати руйнівні наслідки, включаючи штрафи за порушення регулятивних норм (наприклад, GDPR), судові позови та значну втрату конкурентних переваг.

Кібератаки та витоки корпративної інформації можуть завдати фінансові шкоди (наприклад, витрати на відновлення систем, виплату викупу), але й серйозно вдарити по репутації організації. Втрата довіри клієнтів, партнерів та інвесторів може бути незворотною, що призведе до зниження прибутків і втрати частки ринку.

З переходом на гібридну та повністю віддалену модель роботи, периметр безпеки організації значно розширився. Співробітники працюють з різних пристроїв і мереж, що створює нові вразливості та вимагає комплексного підходу до захисту корпоративних інформаційних ресурсів, включаючи використання VPN, багатофакторної автентифікації, рішень для захисту від несанкціонованого витоку інформації.

Організації, які демонструють високий рівень захисту своїх корпоративних ресурсів, отримують конкурентну перевагу. Клієнти та партнери все більше

усвідомлюють ризики кібербезпеки та віддають перевагу співпраці з організаціями, які можуть гарантувати безпеку їхніх даних. Надійний захист також підвищує інвестиційну привабливість організацій.

Отже, захист корпоративних інформаційних ресурсів – це не просто технічна проблема, а стратегічне завдання, що вимагає постійної уваги та інвестицій. Комплексний підхід до кібербезпеки, що включає технологічні рішення, навчання співробітників, регулярні аудити та оновлення політик безпеки, є життєво важливим для сталого розвитку та успіху будь-якої організації. Тому дана робота буде присвячена дослідженню методів та засобів захисту корпоративних інформаційних ресурсів та розробці рекомендацій, які дозволять сфокусуватися фахівцям над даною проблемою.

Об’єкт дослідження – захист корпоративних інформаційних ресурсів.

Предмет дослідження – методи та засоби захисту корпоративних інформаційних ресурсів на основі Forcepoint DLP.

Мета роботи розробити варіант застосування методів та засобів захисту корпоративних інформаційних ресурсів на основі Forcepoint DLP та рекомендації щодо їх застосування.

Наукові завдання:

дослідити сутність проблеми корпоративних інформаційних ресурсів;

проаналізувати основні підходи захисту корпоративних інформаційних ресурсів;

проаналізувати існуючі рішення корпоративних інформаційних ресурсів;

проаналізувати методи та засоби захисту корпоративних інформаційних ресурсів на основі Forcepoint DLP;

запропонувати варіант застосування методів та засобів захисту корпоративних інформаційних ресурсів на основі Forcepoint DLP;

розробити рекомендацій щодо застосування методів та засобів захисту корпоративних інформаційних ресурсів.

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

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методи та засоби захисту корпоративних інформаційних ресурсів на основі Forcepoint DLP, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ

1.1. Визначення корпоративних ресурсів організації

Інформаційні ресурси — інформація, представлена у формі для зберігання, накопичення, оброблення та використання [1].

Для біль глибокого розуміння поняття корпоративних інформаційних ресурсів організації надаймо інше визначення.

Корпоративні інформаційні ресурси (КІР) — це сукупність усіх даних, інформації, знань, а також інформаційних систем, технологій та інфраструктури, які створюються, обробляються, зберігаються та використовуються організацією для досягнення своїх бізнес-цілей. Вони є одним з найцінніших активів будь-якої сучасної компанії, оскільки безпосередньо впливають на її функціонування, конкурентоспроможність, репутацію та фінансове становище.

До складу КІР входять не тільки цифрові дані, а й фізична інфраструктура, яка виконує процеси обробки, зберігання та передачі даних.

Важливо розуміти, що КІР охоплюють не лише цифрові дані, а й значну частину людського фактору та фізичної інфраструктури, що забезпечує їх існування.

Інфраструктуру будь-якої організації можна представити у вигляді складної системи (рис 1.1). До складу такої інфраструктури входить різне обладнання, таке як кінцеві точки, маршрутизатори, сервера та бази даних, які приймають участь в обробці, зберіганні та передачі інформаційних ресурсів. Архітектура є багатошаровою і на кожному рівні можуть бути задіяні різні ресурси і різні користувачі цих ресурсів. Отже надалі спробуємо визначити що входить до поняття інформаційних ресурсів організації.

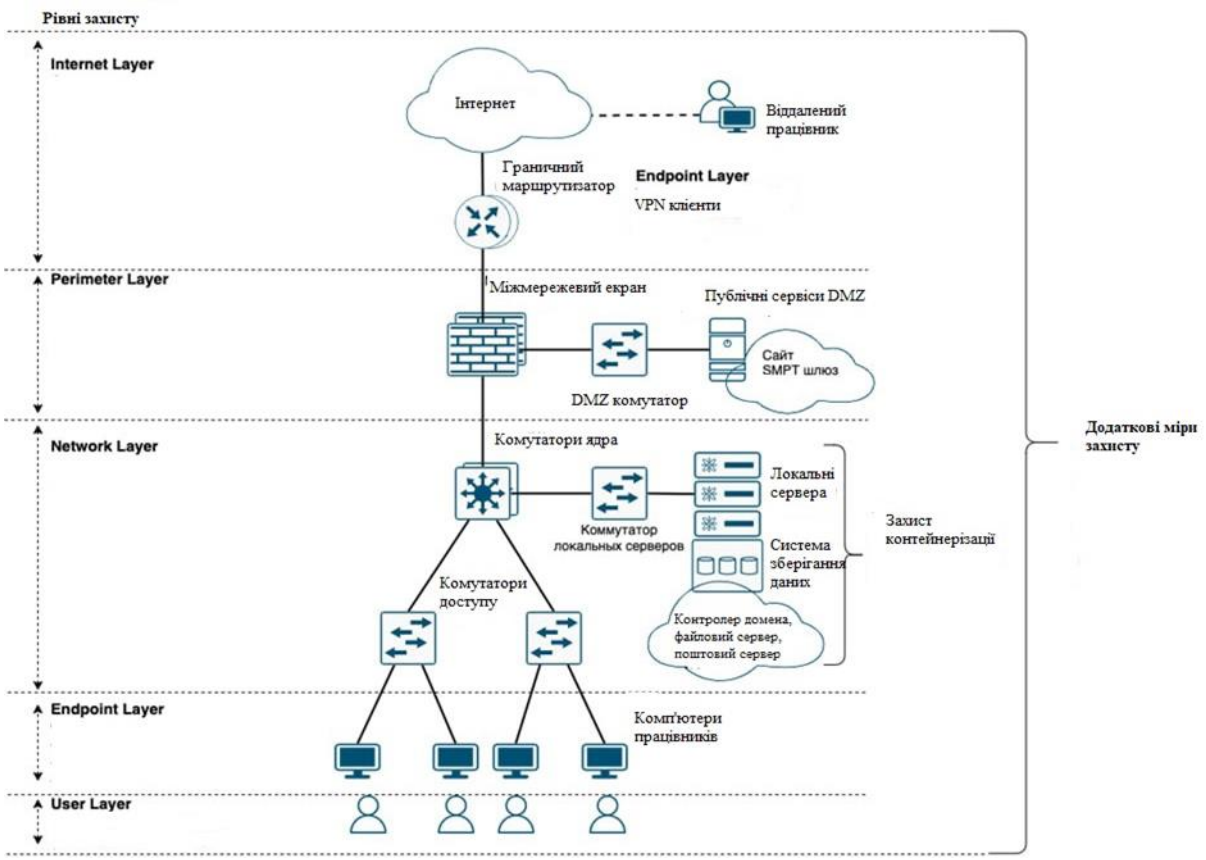

Рис.1.1. Архітектура інфраструктури організації

Типологія корпоративних інформаційних ресурсів

Корпоративні інформаційні ресурси можна класифікувати за різними критеріями, що допомагає систематизувати підходити до їх захисту. Основна класифікація і її типи показана на рис.1.2.

Рис.1.2. Класифікація інформаційних ресурсів

Надаймо більш широкий опис типів класифікації КІР.

1. За формою представлення

Дані (структуровані та неструктуровані):

Бази даних. Клієнтські дані, фінансові операції, запаси, дані про співробітників, виробничі показники тощо. Це можуть бути реляційні, NoSQL бази даних.

Файли. Документи (текстові, табличні, презентації), зображення, відео, аудіофайли, креслення, програмний код, електронні листи.

Архівні дані. Історичні записи, резервні копії, журнали подій.

Інформація. Опрацьовані та осмислені дані, що мають певну цінність та контекст. Це можуть бути звіти, аналітичні дослідження, бізнес-плани, маркетингові стратегії.

Знання: Кумулятивний досвід, експертиза, ноу-хау, інтелектуальна власність, методології, розробки та винаходи.

2. За місцем зберігання та обробки

На локальних серверах та робочих станціях. Дані, що зберігаються та обробляються безпосередньо в мережі компанії.

У хмарних сховищах (Public, Private, Hybrid Cloud). Дані, що розміщені на віддалених серверах постачальників хмарних послуг (наприклад, Google Cloud, AWS, Azure).

На мобільних пристроях Інформація, що зберігається на смартфонах, планшетах, ноутбуках співробітників.

На знімних носіях. USB-накопичувачі, зовнішні жорсткі диски, оптичні диски.

3. За функціональним призначенням

Операційні дані. Необхідні для повсякденної діяльності компанії (замовлення, транзакції, виробничі дані).

Стратегічні дані. Використовуються для довгострокового планування та прийняття ключових рішень (ринкові дослідження, аналіз конкурентів).

Регуляторні дані. Інформація, яку компанія зобов'язана зберігати та надавати відповідно до законодавчих та галузевих вимог (фінансові звіти, персональні дані

клієнтів).

Дані інтелектуальної власності. Патенти, торгові марки, авторські права, комерційні таємниці, алгоритми, формули.

4. За критичністю (рівнем чутливості).

Публічні дані. Інформація, яка не становить загрози у разі розкриття (наприклад, контактна інформація компанії).

Конфіденційні дані. Інформація, розкриття якої може завдати шкоди репутації або бізнесу (наприклад, дані про зарплати, внутрішні звіти).

Приватні (персональні) дані. Інформація, що стосується ідентифікованої або такої, що може бути ідентифікована, фізичної особи (наприклад, ПІБ, адреса, паспортні дані, медичні записи). Захист таких даних регулюється окремими законами (GDPR, HIPAA тощо).

Комерційна таємниця. Інформація, що має комерційну цінність через її конфіденційність і до якої застосовуються заходи щодо її захисту.

Цілком таємні/Секретні дані. Інформація найвищого рівня секретності, розкриття якої може мати катастрофічні наслідки для компанії.

5. За складовими інформаційної системи

Апаратне забезпечення. Сервери, робочі станції, мережеве обладнання (маршрутизатори, комутатори, точки доступу Wi-Fi), пристрої зберігання даних (NAS, SAN).

Програмне забезпечення. Операційні системи, офісні програми, корпоративні системи (ERP, CRM), антивіруси, системи управління базами даних, спеціалізоване галузеве ПЗ.

Мережі. Локальні обчислювальні мережі (LAN), глобальні обчислювальні мережі (WAN), Інтернет-з'єднання, бездротові мережі.

Інформаційні системи та додатки. Всі програмно-апаратні комплекси, що забезпечують обробку, зберігання та передачу інформації.

Людський фактор. Знання, навички та досвід співробітників, а також їхня обізнаність у питаннях інформаційної безпеки. Хоча це не "ресурс" у традиційному розумінні, людський фактор є критично важливим компонентом і може бути

джерелом як загроз, так і захисту.

Розуміння цієї типології дозволяє організаціям системно підходити до ідентифікації своїх активів, оцінки їхньої цінності та ризиків, а також розробки адекватних стратегій захисту для кожної категорії інформаційних ресурсів.

1.2. Аналіз загроз до інформаційних ресурсів організації

Основною загрозою для корпоративних інформаційних ресурсів організаціє є несанкціонований доступ, який може спричинити виток інформації. Такий вид загрози може спричинити негативні наслідки для виконання бізнес-процесів організації.

Витік інформації – це розголошення конфіденційних, захищених або чутливих даних у ненадійне середовище. Витік даних може статися в результаті хакерської атаки, внутрішніх інсайдерів, які зараз або раніше працювали в організації, або ненавмисної втрати чи розголошення даних [2].

Витоки даних можуть включати витік інформації, також відому як ексфільтрація — несанкціоноване копіювання або передача даних без впливу на вихідні дані. В інших випадках порушення призводять до повної втрати даних, як-от атаки програм-вимагачів , під час яких хакери шифрують дані, щоб заборонити власнику доступ до них [2].

Іншими словами, під час витоку даних хакери або співробітники розголошують або забирають конфіденційні дані. В результаті дані можуть бути втрачені або використані зловмисниками для різних зловмисних цілей [2].

Витік даних може призвести визначити для декількох типів інформації [2]:

Фінансові дані, такі як номери кредитних карток, банківські реквізити, податкові форми, рахунки-фактури, фінансові звіти.

Медична або особиста інформація про здоров’я (PHI) — згідно зі стандартом HIPAA, «інформація, створена медичним працівником стосується минулого, теперішнього або майбутнього фізичного чи психічного здоров’я чи стану будь-якої особи».

Особиста ідентифікаційна інформація (PII) — інформація, яка може бути використана для ідентифікації, зв’язку або визначення місцезнаходження особи.

Інтелектуальна власність — така як патенти, комерційні таємниці, креслення, списки клієнтів, контракти.

Вразлива та конфіденційна інформація (зазвичай військового чи політичного характеру) — така як записи або протоколи зустрічей, угоди, секретні документи.

