РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 50 сторінок, 10 рисунків, 16 джерел.

Об'єкт дослідження – процес забезпечення захисту кінцевих точок від витоку даних.

Предмет дослідження – методи та засоби захисту кінцевих точок на основі Symantec DLP.

Мета роботи розробити рекомендації щодо застосування методів та засобів захисту кінцевих точок від витоку даних на основі Symantec DLP.

Методи дослідження – опрацювання за даною темою, аналіз експлуатаційної документації, нормативної документації та їх порівняння.

Системи запобігання витоку конфіденційних даних на кінцевих точках (DLP) відіграють важливу роль у підвищенні безпеки кінцевих точок підприємства чи компанії. Системи DLP призначені для постійного моніторингу дій та поведінки користувачів на кінцевих точках. Системи DLP забезпечують даними про активності на кінцевих точках у реальному часі, що дозволяє швидко реагувати на інциденти безпеки.

В роботі досліджено проблему захисту кінцевих точок організації, визначено його мету та завдання. Проведено аналіз існуючих методів та засобів захисту кінцевих точок від витоку даних. Досліджено методи та засоби захисту кінцевих точок на основі Symantec DLP . Визначено призначення, основні функції та склад рішення Symantec DLP.

На основі досліджень проведених в роботі запропоновано варіант системи на основі Symantec DLP. Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації методів та засобів захисту кінцевих точок від витоку даних.

Галузь використання – кібербезпека інформаційних ресурсів компанії.

DLP, ІНФОРМАЦІЙНІ РЕСУРСИ, КІНЦЕВІ ТОЧКИ, ЗАХИСТ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ВІД ВИТОКУ

ДАНИХ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DLP	—	Data Loss Prevention;
SIEM	—	Security information and event management;
IAM	—	Identity and Access Management;
AD	—	Active Directory;
PGP	—	Pretty Good Privacy;
LDAP	—	Lightweight Directory Access Protocol;
SSO	—	Single Sign-On;
IDS	—	Intrusion Detection System;
IPS	—	Intrusion Prevention System;
IoT	—	Internet of Things;
MSP	—	Managed Service Provider;
DCM	—	Described Content Matching;
EDM	—	Exact Data Matching;
IDM	—	Indexed Document Matching;
VML	—	Vektor Machine Learning;
HIPAA	—	Health Insurance Portability and Accountability Act;
GDPR	—	General Data Protection Regulation.

ВСТУП

Актуальність дослідження. Забезпечення захисту кінцевих точок від витоку даних на основі Symantec DLP може бути визначена з ряду причин. По-перше, кінцеві точки є важливими носіями конфіденційної інформації, і захист цих пристроїв - ключове питання в запобіганні несанкціонованому доступу та витоку конфіденційної інформації.

У сучасному інформаційному просторі захист кінцевих точок став важливим аспектом безпеки підприємства у зв'язку зі зростанням кількості загроз і атак, спрямованих на крадіжку конфіденційних даних. По-друге, кінцеві точки є ключовим вектором атак, оскільки організації дедалі частіше працюють з віддалених платформ і дедалі більше покладаються на хмарні технології. Витоки даних через вразливі кінцеві точки можуть вплинути на безпеку інфраструктури підприємства чи компанії та середовища віддаленої роботи. По-третє, розробка рекомендацій щодо захисту кінцевих точок від витоків даних є ключовим елементом стратегії кібербезпеки. Рішення Symantec Data Loss Prevention (DLP) вважається ефективним інструментом для моніторингу та контролю витоків конфіденційної інформації. Дане дослідження допоможе визначити оптимальну конфігурацію та інтеграцію Symantec DLP для ефективного захисту кінцевих точок. По-четверте, зі зростанням обчислювальної потужності та обсягів даних нові загрози витоку даних стають дедалі складнішими, і дослідження в галузі захисту кінцевих точок на базі Symantec DLP можуть виявити інноваційні підходи та стратегії, здатні ефективно протистояти сучасним загрозам кібербезпеки. У майбутньому вони можуть бути використані для боротьби із загрозами кібербезпеки.