Спираючись на останні дослідницькі звіти таких авторитетних компаній, як IBM, Verizon можна отримати останні данні щодо актуальної та достовірної статистики, яка допоможе організаціям отримати повне уявлення про поточний ландшафт загроз від несанкціонованого доступу та його наслідки для їхньої стратегії кібербезпеки [3].

Згідно з [3-5] найважливіші статистичні даних щодо витоків даних, полягають у наступному:

Прогнозується, що до 2025 року світові збитки від кіберзлочинності сягнуть 10,5 трильйона доларів, зростаючи на 15 відсотків щорічно.

Середня вартість витоку даних досягла історичного максимуму у 2024 році в 4,88 мільйона доларів, що на 10% більше, ніж у 2023 році.

Майже половина (46%) усіх порушень стосується персональних даних клієнтів, що можуть включати ідентифікаційні номери платників податків, електронні адреси, номери телефонів та домашні адреси.

Організаціям потрібно в середньому 204 дні, щоб виявити витік даних, і 73 дні, щоб його локалізувати.

Витрати на повідомлення про порушення зросли до 370 тисяч доларів у 2023 році, що на 19,4% більше, ніж у 2022 році.

Кібератаки з використанням викрадених або скомпрометованих облікових даних зросли на 71% у порівнянні з минулим роком.

74% усіх порушень включають людський фактор.

12% співробітників забрали з собою конфіденційну інтелектуальну власність, коли залишали організацію, включаючи дані клієнтів, дані співробітників, медичні записи та договори купівлі-продажу.

У 98% організацій є щонайменше один сторонній постачальник, який постраждав від витоку даних.

61% організацій використовують певний рівень безпеки, штучний інтелект та автоматизацію.

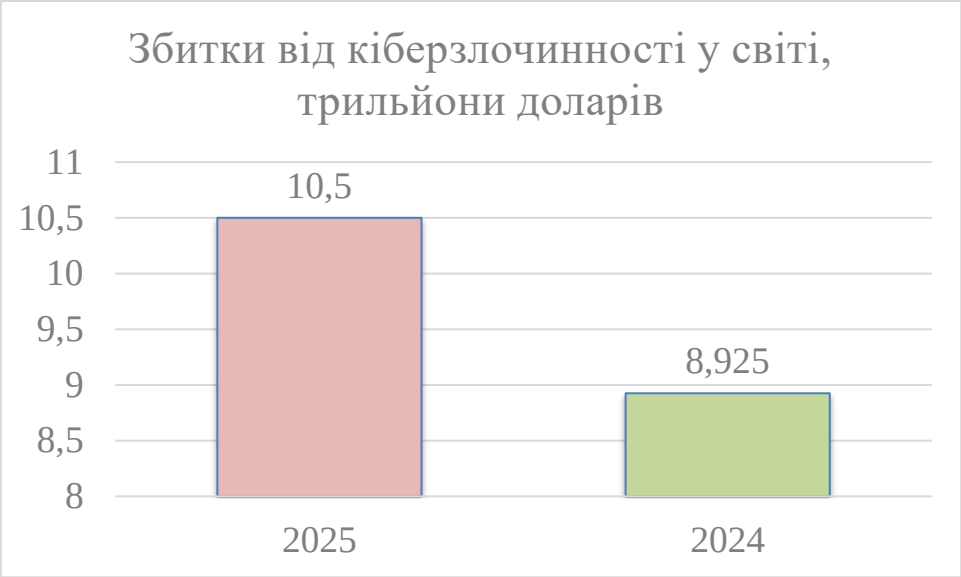

Рис. 1.3. Прогнозовані збитки від кіберзлочинності [4]

Розглянемо поширені причини витоку інформації в організаціях.

Витоки інсайдерської інформації

До внутрішніх загроз належать невдоволені співробітники, колишні співробітники, які досі зберігають облікові дані для доступу до конфіденційних систем, або ділові партнери. Вони можуть бути мотивовані фінансовою вигодою, комерційно цінною інформацією або бажанням помсти [2].

Шахрайство з оплатою

Шахрайство з оплатою – це спроба створити фальшиві або незаконні транзакції. Поширеними сценаріями є злом кредитної картки, що призводить до шахрайства, фальшиві повернення та шахрайство з тріангуляцією, коли зловмисники відкривають фальшиві інтернет-магазини з надзвичайно низькими цінами та використовують отримані платіжні дані для покупок у реальних магазинах [2].

Втрата або крадіжка

Організації зберігають конфіденційну інформацію на таких пристроях, як мобільні телефони, ноутбуки, флеш-накопичувачі, портативні жорсткі диски або навіть настільні комп'ютери та сервери. Будь-який із цих пристроїв може бути фізично викрадений зловмисником або ненавмисно втрачений співробітниками організації, що призведе до порушення безпеки [2].

Ненавмисне розголошення

Багато витоків даних спричинені не атакою, а ненавмисним розголошенням конфіденційної інформації. Наприклад, співробітники можуть переглядати конфіденційні дані та зберігати їх у незахищеному місці, або IT-персонал може помилково надати доступ до Інтернету на конфіденційному внутрішньому сервері [2].

Згідно визначення інсайдера, яке надає NIST 800-53 [6], яке визначає загрозу з боку інсайдера як «загрозу того, що інсайдер використає свій санкціонований доступ, свідомо чи несвідомо, для завдання шкоди безпеці операцій та активів організації, окремих осіб, інших організацій та країни» можна виділити три основні джерела внутрішніх загроз для організацій [7] (рис.1.4).

Рис.1.4. Джерела інсайдерських загроз [7]

Три джерела інсайдерських загроз:

– Недбалі або ненавмисні користувачі (Negligent or inadvertent users);

– Злочинні або зловмисні інсайдери (Criminal or malicious insiders);

– Зловмисники, які викрали облікові дані користувачів (Attackers that stole user credentials).

Внутрішні атаки особливо небезпечні з трьох основних причин: Інсайдери здебільшого не діють зловмисно. Саме тому виявити шкідливу діяльність інсайдерів важче, ніж зовнішні атаки. Інсайдери знають про слабкі місця в кібербезпеці вашої організації. Інсайдери знають місцезнаходження та характер конфіденційних даних, які вони можуть використати.

З цих причин інсайдерські атаки спрямовані саме на найчутливіші активи та потребують багато часу для їх стримування, що призводить до руйнівних втрат для організацій.

1.3. Аналіз підходів захисту інформаційних ресурсів організації

Для вибору засобів захисту корпоративних інформаціних ресурсів, розглянемо основні підходи, які дозволять зменшити ризики витоку від несанкціонованого доступу до інфраструктури організації.

Для ефективного захисту корпоративних інформаційних ресурсів використовуються різноманітні технічні рішення, кожне з яких спрямоване на протидію певним типам загроз та захист конкретних корпоративних інформаційних ресурсів організації (рис.1.5).

1. Антивірусні програмні засоби (Endpoint Protection Platforms – EPP, Endpoint Detection and Response – EDR).

EPP представляє собою традиційний підхід до захисту кінцевих точок (комп'ютерів, серверів) від відомих загроз, таких як віруси та шкідливі програми, за допомогою баз сигнатур.

EDR в свою чергу є більш сучасний підхід, який не лише виявляє, а й реагує на складні загрози в реальному часі, аналізуючи поведінку процесів та виявляючи аномалії, що свідчать про кібератаки, навіть якщо вони не мають відомих сигнатур.

Підхід. Захист кінцевих точок – це базовий рівень оборони, що фокусується на запобіганні проникненню шкідливого програмного забезпечення та реагуванні на інциденти безпосередньо на пристроях користувачів.

Рис. 1.5. Підходи до захисту корпоративних інформаційних ресурсів організації

2. Міжмережеві екрани (Firewalls) та системи виявлення/запобігання вторгнень (Intrusion Detection/Prevention Systems – IDS/IPS).

Міжмережеві екрани контролюють мережевий трафік, дозволяючи або блокуючи його на основі встановлених правил. Це перша лінія оборони на межі мережі організації.

IDS виявляють підозрілу активність та вторгнення, але не блокують їх, а тільки сповіщають про загрозу.

IPS, в свою чергу, не тільки виявляють, а й активно блокують виявлені вторгнення та атаки в реальному часі.

Підхід: Мережевий захист та моніторинг трафіку – це стратегія, яка спрямована на контроль доступу до внутрішньої мережі, виявлення та блокування

небажаної або шкідливої активності на мережевому рівні, що допомагає запобігти несанкціонованому доступу та розповсюдженню загроз.

3. Системи управління ідентифікацією та доступом (Identity and Access Management – IAM).

IAM дозволяють ефективно управляти обліковими даними користувачів (співробітників, клієнтів, партнерів) та їхніми правами доступу до корпоративних ресурсів. Вони забезпечують, щоб правильні користувачі мали доступ до правильних ресурсів у правильний час.

Підхід: Контроль доступу та управління правами – це централізована система, яка гарантує, що лише автентифіковані та авторизовані користувачі можуть отримати доступ до визначених ресурсів, зменшуючи ризик несанкціонованого використання або витоку інформації.

4. Шифрування даних (data encryption). Шифрування перетворює інформацію на нечитабельний формат, доступний лише для авторизованих осіб, які мають ключ дешифрування. Застосовується для захисту даних у стані спокою (на дисках) та в русі (під час передачі).

Підхід. Захист конфіденційності та цілісності даних – це криптографічний метод, що забезпечує неможливість прочитання або модифікації інформації сторонніми особами, навіть якщо вони отримали доступ до зашифрованих даних.

5. Засоби захисту веб-додатків (Web Application Firewalls – WAF).

WAF захищають веб-додатки від специфічних атак на рівні додатків (наприклад, SQL-ін'єкції, міжсайтовий скриптинг – XSS), які не можуть бути ефективно заблоковані звичайними міжмережевими екранами.

Підхід. Спеціалізований захист веб-ресурсів – це рішення, що фокусується на унікальних вразливостях веб-додатків, які часто є точкою входу для зловмисників, забезпечуючи захист від складних атак, спрямованих саме на програмний код.

6. VPN-технології (Virtual Private Network).

VPN створюють зашифрований тунель через загальнодоступну мережу (Інтернет), забезпечуючи безпечний та конфіденційний зв'язок між користувачами

або мережами. Це дозволяє віддаленим співробітникам безпечно підключатися до корпоративної мережі.

Підхід. Безпечний віддалений доступ та конфіденційність передачі – це метод, що дозволяє користувачам працювати з корпоративними ресурсами з будь-якої точки світу, забезпечуючи захист даних під час їх передачі через незахищені мережі.

7. Системи запобігання витокам даних (Data Loss Prevention – DLP).

DLP-системи моніторять, виявляють та запобігають несанкціонованій передачі конфіденційних даних за межі корпоративної мережі, чи то через електронну пошту, хмарні сховища, знімні носії або інші канали.

Підхід. Контроль та запобігання несанкціонованому розголошенню – це технологія, яка допомагає уникнути витоку конфіденційної інформації шляхом відстеження, фільтрації та блокування передачі чутливих даних відповідно до визначених політик безпеки.

Ці технічні засоби, працюючи разом та доповнюючи один одного, формують багатошарову систему захисту корпоративних інформаційних ресурсів організації, яка є ключовим елементом сучасної стратегії кібербезпеки.

Отже, для подальшого дослідження виберемо DLP-системи запобігання витокам даних, які зможуть запобігти несанкціонованій передачі даних, але активно інтегрують UEBA (User and Entity Behavior Analytics), що дозволитяє розширити свій функціонал у бік більш широкої платформи безпеки корпоративних інформаційних ресурсів з боку внутрішніх інсайдерів.

1.4. Аналіз існуючих засобів захисту інформаційних ресурсів організації

Важливо зазначити, що ринок рішень з кібербезпеки дуже динамічний, і функціонал продуктів постійно оновлюється. Ця таблиця відображає загальні сильні сторони та орієнтацію кожного рішення [8-12].

Порівняння для вибору рішення буде проводитись для трьох варіантів рішень, а саме DLP-рішень: Forcepoint, Symantec (Broadcom придбав Symantec

Enterprise Security у 2019 році, тому "Symantec DLP" тепер є частиною портфоліо Broadcom), Proofpoint.

Таблиця 1.1.

Порівняльна таблиця провідних DLP-рішень

Критерій	**Forcepoint DLP**	**Symantec DLP (Broadcom)**	**Proofpoint Enterprise DLP**
Основна спеціалізація	Комплексна безпека даних, орієнтована на людину (human-centric security), поведінковий аналіз (UEBA).	Традиційно потужний захист даних на кінцевих точках, мережі та зберіганні.	Захист електронної пошти та хмарних додатків, фокус на інсайдерських загрозах та навчанні користувачів.
Покриття ресурсів організації	Кінцеві точки, мережа, хмара (SaaS, IaaS), веб, електронна пошта, USB, принтери.	Кінцеві точки, мережа, хмара (SaaS, IaaS), веб, електронна пошта, USB, принтерию	Електронна пошта, хмара (Microsoft 365, Google Workspace, Salesforce), веб, кінцеві точки (менш глибоко, ніж інші).
Виявлення та класифікація даних	Висока точність, запатентована технологія "відбитків пальців" (fingerprinting), AI/ML для зниження хибних спрацьовувань. Понад 1700+ вбудованих класифікаторів.	Глибокі технології виявлення: Exact Data Matching (EDM), Indexed Document Matching (IDM), Described Content Matching (DCM), Sensitive Image Recognition (OCR).	Точне виявлення чутливого вмісту, підтримка Exact Data Matching (EDM), понад 80+ вбудованих шаблонів політик.

Продовження таблиці 1.1

Захист від інсайдерів	Сильний акцент на поведінковому аналізі користувачів (UEBA) для виявлення ризикованої поведінки та інсайдерських загроз.	Досвідчена функціональність виявлення інсайдерських загроз, моніторинг поведінки користувачів на кінцевих точках.	Дуже сильний, особливо в контексті електронної пошти та хмари, фокусується на людському факторі та навчанні (Human-Centric Security).
Управління та моніторинг	Централізована консоль управління, яка прагне уніфікувати управління політиками та інцидентами по всіх каналах.	Єдина консоль для управління політиками та інцидентами, гнучкі можливості звітності. Може бути дещо застарілою у порівнянні з новішими інтерфейсами.	Єдина, інтуїтивно зрозуміла консоль для управління сповіщеннями та розслідуваннями інцидентів. Добре інтегрована з іншими продуктами Proofpoint.
Інтеграція з IAM	Інтеграція можлива через API, але зазвичай фокус на даних та поведінці, а не на прямому управлінні ідентифікацією.	Інтеграція з IAM-системами для контекстуалізації подій безпеки на основі ідентичності та привілеїв користувача.	Інтеграція з основними IAM-платформами (наприклад, Okta, Microsoft), щоб посилити контекст для політик DLP та інцидентів.
Хмарне покриття	Потужна хмарна DLP (Data Security Cloud), включаючи захист SaaS-додатків (Microsoft 365, Google Drive, Slack, GitHub) та IaaS.	Підтримує як локальне, так і гібридне розгортання, з можливістю захисту хмарних додатків (Office 365, G-Suite, Box, Salesforce).	Сильні можливості для хмарних додатків (Microsoft 365, Google Workspace, Salesforce) та електронної пошти як SaaS-сервісу.
Цільова аудиторія	Великі підприємства, з акцентом на поведінці користувачів та хмарну безпеку.	Великі корпорації та організації з високими вимогами до захисту даних на всіх рівнях та зрілими IT-процесами.	Компанії, для яких критично важливий захист електронної пошти та даних у хмарних додатках. пов'язаними з персоналом.

Отже, зробимо загальний висновок.

Forcepoint виділяється своїм акцентом на людському факторі та поведінковому аналізі, що робить його сильним вибором для виявлення складних інсайдерських загроз та захисту даних у динамічних хмарних середовищах.

Symantec (Broadcom) пропонує найбільш глибоке, більше покриття каналів та точне виявлення даних, що ідеально підходить для великих, складних корпоративних інфраструктур.

Proofpoint є лідером у сфері захисту електронної пошти та хмарних даних, інтегруючи DLP у свою ширшу платформу Human-Centric Security, що робить його відмінним вибором для компаній, де ці канали є основними точками витоку інформації.

Для подальшого дослідження, було обрано рішення Forcepoint, як таке що пропонує захист у хмарних середовищах та забезпечує повний контроль інформаційних ресурсів організації.

2 МЕТОДИ ТА ЗАСОБИ КОРПОРАТИВНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ

2.1. Архітектура Forcepoint DLP

Архітектура Forcepoint DLP є комплексною системою і використовується для виконання наступних завдань [13]:

1. Веб-безпека Forcepoint та фільтрація URL-адрес Forcepoint.
2. Захист від пошкоджень Forcepoint.
3. Безпека електронної пошти Forcepoint.
4. Прилади Forcepoint.

Forcepoint Web Security, Forcepoint Email Security та Forcepoint DLP можна розгортати разом для створення комплексного рішення безпеки.

Forcepoint Security Manager представляє собою інтерфейс керування для розширених рішень захисту веб-сайтів, даних та електронної пошти, розташований на сервері Windows.

Forcepoint Web Security можна розгорнути на пристроях Forcepoint, виділених серверах Windows або Linux, або на комбінації платформ.

Forcepoint DLP працює на серверах Windows, додаткових пристроях та в інших місцях мережі. Деякі компоненти працюють у хмарних інфраструктурах, таких як Microsoft Azure.

Компоненти Forcepoint Email Security використовують для забезпечення дотримання правил, які знаходяться на пристроях Forcepoint або в Microsoft Azure. Компоненти керування та звітності знаходяться на серверах Windows. Починаючи з версії 8.5.3, компоненти керування та звітності можна розгортати в Microsoft Azure.

Архітектура Forcepoint DLP розгортання рішення високого рівня показано на рис.2.1.

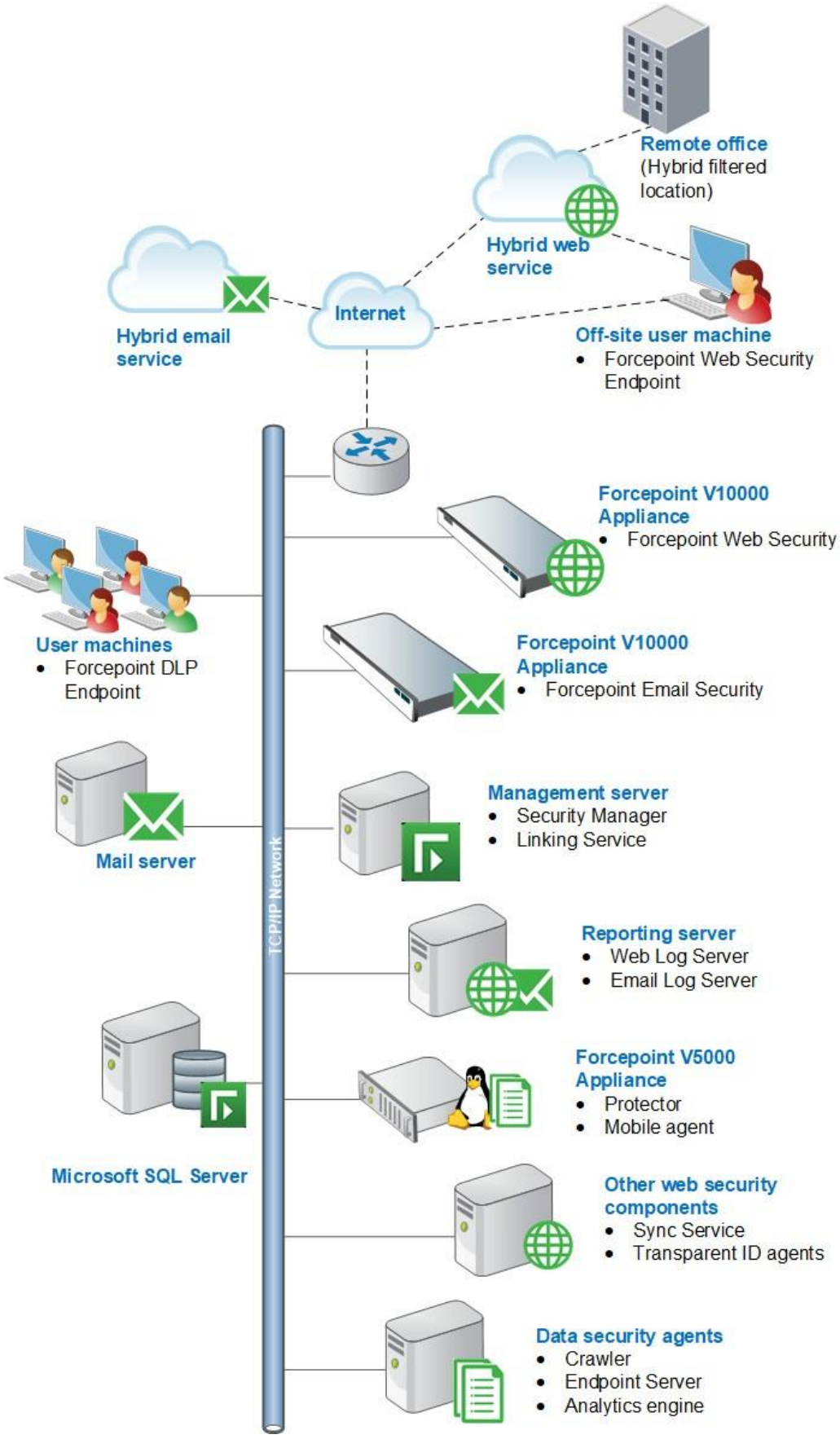

Рис.2.1. Архітектура Forcepoint DLP [13]

Зображена архітектура Forcepoint DLP представляє віддалений офіс та користувачів поза офісом.

Для невеликих організацій можна використовувати гібридний модуль Forcepoint Web Security для забезпечення веб-безпеки. Це досягається шляхом призначення віддаленого офісу як гібридного фільтрованого розташування.

Гібридний сервіс також може забезпечувати веб-безпеку для користувачів, які працюють з дому, подорожують тощо.

Запити користувачів можна спрямовувати до гібридної служби за допомогою PAC-файлу або клієнтського програмного забезпечення кінцевої точки. Це дозволяє гібридній службі аналізувати веб-запити та застосовувати політики.

Для організацій, які використовують гібридний модуль Forcepoint Web Security та Forcepoint Email Security надаються наступні гібридні послуги [13]:

1. Хмарний гібридний веб-сервіс може забезпечити інтернет-безпеку для віддалених офісів та користувачів, які перебувають за межами офісу.

2. Гібридний хмарний сервіс електронної пошти забезпечує додатковий рівень сканування електронної пошти, зупиняючи спам, віруси, фішинг та інші атаки шкідливого програмного забезпечення, перш ніж вони досягнуть вашої мережі, та, можливо, зменшуючи вимоги до пропускної здатності та сховища електронної пошти.

2.2. Функції Forcepoint Web Security Cloud

Forcepoint Web Security Cloud працює як проксі-сервер для HTTP та HTTPS-трафіку, а також FTP через HTTP. Коли користувачі запитують веб-ресурс, їхні браузери не підключаються безпосередньо до веб-серверів Інтернету (показаних на рис. 2.2. як сервери походження), а натомість підключаються до хмарного проксі-сервера, який, у свою чергу, передає запити на сервер походження. Це дозволяє хмарному сервісу застосовувати правила фільтрації та виконувати сканування контенту, забезпечуючи захист від загроз безпеці, втрати даних та неприйнятного контенту [14].

Служба може використовувати різні методи для ідентифікації та автентифікації користувачів: клієнт Forcepoint Endpoint, сторонній постачальник ідентифікації єдиного входу, прозору ідентифікацію NTLM або ручну автентифікацію за допомогою імені користувача та пароля. Користувачів у роумінгу (тих, хто підключається з невідомої IP-адреси) можна ідентифікувати через клієнт Forcepoint Endpoint, через постачальника єдиного входу, або ж від них потрібно буде пройти автентифікацію [14].

Додаткове шифрування SSL дозволяє сканувати вміст сеансів HTTPS і дозволяє сервісу показувати користувачам правильну сторінку сповіщень (наприклад, сторінку блокування, якщо сайт SSL належить до категорії блокування). Після перевірки вміст повторно шифрується [14].

На наступному рисунку показано базовий огляд веб-трафіку, захищеного Forcepoint Web Security Cloud.

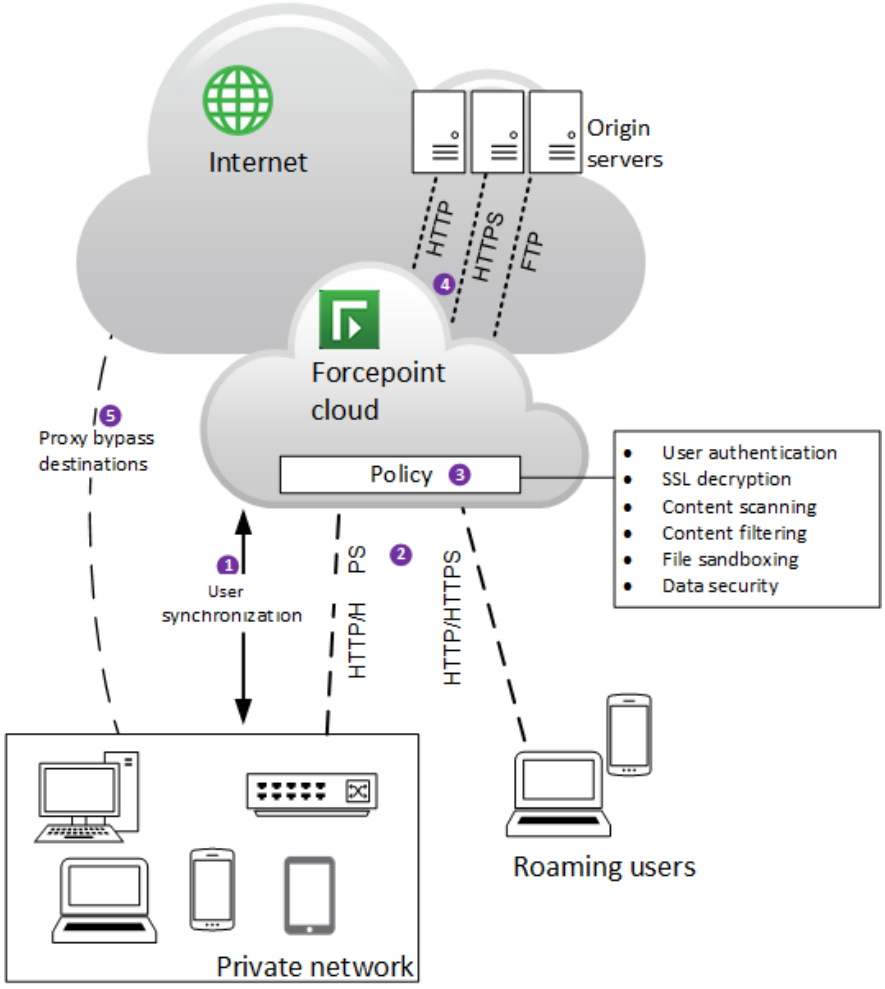

Рис. 2.2. Forcepoint Web Security Cloud [14]

На Рис. 2.2. показано наступні елементи сервісу.

1. Керування ідентифікацією дозволяє синхронізувати дані користувачів із хмарою, що дозволяє ідентифікувати та автентифікувати користувачів. Це дозволяє застосовувати налаштування політик на рівні користувачів і груп, а також надавати детальну звітність на рівні користувачів[14].

2. Веб-трафік спрямовується до хмарного сервісу з приватної мережі та від користувачів роумінгу, які підключаються з-за меж своєї локальної мережі [14].

3. Налаштування автентифікації, фільтрації та примусового виконання застосовуються політикою, яка визначає, які запити дозволяти або блокувати, виконує сканування вмісту в режимі реального часу та застосовує фільтрацію безпеки даних, допомагаючи запобігти ненавмисній або зловмисній втраті даних [14].

4. Після застосування рішень щодо політики веб-запити пересилаються на сервер-джерело, а контент доставляється до браузера користувача. Якщо контент заблоковано або виявлено загрози безпеці, відображаються налаштовувані сторінки сповіщень, які інформують користувача про причину заборони доступу до ресурсу[14].

5. Деякі веб-запити можуть надсилатися безпосередньо на сервер-джерело, якщо адреса визначена як адреса для обходу проксі-сервера [14].

Захищені сеанси (HTTPS) пересилаються через тунельоване з’єднання. Якщо ввімкнути SSL-шифрування, вміст цих сеансів можна буде сканувати, а параметри політики застосовувати до повторного шифрування трафіку. Ця функція вимагає встановлення кореневого сертифіката на комп’ютерах кінцевих користувачів, що дозволить клієнтам безпечно підключатися до хмарного проксі-сервера.

Щоб розпочати роботу з сервісом, потрібно налаштувати переадресацію веб-трафіку до сервісу, додати користувачів до сервісу (за потреби) та створити політики для керування веб-доступом (політика за замовчуванням попередньо налаштована).

Щоб сервіс міг виконувати фільтрацію, потрібно перенаправити веб-трафік до хмарного сервісу та налаштувати брандмауер, щоб дозволити доступ до сервісу через певні порти.

Трафік можна спрямовувати до хмарного сервісу кількома способами:

– кінцева точка Forcepoint - легкий програмний клієнт, який працює на пристроях кінцевих користувачів і забезпечує дотримання політик для перегляду веб-сторінок.

– файл PAC (автоматичної конфігурації проксі-сервера) браузера - скрипт конфігурації, який можна налаштувати в браузерах ваших користувачів (через GPO або подібний об'єкт) для перенаправлення запитів браузера до сервісу.

– перенаправлення брандмауера - простий метод, реалізований на брандмауері, для перенаправлення всього HTTP/HTTPS-трафіку до сервісу.

– тунелювання - підключення IPsec або GRE для переадресації трафіку до служби з підтримуваного периферійного пристрою.

Сервіс може ідентифікувати та автентифікувати користувачів, щоб забезпечити дотримання політик для окремих користувачів та груп, а також детальну звітність про активність користувачів. Користувачів можна додавати вручну або налаштувати керування ідентифікацією таким чином, щоб дані користувачів автоматично оновлювалися в хмарному сервісі.

Політики дозволяють або блокують доступ до веб-ресурсів, а також контролюють налаштування автентифікації, фільтрації контенту, безпеки та запобігання втраті даних. Винятки можна налаштувати для заміни або обходу налаштувань політик для кожного користувача або групи.

Фільтрація базується на наборі веб-категорій, взятих з бази даних URL-адрес Forcepoint, яка постійно оновлюється Forcepoint Security Labs, а загрози безпеці виявляються в режимі реального часу за допомогою Forcepoint ThreatSeeker Intelligence.

Доступна політика за замовчуванням, яка надає набір стандартних налаштувань веб-фільтрації. Після налаштування служби ви можете редагувати цю

політику та створювати нові, забезпечуючи різні рівні доступу для різних користувачів і відділів.

2.3. Функції та призначення Forcepoint Email Security

Forcepoint Email Security застосовується для:

– безпеки електронної пошти Forcepoint;

– прилади Forcepoint.

Forcepoint Email Security забезпечує максимальний захист поштових систем, запобігаючи проникненню шкідливих загроз у мережу організації. Forcepoint Email Security забезпечує комплексний захист, розміщений на фізичному або віртуальному пристрої Forcepoint, або в хмарному середовищі Microsoft Azure. Функції керування поштовою системою розташовані на окремому сервері Windows у Forcepoint Security Manager. Схеми підключення Forcepoint Email Security мають два варіанта:

– яким потрібен лише захист даних у каналі вихідної електронної пошти;

– з захистом вхідної і вихідної електронної пошти.

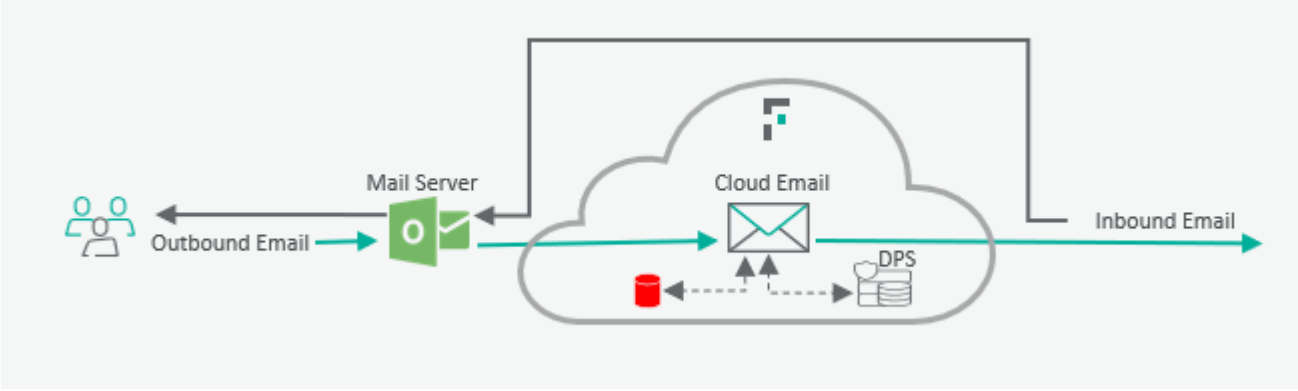

Рис. 2.3. Forcepoint Email Security, яким потрібен лише захист даних у каналі вихідної електронної пошти

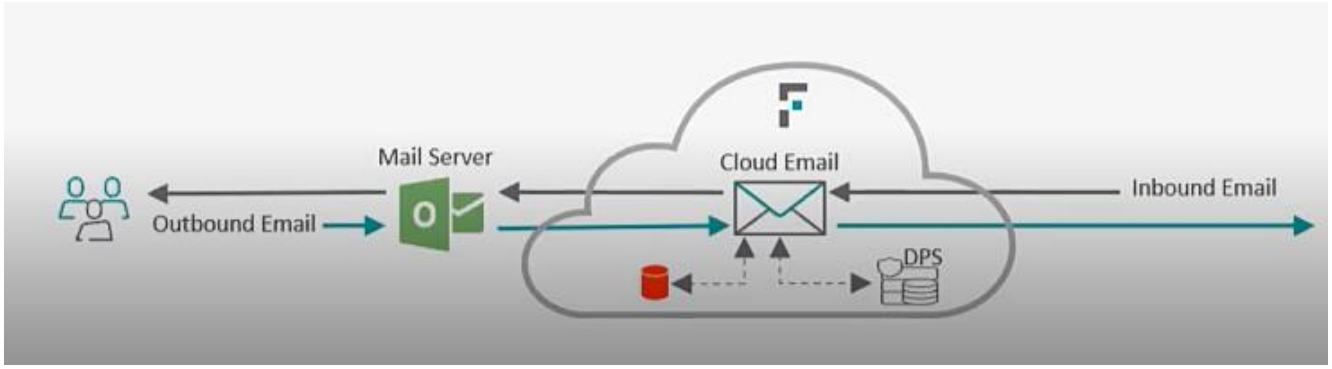

Рис. 2.4. Forcepoint Email Security, з захистом вхідної і вихідної електронної пошти

Forcepoint Email Security можна розгорнути на таких пристроях:

– Серія Forcepoint V;
– Віртуальний пристрій;
– Віртуальний пристрій Microsoft Azure.

Розгортання віртуального пристрою використовує платформу VMware (ESXi v6.x). Образ пристрою доступний для завантаження на сторінці «Мій обліковий запис» Forcepoint у пакеті відкритого формату віртуалізації. Віртуальний пристрій не може бути кластеризований з апаратним пристроєм.

Принцип роботи Forcepoint Email Security Forcepoint Email Securityполягає у виконання наступних функцій.

Кожне електронне повідомлення обробляється надійним набором аналітичних засобів, щоб запобігти потраплянню шкідливих загроз у мережу. Налаштовувані фільтри вмісту дозволяють Forcepoint Email Security аналізувати повідомлення на основі умов атрибутів, визначених адміністратором. Аналіз комерційної масової розсилки електронної пошти може визначити, чи було повідомлення надіслано від сторонньої компанії з управління масовою розсилкою електронною поштою, чи безпосередньо від бізнесу. Політики вхідної, вихідної та внутрішньої електронної пошти можна застосовувати до визначених користувачем наборів відправників та одержувачів.

У хмарі знаходяться лише компоненти Forcepoint Email Security; функції керування системою електронної пошти залишаються локальними. Для розгортання Forcepoint Email Security в Azure потрібен активний обліковий запис

Azure та віртуальна мережа в Azure з підключенням типу "сайт-сайт" до локальних ресурсів.

Як Email Security, так і Security Manager знаходяться в хмарі, без жодних функцій локально. Для розгортання Forcepoint Email Security та Forcepoint Security Manager в Azure потрібен активний обліковий запис Azure.

Деякі пристрої Forcepoint Email Security знаходяться в хмарі, а деякі встановлені локально. Forcepoint Security Manager можна розгорнути або в Azure, або локально. Для розгортання потрібен активний обліковий запис Azure та віртуальна мережа в Azure з підключенням типу "сайт-сайт" до локальних ресурсів.

Включення гібридного модуля Forcepoint Email Security у ваше розгортання додає підтримку для можливості попередньої фільтрації гібридної служби електронної пошти в хмарі, яка аналізує характеристики вхідної електронної пошти на основі бази даних Forcepoint про відомі загрози.

Forcepoint Email Security надає можливість підвищити безпеку організації, додавши до своєї підписки набір хмарних функцій:

– URL-пісочниця;

– розширений аналіз файлів;

– освіта з питань фішингу;

– функція URL-пісочниці забезпечує аналіз URL-адрес без категорії, вбудованих у вхідну пошту, у режимі реального часу.

Розширені можливості аналізу файлів можна розгорнути одним із двох способів:

– розширене виявлення шкідливого програмного забезпечення Forcepoint – хмара;

– розширене виявлення шкідливих програм Forcepoint – локальне.

Розгортання розширеного аналізу файлів перевіряє типи файлів вкладень електронної пошти, які зазвичай містять загрози безпеці (наприклад, .exe, .pdf, .xlsx, .docx, .ppt та архівні файли).

Навчання фішинговим повідомленням забезпечує хмарний аналіз вхідного повідомлення на наявність характеристик фішингової електронної пошти. Варіанти обробки підозрілої фішингової пошти включають блокування доставки або заміну листа повідомленням з інформацією про фішинг.

Можливо підвищити безпеку шляхом додавання модулю шифрування електронної пошти Forcepoint Email Security до своєї підписки, щоб використовувати розширені можливості шифрування електронної пошти Forcepoint разом із гібридним сервісом електронної пошти [14].

Інтеграція з Forcepoint DLP надає цінні функції запобігання втраті даних (DLP) для захисту найчутливіших даних організації та спрощення шифрування повідомлень. Політики, налаштовані в модулі безпеки даних Security Manager, можуть виявляти наявність конфіденційних даних компанії та блокувати несанкціоновану передачу цих даних електронною поштою. Forcepoint DLP також може визначати, чи слід шифрувати вихідне повідомлення, та передавати його на сервер шифрування [14-15].

Якщо ваша мережа включає Forcepoint Web Security або Forcepoint URL Filtering, ви також можете використовувати функцію аналізу URL-адрес. Forcepoint Email Security запитує головну базу даних категорій URL-адрес Forcepoint і визначає рівень ризику URL-адреси, знайденої в електронному листі.

Можливості ведення журналу та звітності дозволяють організації переглядати стан системи та повідомлень, а також створювати звіти про активність системи та трафіку електронної пошти.

Функція «Персональний менеджер електронної пошти» дозволяє авторизованим кінцевим користувачам випускати електронні листи, заблоковані політикою електронної пошти, але які можна безпечно доставити. Кінцеві користувачі можуть створювати особисті списки адрес електронної пошти «Завжди блокувати» та «Завжди дозволяти» для спрощення доставки повідомлень. Можливості керування обліковими записами користувачів дозволяють керувати кількома обліковими записами електронної пошти та делегувати це управління іншим особам.

Функція безпечної доставки повідомлень дозволяє налаштувати параметри доставки для безпечного порталу, на якому клієнти вашої організації можуть переглядати, надсилати та керувати зашифрованою електронною поштою. Наприклад, ви можете захотіти включити конфіденційну особисту фінансову інформацію в повідомлення клієнту. Портал забезпечує безпечне місце для передачі цих даних, тоді як ваша конфіденційна інформація зберігається на вашому захищеному сервері.

Системні вимоги та варіанти розгортання Forcepoint Email Security:

1. Розгортання Forcepoint Email Security на одному пристрої;
2. Розгортання Forcepoint Email Security на кількох пристроях.

2.4. Функції та призначення Forcepoint NGFW

Центр керування безпекою Forcepoint NGFW забезпечує єдине, централізоване адміністрування всіх моделей брандмауерів Forcepoint Next Generation Firewall. Центр керування безпекою Forcepoint працює на всіх платформах: фізичних, віртуальних або хмарних, у розширених та географічно розподілених середовищах[16].

Брандмауер Forcepoint (NGFW) нового покоління спеціально розроблений для централізованого адміністрування в розподілених мережах. Тому за допомогою Forcepoint NGFW Security Management Center (SMC) можна налаштовувати, контролювати та оновлювати до 2000 пристроїв Forcepoint NGFW з однієї панелі. Це стосується фізичних, віртуальних та хмарних пристроїв [16].

SMC спрощує відображення бізнес-процесів в автоматизовані засоби контролю безпеки. Ці засоби контролю успішно інтегрують конфігурацію VPN, IPS, SD-WAN, критично важливих проксі-серверів додатків та інших функцій безпеки. В результаті ви можете оновлювати політики за лічені секунди та впроваджувати їх у всій корпоративній мережі одним клацанням миші [16].

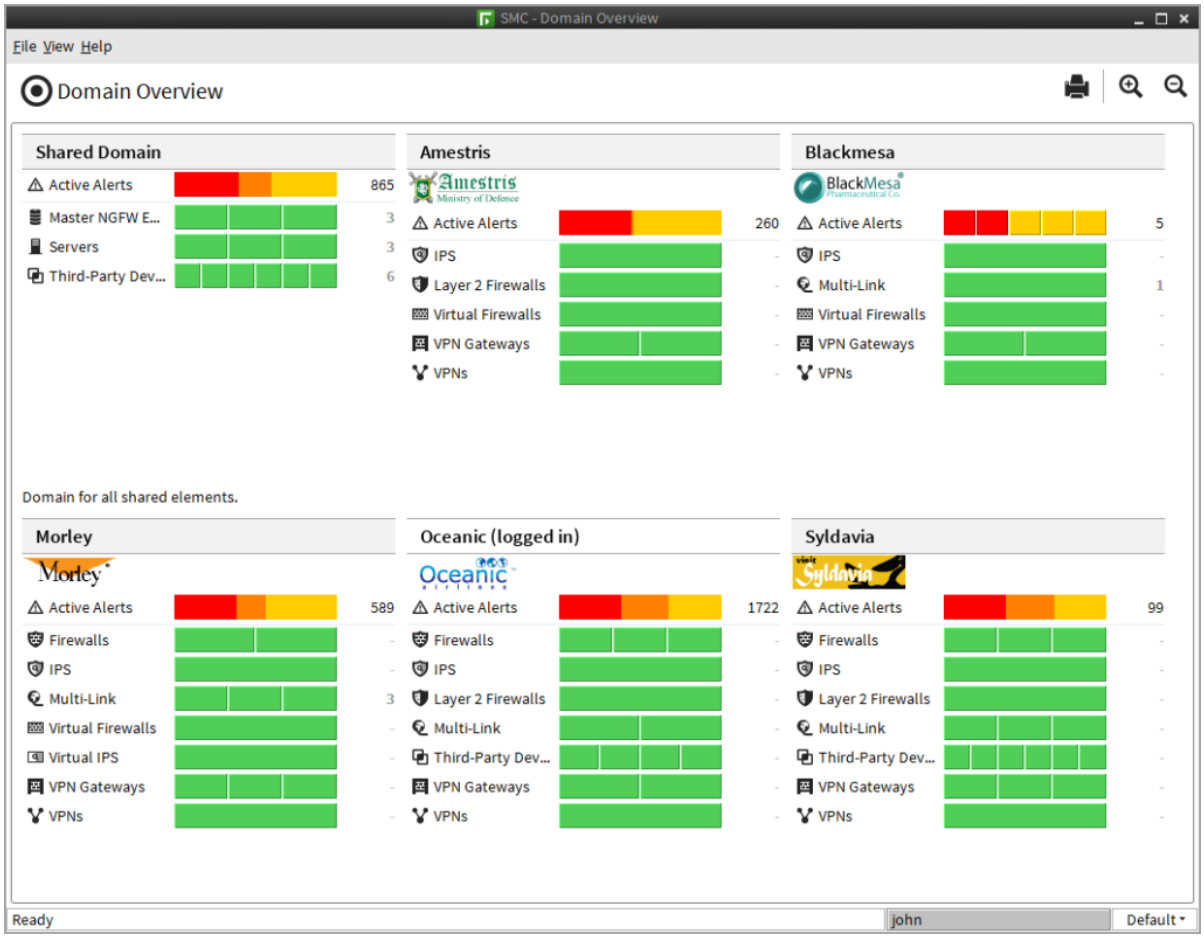

Рис.2.5. Менеджер управління Forcepoint NGFW

При виборі рішень для управління безпекою дуже важливими є їхня простота та швидкість роботи. Великі мережі вимагають команди архітекторів, впроваджувачів, адміністраторів, тестувальників, аналітиків та технічних спеціалістів. Вони забезпечують безперервність бізнесу та оптимальне налаштування середовища. Великі команди тягнуть за собою величезні витрати. Однак іноді різні ролі можуть бути на одних і тих самих людях, головне, щоб вони мали інструменти для автоматизації операцій. Саме тому простота використання мережевих рішень після процесу впровадження є такою важливою.

Завдяки централізованому управлінню, рішення Forcepoint дозволяють швидко впроваджувати багатофілійні середовища. Механізм розгортання без дотику забезпечує розробку середовища з безпрецедентною швидкістю . Після планування впровадження наступних локацій відраховується за лічені секунди. Підтримка послідовної політики максимально автоматизована.

Централізоване управління безпекою Forcepoint дозволяє замінити статичні правила брандмауера динамічними, високорівневими інтелектуальними правилами. Вони реалізують бізнес-процеси відомим чином, використовуючи категорії користувачів, організації, програми, служби, розташування, дії тощо. За допомогою Forcepoint SMC ви зможете створювати групи різних типів та використовувати їх як частину політик, щоб замінити закодовані значення змістовними іменами, які можна оновлювати з одного місця. Forcepoint SMC дозволить повторно використовувати політики (по всій мережі) за допомогою передових методів, таких як ієрархічне успадкування та дочірні політики.

Forcepoint SMC забезпечує повний огляд корпоративної мережі на 360 градусів [16] . Він збирає інформацію про управління інцидентами та моніторинг стану з Forcepoint NGFW, кінцевих точок та інших компаній, що дозволяє проводити інтерактивний аналіз та створювати детальні звіти. Завдяки інтеграції журналів подій з одночасною обробкою до 2000 машин, адміністратори отримують повну продуктивність мережі. Команди реагування на інциденти можуть швидко реагувати на приховані загрози.

Рис. 2.6. Огляд та управління всієї корпоративної мережі

Великий вибір платформ та спеціальних моделей гарантує відповідну продуктивність навіть для найвимогливіших середовищ. Незалежно від того, чи потрібно захистити головну серверну кімнату, невеликий філіал чи центр хмарних обчислень, усі брандмауери використовують централізовано розподілені політики.

Переваги Forcepoint NGFW:

– централізоване єдине представлення даних для керування понад 2000 фізичними або віртуальними Forcepoint NGFW у розподілених середовищах;

– гнучкість та масштабованість для потреб впровадження у великих корпоративних мережах;

– варіант високої доступності для задоволення суворих вимог до безвідмовної роботи;

– Ефективна автоматизація робочих процесів , що дозволяє швидко та ефективно впроваджувати та обслуговувати Forcepoint NGFW;

– Контекст користувача та кінцевої точки , видимість у масштабі всієї мережі – від центру обробки даних, межі мережі та окремих відділів, до хмарних обчислень.

2.5. Функції та призначення Forcepoint mobile agent

Мобільний агент — це пристрій на базі Linux, який дозволяє захистити тип вмісту електронної пошти, що синхронізується з мобільними пристроями користувачів під час підключення до мережі (рис.2.7.). Це включає вміст електронних листів, події календаря та завдання [17].

Мобільний агент аналізує контент, коли користувачі синхронізують свої мобільні пристрої із сервером Exchange вашої організації. Якщо контент або дані, що надсилаються на їхній пристрій, порушують політику DLP організації для мобільних пристроїв, вони відповідно поміщаються в карантин або дозволяються [17].

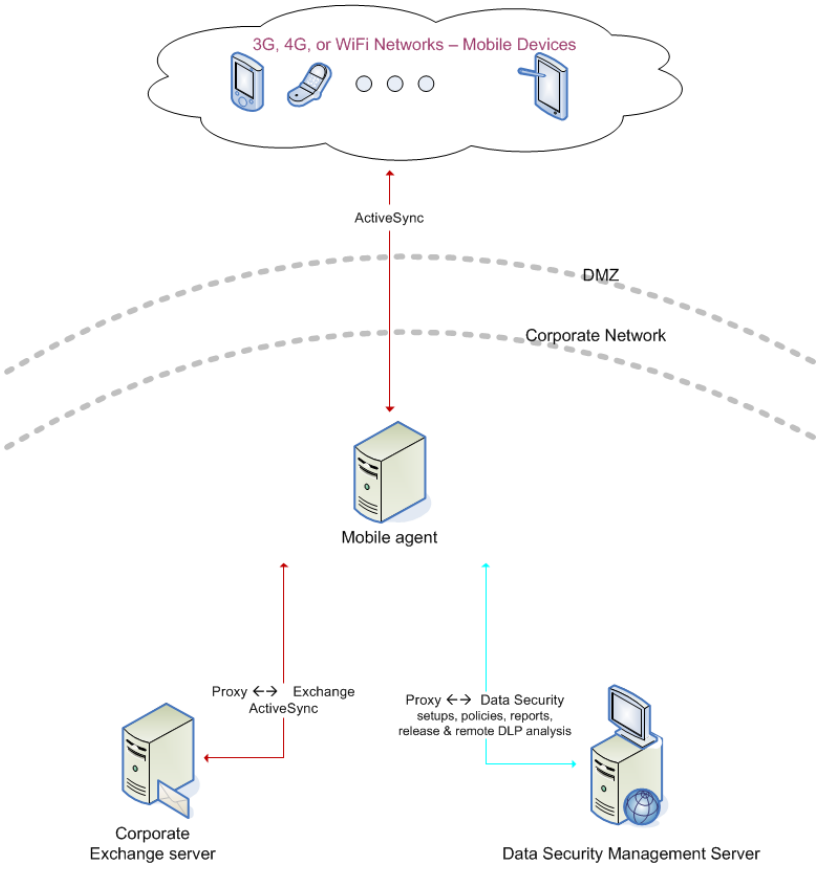

Рис. 2.7. Архітектура розгортання мобільного сервера

У корпоративній мережі пристрій підключається до сервера керування безпекою даних та до вашого агента Microsoft Exchange для забезпечення цієї функції. Аналіз DLP виконується на пристрої або на інших серверах безпеки даних (а не на сервері керування) для оптимізації продуктивності та балансування навантаження.

Поза демілітаризованою зоною мобільний агент підключається до будь-якого мобільного пристрою, сумісного з Microsoft ActiveSync, через мережі 3G та бездротові мережі, такого як i-pad, мобільні телефони Android та iPhone. (ActiveSync – це протокол бездротового зв'язку, який використовується для передачі ресурсів, таких як електронна пошта, з програм на мобільні пристрої.)

На відміну від прокси сервера, пристрій мобільного агента діє як зворотний проксі-сервер, оскільки він отримує ресурси, такі як електронна пошта, із сервера Exchange від імені мобільного пристрою.

Наведений рисунок 2.7 ілюструє архітектуру системи типового розгортання мобільного агента. Залежно від корпоративної мережі та вимог безпеки, можна використовувати периферійний пристрій, такий як сервер Microsoft ISA, який діє як зворотний проксі-сервер для мобільного агента.

Forcepoint Mobile з використанням агента, забезпечує продуктивність через безпечний веб-доступ до корпоративних ресурсів, одночасно захищаючи мобільний пристрій користувача від веб-загроз. Він забезпечує захист пристроїв iOS та iPadOS.

Forcepoint дозволяє компанії застосовувати на мобільних пристроях ті ж самі засоби безпеки, що й на ноутбуках і настільних комп'ютерах.

2.6. Функції та призначення агентів Websense Data Security

Безпека даних — це комплексна система запобігання втраті даних (DLP), яка виявляє, контролює та захищає ваші критично важливі інформаційні сховища, незалежно від того, чи ці дані зберігаються на ваших серверах, використовуються наразі чи розташовані в кінцевих точках поза мережею. Безпека даних захищає від втрати даних, швидко аналізуючи дані та автоматично застосовуючи налаштовані політики, незалежно від того, чи перебувають користувачі в мережі, чи офлайн. Адміністратори керують тим, хто може надсилати яку інформацію, куди та яким чином. Безпека даних також може працювати як частина Websense TRITON Enterprise для захисту всієї організації [18].

Основні компоненти Websense Data Security:

- сервер керування безпекою даних;
- додаткові сервери безпеки даних;
- Protector;
- агенти;
- кінцеві точки.

Сервер керування безпекою даних (Data Security Management Server) , який розташований на сервері керування TRITON, є ядром системи, забезпечуючи повний аналіз запобігання втратам даних у мережі. Крім того, сервер керування безпекою даних збирає та зберігає всю статистику управління. Для балансування навантаження аналіз може бути спільним для кількох серверів безпеки даних. Protector може забезпечити додаткові можливості блокування для системи запобігання втратам [18].

За потреби, проксі-сервер працює разом із сервером керування безпекою даних (Data Security Management Server). Сервер керування безпекою даних виконує виявлення (виконується сканером) та надає розширені можливості аналізу. Protector знаходиться в мережі, перехоплює та аналізує трафік, а також може відстежувати або блокувати його за потреби. Protector підтримує аналіз SMTP, HTTP, FTP, Generic Text та IM-трафіку (чат та передача файлів). Проксі-сервер також є точкою інтеграції для сторонніх рішень, що підтримують ICAP[18].

Protector вписується у існуючу мережу організації з мінімальною конфігурацією та не потребує змін мережевої інфраструктури.

Агенти Websense Data Security також є невід'ємною частиною системи. Ці агенти встановлюються на відповідних серверах (агент ISA на сервері Microsoft ISA, агент принтера на сервері друку тощо), щоб Data Security мав доступ до даних, необхідних для аналізу трафіку з цих серверів. Агенти, такі як кінцева точка даних, дозволяють адміністраторам аналізувати контент у робочому середовищі користувача (ПК, ноутбук тощо) та блокувати або відстежувати порушення політик [18].

Базове розгортання може мати лише один сервер керування та один Protector. Protector включає кілька агентів, зокрема SMTP, HTTP, FTP, IM та ICAP. Сервери легко налаштовуються для простого моніторингу або моніторингу та захисту конфіденційних даних. Це ідеально підходить для малого та середнього бізнесу з однією точкою виходу в Інтернет. Наведений нижче рис 2.8 є високорівневою діаграмою базового розгортання безпеки даних. Таке розгортання ідеально

підходить для невеликих та середніх організацій з однією точкою виходу в Інтернет.

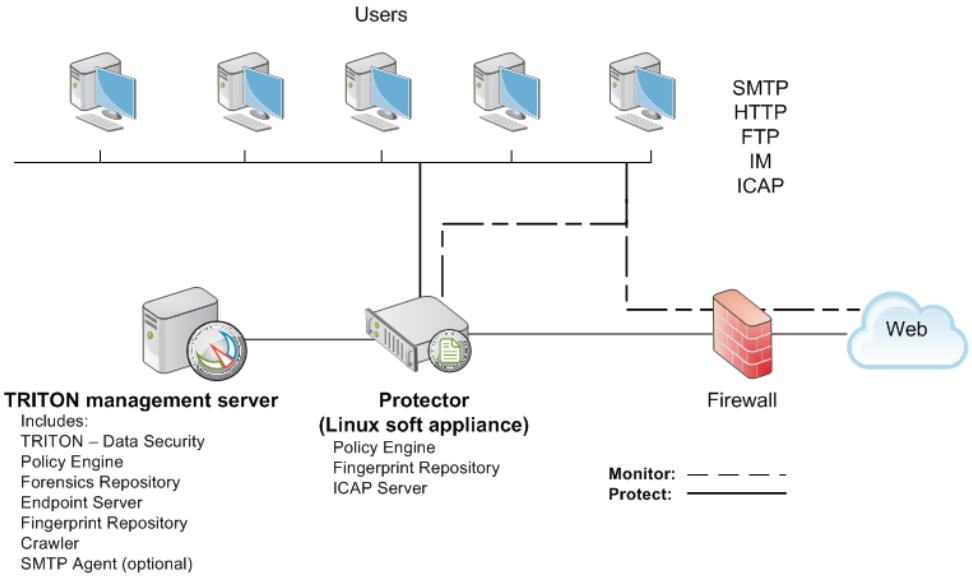

Рис. 2.8. Базове розгортання безпеки даних

Сервер керування безпекою даних дозволяє визначати які дані необхідно захищати. Відповідно до політик різних галузей та регіонів захист організовується за географічним знаходженням, промисловістю, сектором та загальними політиками та типами конфіденційної інформації, такої як особиста, фінансова та медична.

Виходячи з досвіду численних розгортань захисту від втрати даних, конфіденційна інформація організацій зберігається на корпоративних файлових серверах або спільних дисках, внутрішніх базах даних, персональних ноутбуках, робочих станціях та знімних носіях.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА ОСНОВІ FORCEPOINT DLP

3.1. Варіант налаштування захисту від втрати даних Forcepoint DLP

DLP — це функція запобігання втраті даних, яка дозволяє зіставляти дані зі шаблонами (за допомогою регулярних виразів і ключових слів) під час їх завантаження, вивантаження або сканування через API у стані спокою.

Об'єкти шаблонів DLP дозволяють встановлювати критерії відповідності для захисту та контролю конфіденційних даних. Forcepoint ONE SSE надає велику бібліотеку шаблонів DLP, що дозволяє клієнтам підтримувати відповідність законодавчим або корпоративним вимогам (наприклад, HIPAA, SOX, PCI тощо).

На сторінці «Об’єкти DLP» , розташованій у розділі «Захист» > «Об’єкти» , можна визначити об’єкти DLP, які використовуватимуться на сторінці політик для керування та виконання дій у захищених програмах (рис.3.1). Сторінка «Об’єкти DLP» складається з попередньо визначених шаблонів та користувацьких шаблонів, які можна створити або імпортувати зі сторінки «Бібліотека». Це можна зробити для деяких попередньо визначених шаблонів, таких як:

ATP – необхідно придбати підписку на будь-який із підтримуваних варіантів розширеного захисту від загроз (ATP), щоб мати змогу впроваджувати його у політики ваших програм.

Forcepoint DLP – Вам слід придбати підписку на Forcepoint DLP, щоб забезпечити застосування політики DLP та пов’язаних із нею дій, налаштованих у Forcepoint Security Manager (FSM) для каналів CASB та SWG у Forcepoint ONE SSE.

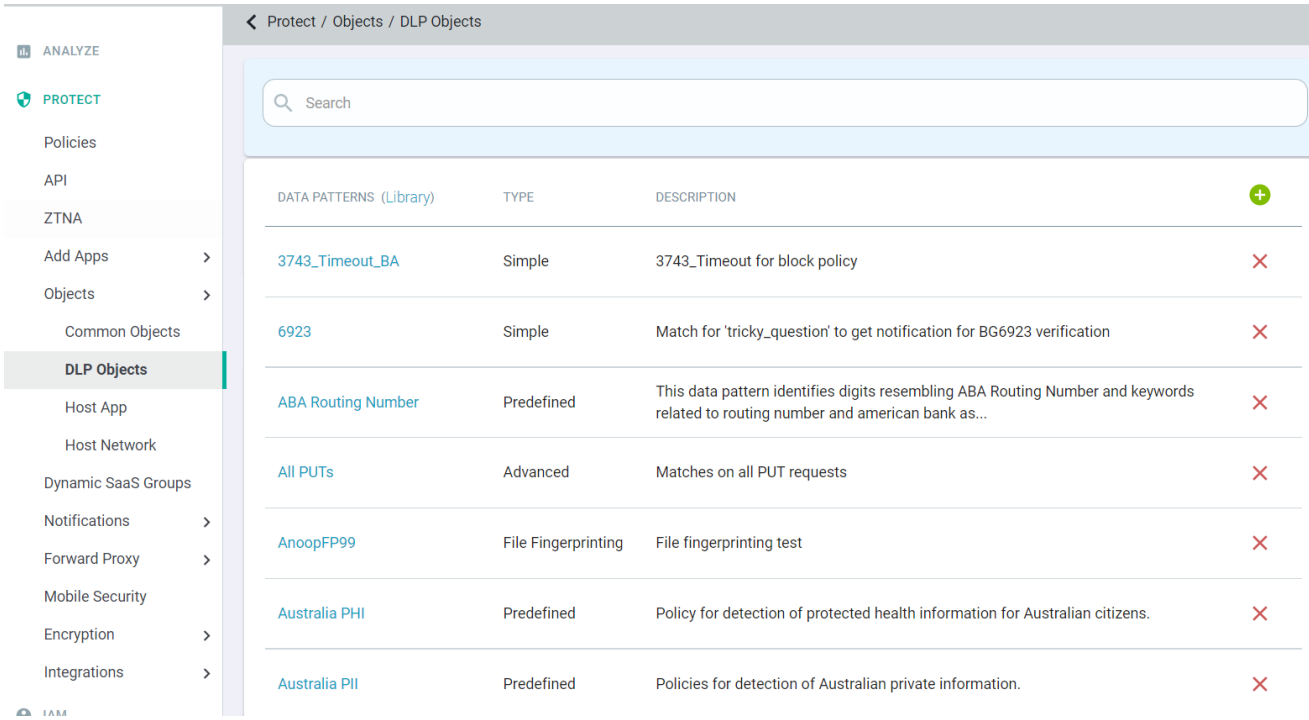

Рис. 3.1. Налаштування об'єктів шаблонів DLP

На сторінці «Об’єкти DLP» можна фільтрувати шаблони даних за назвами стовпців). Також можна сортувати шаблони даних, натиснувши на «Шаблони даних і тип».

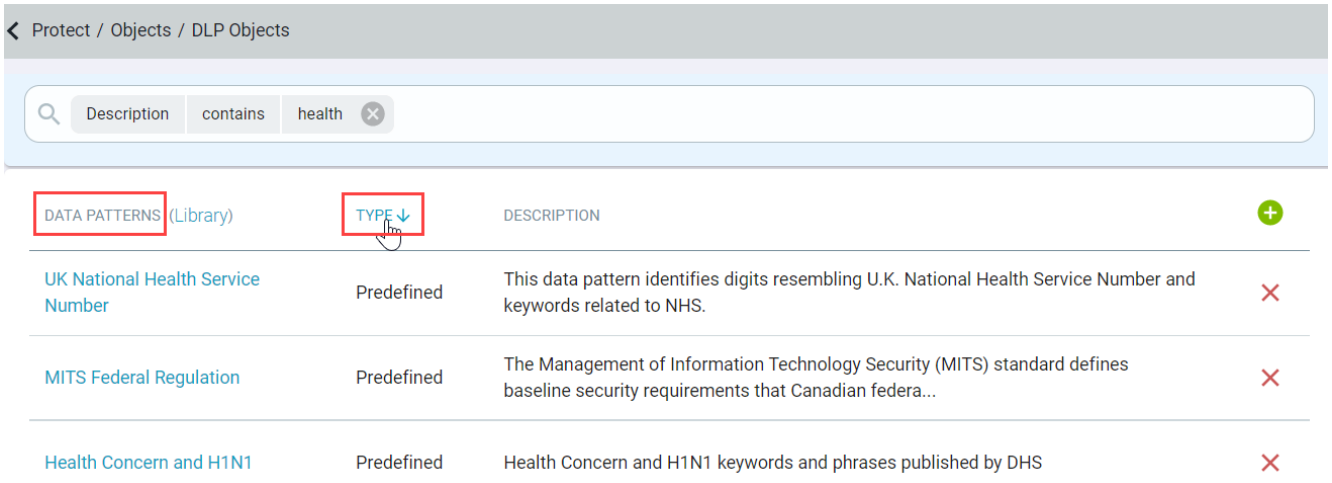

Рис.3.2. Сортування шаблонів даних

Forcepoint ONE SSE дозволяє створювати власні шаблони DLP на основі кількох різних типів:

Простий. Дозволяє прості збіги ключових слів та/або регулярні вирази. Найпоширеніший тип шаблону даних.

Розширений. Дозволяє створювати складніші шаблони, використовуючи комбінації інших шаблонів або змінних шаблонів на основі булевої логіки.

Точна відповідність. Дозволяє створювати шаблон даних на основі точного набору даних для ідентифікації конкретних точних даних (наприклад, особистої інформації певної особи).

Крім того, Forcepoint ONE SSE також підтримує низку типів шаблонів на основі файлів:

Відбиток файлу. Може створити «відбиток» файлу-прикладу, щоб визначити відсоткове збігання (шукайте інші файли, схожі на цей файл-приклад, збіг має бути щонайменше 70%).

Тип MIME файлу. Базувати шаблон на форматі/природі файлу (ідентифікація та блокування документів типу PDF).

Розмір файлу. Дозволяє клієнтам застосовувати шаблон даних на основі розміру файлу (блокувати всі завантаження, якщо вони перевищують 50 МБ).

Метадані файлу. Можна вказати точні метадані для перевірки та значення, з яким потрібно зіставити дані. Це можуть бути будь-які властиві файлу метадані, такі як назва файлу, версія продукту, точний розмір тощо.

Після ввімкнення попередньо визначених шаблонів DLP на основі типів файлів у вашому клієнті, на сторінці «Об’єкти DLP» відображаються три попередньо визначені шаблони DLP для стандартних типів файлів, які можна використовувати під час налаштування вбудованих політик (ZTNA та CASB), вмісту SWG та API для виявлення або блокування вмісту на основі типів файлів.

У таблиці 3.1. наведено три попередньо визначені шаблони DLP для стандартних типів файлів.

В таблиці вказані назва шаблону, опис та тип файлів для використання шаблону даних, які ви хочете використовувати.

Таблиця 3.1.

Попередньо визначенні шаблони

Назва шаблону даних	**Опис**	**Типи файлів**
Виконувані файли	Цей шаблон даних відповідає всім виконуваним файлам.	Виконувані файли Windows, Linux та macOS - .exe - .com - .bin - .o - .отже - .dylib
Файли багатих інтернет-застосунків	Цей шаблон даних відповідає всім файлам Rich Internet Application.	Файли MacroMedia Flash та Microsoft Silverlight - .swf
Документи та PDF-файли	Цей шаблон даних відповідає всім документам та файлам, пов'язаним з офісом.	- PDF (.pdf) - Документи Microsoft Office (OLE та OOXML) - .doc - .docx - .pptx - .ppt - .xls - .xlsx - RTF-файли (.rtf)

Якщо клацнути будь-який із попередньо визначених шаблонів DLP на основі типу файлу, шаблони даних відображатимуть лише вкладку «Тестовий шаблон» . Ви можете перевірити відповідність шаблону DLP, завантаживши файл і натиснувши кнопку «Тест». Результат тесту показує успішне або невдале зіставлення з типом файлу та відображає тип MIME завантаженого файлу.

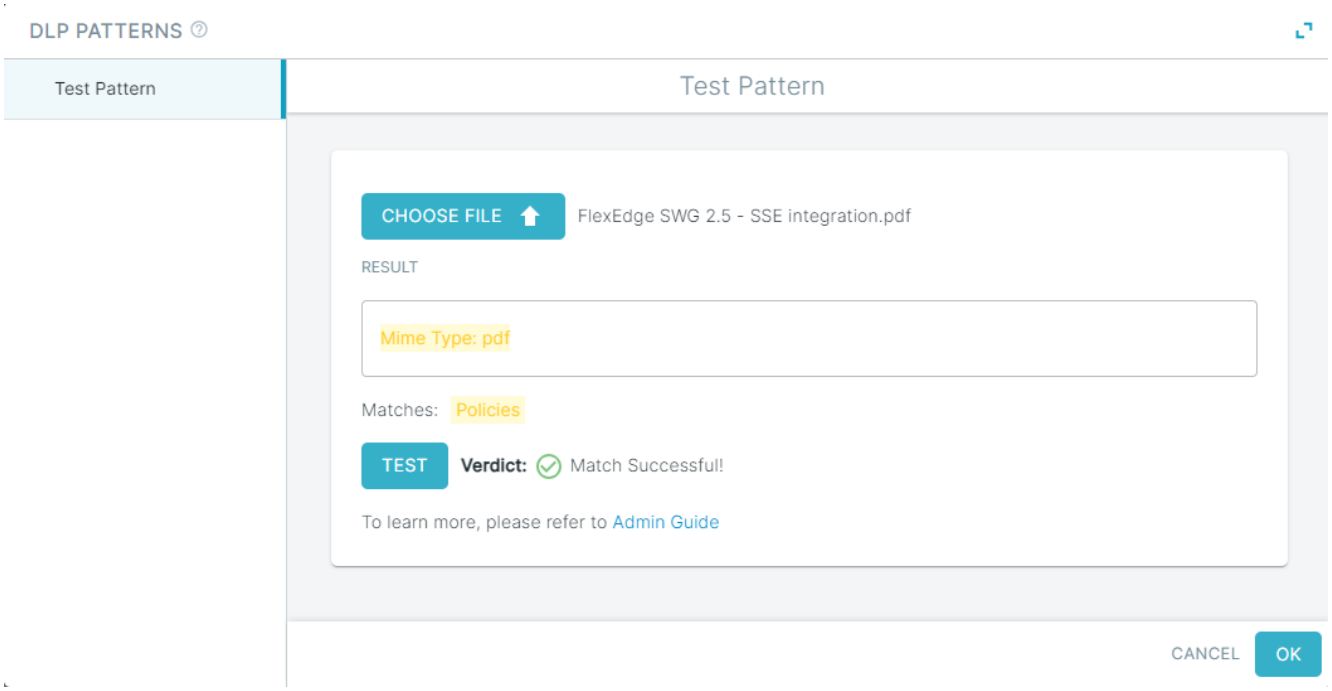

Рис.3.3. Результат зіставлення з типом файлу

Forcepoint ONE SSE містить велику кількість попередньо визначених шаблонів DLP на основі часто використовуваних об'єктів, включаючи шаблони зіставлення для кредитних карток, конфіденційних ключових слів, номерів соціального страхування тощо.

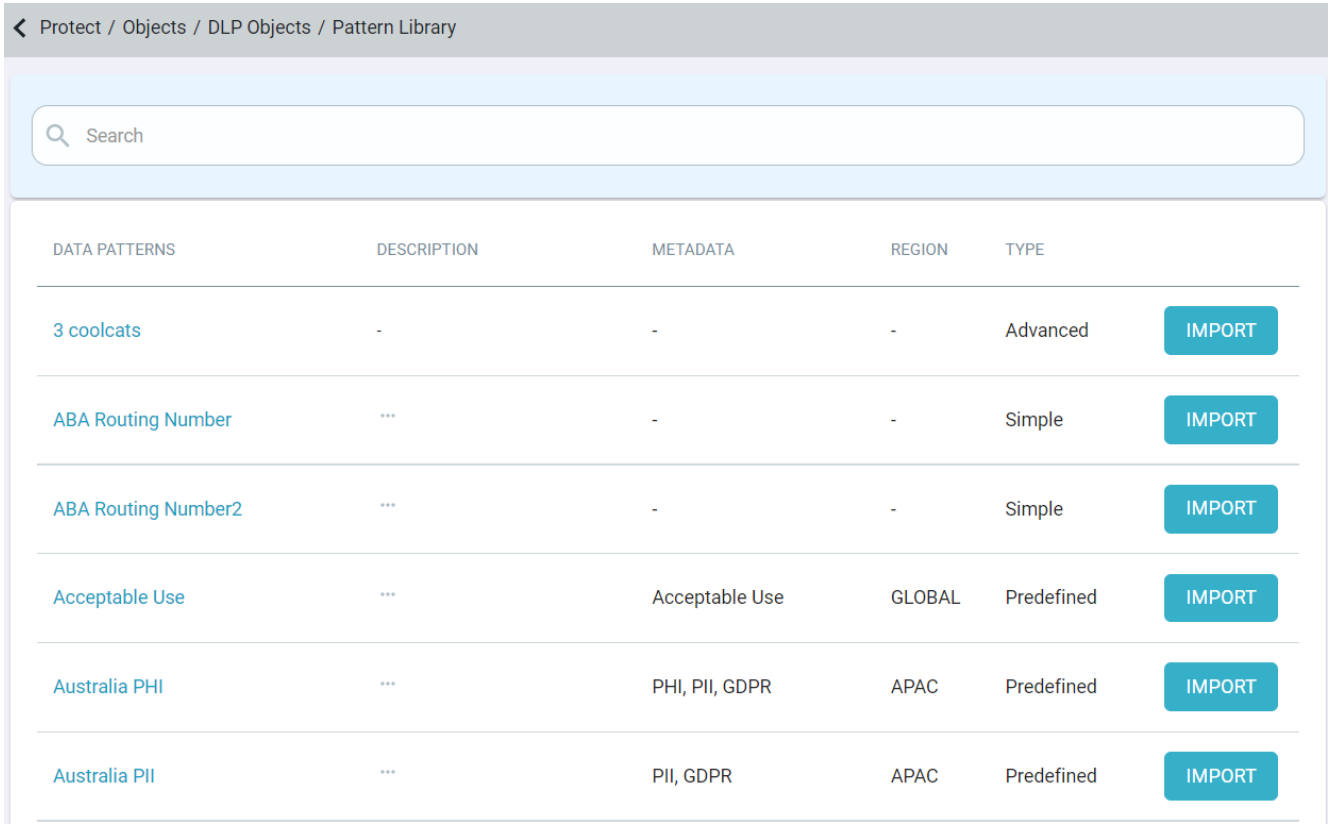

Рис.3.4. Визначені шаблони

На сторінці «Бібліотека шаблонів» (рис.3.2) ви можете додавати шаблони для використання у своїх політиках, натискаючи кнопку «Імпортувати» , пов’язану зі шаблоном даних, який ви хочете використовувати.

Після натискання кнопки «Імпорт» відкриється діалогове вікно з двома варіантами:

Функція «Автоматичне оновлення» додасть шаблон як попередньо визначений шаблон, який ви не зможете редагувати, і який автоматично оновлюватиметься щоразу, коли Forcepoint ONE SSE потрібно буде оновити шаблон.

З іншого боку, функція «Створити копію» додасть шаблон, щоб ви могли вносити зміни до шаблону (наприклад, назву або навіть сам шаблон). Це дозволяє вам налаштувати шаблон за потреби, але також означає, що якщо Forcepoint ONE SSE коли-небудь оновить його, адміністраторам потрібно буде повернутися на сторінку «Бібліотека», щоб імпортувати нові зміни.

Розглянемо для прикладу *створення шаблону даних для відбитків файлів*

Тип «Відбиток файлу» дозволяє створити відбиток на основі документа або кількох документів для виконання відсоткового зіставлення.

Це можна зробити, якщо адміністратори шукають шаблон форми або стандартизований документ у своїй хмарній програмі, але не впевнені в точному вмісті документа.

Налаштування зчитування відбитків файлів дещо відрізняється від багатьох інших типів шаблонів, які можете створити.

Кроки

1. Перейдіть до Захист > Об’єкти > Об’єкти DLP (рис 3.5).
2. Натисніть зелений значок із плюсом і виберіть «Відбитки файлів» , щоб створити шаблон даних.
3. Введіть назву та опис шаблону даних. Потім перейдіть на вкладку «Критерії відповідності» .

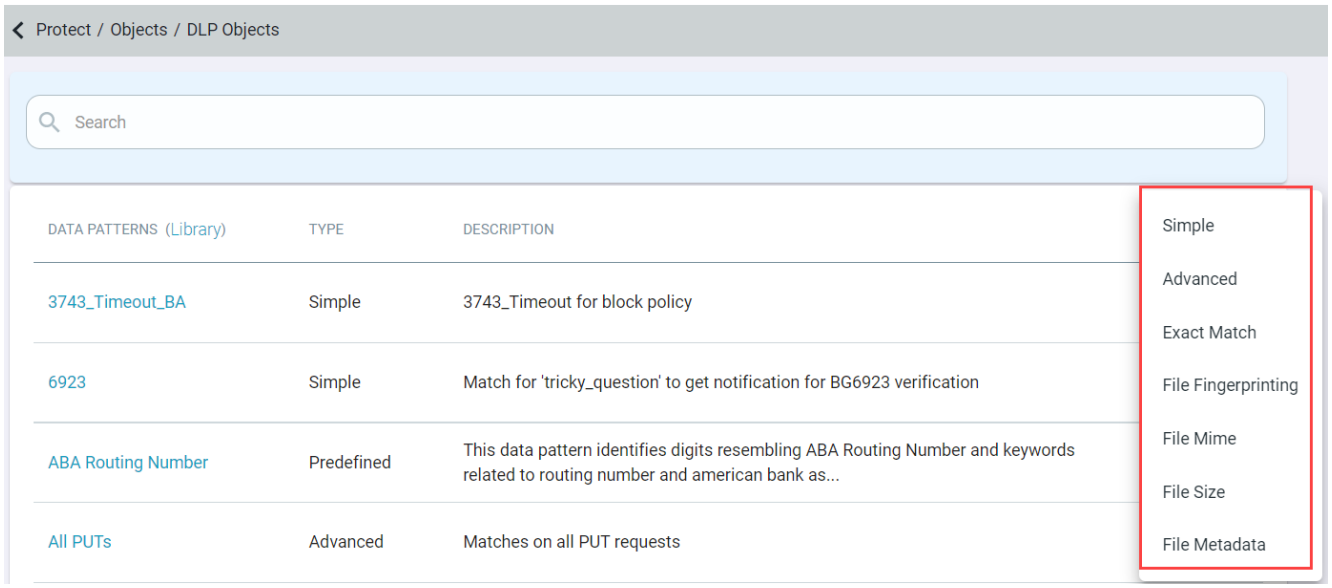

Рис. 3.5. Налаштування відбитків файлів

4. Виберіть відсоток, якому має відповідати відбиток файлу, і натисніть «Застосувати» , щоб побачити посилання «Завантажити відбиток файлу» (рис 3.6).

5. Натисніть посилання «Завантажити файл відбитків пальців» , щоб завантажити скрипт, який потрібно буде запустити для обраних файлів.

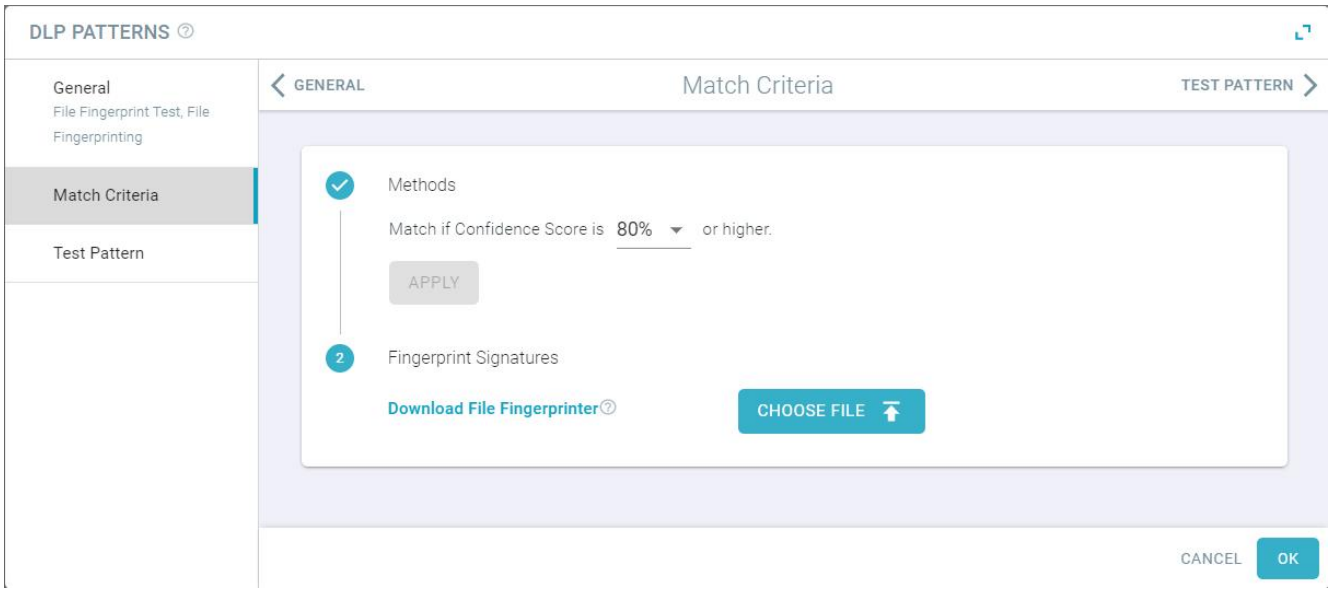

Рис. 3.6. Налаштування відбитку файлу

6. Завантаження міститиме скрипти, які потрібно буде запустити на ваших файлах, щоб згенерувати підпис відбитка пальця, який буде завантажене назад до цього шаблону даних та встановите показник достовірності. У папці є два скрипти для Linux та Windows.

Сканер відбитків пальців підтримує Java 8 або 11 у Linu x та Java 8 у Windows.

Процес запуску скрипта полягає у попередньому створенні папки на комп’ютері та розміщенні файлу або файлів, для яких потрібно створити відбиток. Скрипт вкаже на всю папку та створить єдиний підпис відбитка для всіх файлів у папці. Це означає, що ви можете мати єдиний шаблон даних, який перевіряє рівень достовірності кількох файлів одночасно. Якщо ви хочете, щоб файли мали різні відсотки, просто створіть новий шаблон даних і розділіть файли по різних папках, щоб ви могли створювати унікальні підписи на основі будь-якого показника достовірності, який ви хочете застосувати.

Показник достовірності – це відсоткове співпадіння, кратне 10, і збігатиметься, якщо відповідний файл відповідає вашому відсотку або більше. Наприклад, якщо встановити показник достовірності на 70%, будуть знайдені файли, які відповідають 70% або більше вмісту документа з відбитком, за допомогою якого ви створили шаблон.

7. Щоб зберегти шаблон даних, натисніть кнопку «ОК» .

8. Натисніть вкладку «Тестовий шаблон», щоб перевірити, чи шаблон налаштовано правильно.

Таким чином, адміністратор безпеки налаштовує у системі всі необхідні шаблони, за якими DLP- система буде виявляти файли, які заборонені для передачі та надавати інформацію щодо виявлення інцидентів витоку інформаційних ресурсів.

3.2. Розробка рекомендацій щодо захисту корпоративних інформаційних ресурсів

Рекомендації щодо ефективного використання засобів запобігання витокам даних (DLP) для захисту корпоративних інформаційних ресурсів - це не просто встановлення програмного забезпечення, а стратегічний процес, який вимагає глибокого розуміння даних, бізнес-процесів та потенційних ризиків. Надаємо основні етапи, які дозволять фахівцям з кібербезпеки підвищити рівень захисту своєї організації

1. Етап планування та підготовки складається з декількох важливих кроків

- Визначте та класифікуйте інформаційних ресурсів:

Проведіть аудит усіх інформаційних ресурсів;

Чітко ідентифікуйте, які типи даних є критично важливими (фінансова інформація, персональні дані клієнтів/співробітників, інтелектуальна власність, комерційна таємниця, стратегічні плани тощо);

Розробіть чітку систему класифікації даних (наприклад, "Публічні", "Внутрішні", "Конфіденційні", "Цілком таємно"). Кожен рівень повинен мати визначені правила обробки та доступу;

Це є найважливіший етап, оскільки без розуміння, які саме дані треба захистити, DLP-система буде працювати неефективно.

- Визначте потенційні канали витоку:

Проаналізуйте всі можливі шляхи, якими дані можуть залишити вашу організацію (електронна пошта, веб-трафік, хмарні сховища, месенджери, USB-накопичувачі, друк, скріншоти, буфер обміну, тощо).

Визначте найризикованіші канали для вашої організації.

Отримана інформація дозволить визначити слабкіші місця і там необхідно впроваджувати додаткові модулі захисту DLP.

- Розробіть чіткі політики безпеки даних:

Створіть внутрішні політики та процедури, які регламентують роботу з конфіденційною інформацією. Ці політики повинні бути зрозумілими для всіх співробітників.

Включіть у них правила використання корпоративної пошти, інтернету, знімних носіїв, мобільних пристроїв та хмарних сервісів.

DLP-система буде автоматизувати та забезпечувати дотримання цих політик.

- Створіть команду впровадження та підтримки:
  - Залучайте представників IT-безпеки, юридичного відділу, HR, бізнес-підрозділів. Захист даних – це не лише технічне питання.

Чіткі і зрозумілі політики організації дозволять фахівцям дотримуватись вимог щодо відповідності DLP-системи нормативним вимогам.

2. Етап впровадження DLP-системи

- Вибір відповідної DLP-системи:

Врахуйте розмір вашої організації, специфіку даних, наявні канали передачі та бюджет.

Зверніть увагу на можливості: ідентифікації даних, гнучкість політик, охоплення каналів (мережевих, хмарних, тощо), аналітичні можливості, інтеграцію з іншими системами безпеки (SIEM, IAM).

- Розробіть поетапне впровадження (Фази):

Фаза 1. Моніторинг (Audit/Monitor-only mode). Запустіть DLP-систему в режимі моніторингу. Це дозволить зібрати дані про фактичний рух корпоритивної інформації, виявити "справжні" канали витоку та налаштувати політики без блокування легітимних операцій. Цей етап критично важливий для мінімізації "хибних спрацювань".

Фаза 2. Попередження. Коли політики налаштовані та протестовані, увімкніть попередження для користувачів. Система інформуватиме їх про потенційні порушення політик та вимагатиме підтвердження або обґрунтування. Це підвищить обізнаність та привчатиме співробітників до нових правил.

Фаза 3. Блокування. Після достатнього періоду моніторингу та попереджень, коли "хибні спрацювання" зведені до мінімуму, можна вмикати режим блокування для критично важливих даних або каналів.

3. Етап експлуатації та оптимізації

- Регулярне оновлення та налаштування політик:

Бізнес-процеси змінюються, з'являються нові види загроз та дані. Регулярно переглядайте та оновлюйте політики DLP відповідно до цих змін.

Аналізуйте спрацювання системи, щоб оптимізувати правила та зменшити кількість "хибних спрацювань".

Навчання та підвищення обізнаності співробітників:

Проводьте постійні тренінги для всіх співробітників щодо важливості захисту даних та правил роботи з DLP-системою.

Пояснюйте, чому впроваджуються ці заходи, і як вони захищають не лише компанію, а й самих співробітників та клієнтів.

Використовуйте кейси з реального життя (без розголошення імен) для демонстрації наслідків витоків.

- Моніторинг та реагування на інциденти:

Забезпечте інтеграцію DLP-системи з SIEM-системою для централізованого збору та аналізу подій безпеки.

Оперативно реагуйте на виявлені інциденти, проводьте розслідування та застосовуйте відповідні заходи.

Включіть DLP-систему в загальний план реагування на інциденти кібербезпеки.

Аудит та звітність:

Регулярно проводьте аудити ефективності DLP-системи.

Аналізуйте звіти DLP для виявлення тенденцій, найчастіших порушень та слабких місць. Використовуйте ці дані для подальшого покращення політик та процесів.

Баланс між безпекою та продуктивністю:

Важливо знайти баланс, щоб DLP-система не створювала надмірних перешкод для легітимної роботи співробітників. Занадто жорсткі правила можуть призвести до обходу системи або зниження продуктивності.

Залучайте бізнес-підрозділи до обговорення політик.

Важливі аспекти, які слід врахувати:

Врахуйте законодавчі вимоги щодо приватності співробітників. Чітко інформуйте персонал про те, яка інформація моніториться.

DLP – це інструмент, який підтримує культуру безпеки даних. Без цієї культури його ефективність буде обмеженою.

Треба розуміти, що DLP не є єдиним рішенням безпеки. Вона працює в комплексі з іншими заходами безпеки (управління доступом, шифрування, навчання, EDR, SIEM).

Ефективне впровадження DLP – це безперервний процес вдосконалення, який захищає найцінніший актив вашої організації – її інформацію, забезпечуючи відповідність регуляторним вимогам та мінімізуючи ризики кіберінцидентів.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

Проведено аналіз проблеми, в результаті якого було визначено поняття інформаційних ресурсів та їх важливість як основних активів організації. Проаналізовані звіти провідних компаній показав, що велика частка інцидентів безпеки відбувається в наслідок внутрішніх інсайдерів. Такий виток інформації може призвести до негативних наслідків у роботі організацій.

На основі проведеного аналізу проблеми, в роботі визначено основні підходи щодо використання різних засобів захисту корпоративних інформаційних ресурсів. Застосування таких засобів є відповідність роботи організацій до основних законодавчих норм. Тому було обрано DLP-системи, які запобігають витокам корпоративним інформаційним ресурсам та запобігти несанкціонованій передачі даних.

В роботі проведено порівняльний аналіз DLP-рішень, яке показує сильні сторони та орієнтацію кожного рішення. В результаті порівняння було обране рішення Forcepoint DLP, як таке що пропонує захист у хмарних середовищах та забезпечує повний контроль інформаційних ресурсів організації.

Аналіз архітектури Forcepoint DLP, дозволив визначити основні складові рішення, яке є комплексним рішенням для виконання завдань фільтрації та веб-безпеки, безпеки електронної пошти, безпеки приладів. Кожний з модулів надано функціональні можливості компонентів, які є комплексним рішенням для забезпечення захисту інформаційних ресурсів, в залежності від потреб організації.

В практичній частині роботи запропоновано варіант налаштування Forcepoint DLP для об'єктів шаблонів як попередньо визначенні та дозволяють встановлювати критерії відповідності для захисту та контролю корпоративних інформаційних ресурсів. Таке налаштування, дозволить фахівцям вчасно виявляти та протидіяти інцидентам несанкціонованого витоку даних.

В результаті виконаного дослідження розроблені загальні рекомендації щодо ефективного використання засобів запобігання витокам даних та підвищення рівня захисту корпоративних ресурсів. Рекомендації розроблено у вигляді основних етапів та кроків, які дозволять визначати та класифікувати критично важливу інформацію, визначати потенційні канали витоку інформації, розробляти політики для дотримання відповідності організації нормативним вимогам.

ПЕРЕЛІК ПОСИЛАНЬ

1. Енциклопедія сучасної Україна. URL: https://esu.com.ua/article-12472 .
2. Витік інформації. URL: https://www.imperva.com/learn/data-security/data-breach/ .
1. Статистична інформація витоку інформації. URL: https://secureframe.com/blog/data-breach-statistics .
2. Вартість витоку даних. URL: https://www.ibm.com/reports/data-breach .
3. Звіт витоку даних Verizon. URL: https://www.verizon.com/business/resources/Tf91/reports/2023-data-breach-investigations-report-dbir.pdf .
4. NIST Special Publication 800-53. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf .
5. Внутрішні інсайдер. URL: https://www.syteca.com/en/blog/real-life-examples-insider-threat-caused-breaches .
6. Можливості управління інформаційною безпекою. URL: https://www.bsigroup.com/en-IN/products-and-services/standards/iso-iec-27001-information-security-management-system/ .
7. Cybersecurity Framework. URL: https://www.nist.gov/cyberframework.
8. Forcepoint DLP. URL: https://www.forcepoint.com/product/dlp-data-loss-prevention .
9. Data Loss Prevention: Enterprise Scale and Highly Accurate. URL: https://www.broadcom.com/products/cybersecurity/information-protection/data-loss-prevention .
10. Proofpoint Email DLP. URL: https://www.proofpoint.com/au/products/information-protection/email-dlp.
11. Архітектура Forcepoint ONE DLP. URL: https://help.forcepoint.com/dlp/90/deployctr/2E255AD0-C9B3-41A7-8361-8ABCBFE022A1.html .

12. Forcepoint Web Security Cloud. URL: https://www.websense.com/content/support/library/web/hosted/getting_started/how_wsc_works.aspx .

13. Кофігурація Forcepoint Email Security. URL: https://support.forcepoint.com/s/article/How-to-configure-Data-Protection-for-Email .

14. Брандмауер Forcepoint. URL: https://notonlyfirewall.eu/en/management/ ..

15. Мобільний агент. URL: https://www.websense.com/content/support/library/deployctr/v77/dic_ds_mob_agent.aspx .

16. Websense Data Security.URL: https://www.websense.com/content/support/library/deployctr/v77/dic_ds_main.aspx .

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)