У контексті сучасної глобалізації та розширення мережевих зв'язків, кінцеві точки залишаються ще більш уразливими перед різноманітними загрозами. Глобальні мережі вимагають комплексного та прогнозованого захисту, оскільки атаки можуть виникнути з будь-якої точки світу. Забезпечення захисту кінцевих точок від витоку даних на базі Symantec DLP стає аспектом глобальної

кібербезпеки, що дозволяє підприємствам уникнути масштабних інцидентів і зберегти довіру клієнтів і партнерів. Саме розгляд забезпечення захисту кінцевих точок на основі Symantec DLP у контексті відповідності та регулювання стає одним з аспектів дослідження.

У багатьох країнах і галузях існують правила та норми щодо захисту конфіденційної інформації та обробки даних. Дотримання цих норм є необхідним для підприємств, і дослідження може використовувати рішення Symantec DLP з метою допомогти дотримуватись вимог відповідності та уникати можливих штрафів або санкцій

Тому дослідження та розробка рекомендацій щодо захисту кінцевих точок від витоків даних на базі Symantec DLP є актуальним завданням, що допоможе розв'язати сучасні проблеми кібербезпеки та підвищити рівень захисту інформації в корпоративному середовищі.

Об’єкт дослідження – процес забезпечення захисту кінцевих точок від витоку даних.

Предмет дослідження – методи та засоби захисту кінцевих точок на основі Symantec DLP.

Мета роботи розробити варіант системи на основі Symantec DLP та рекомендації щодо застосування методів та засобів захисту кінцевих точок від витоку даних.

Наукові завдання:

дослідити сутність проблеми захисту кінцевих точок від витоку даних;

проаналізувати основні підходи до захисту кінцевих точок від витоку даних;

проаналізувати існуючі рішення із захисту кінцевих точок від витоку даних;

проаналізувати методи та засоби захисту кінцевих точок від витоку даних на основі Symantec DLP;

запропонувати варіант системи захисту кінцевих точок від витоку даних на основі Symantec DLP;

розробити рекомендацій щодо застосування методів та засобів захисту кінцевих точок від витоку даних.

Методи дослідження – опрацювання літератури за даною темою, аналіз технічної документації, нормативної документації та їх порівняння.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів захисту кінцевих точок від витоку даних, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх впровадження.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 26 квітня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ВІД ВИТОКУ ДАНИХ

1.1. Аналіз використання Symantec DLP у контексті існуючих проблем

Тенденція до витоку даних продовжує стрімко зростати в усьому світі: згідно з останнім звітом Cost of Data Breach, який щорічно публікують IBM та Ponemon Institute, збитки від витоку даних у 2021 році досягли рекордного рівня. у цьому році середній показник сягнув 4,24 мільйона доларів США знизився з 3,83 мільйона доларів США минулого року [1].

Заходи з мінімізації наслідків таких інцидентів вимагають комплексного рішення, яке охоплює всю поверхню атаки, включаючи мережі третіх і навіть четвертих сторін.

Розширеність кіберзлочинності змушує організацію вдосконалювати свої програми кібербезпеки, але багато хто все ще ігнорує одну з головних причин-витік даних.

Витік даних - це отримання нелегітимним користувачем несанкціонованого доступу до інформації. Це може статися фізично, наприклад, через наліпку з логіном і паролем, або електронно, наприклад, через вразливість у програмному забезпеченні.

Якщо кіберзлочинці можуть використовувати вікно даних, особливо якщо скомпрометовані дані містять особисту інформацію (PII), вони можуть використовувати цю інформацію для успішної кібератаки [1].

Витоки даних відбуваються не лише через кіберзлочинців. За статистикою викликані існуючими вразливими проявами, і часто громадськість тривалий час не знає про даний кіберінцидент. Розголошена чутлива або конфіденційна інформація (до конфіденційної інформації відноситься: інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень) може залишатися непоміченою роками, перш ніж її помітять кіберзлочинці або служби безпеки.

З іншого боку, витоки даних є результатом дії кіберзлочинців. Такі зломи є основною метою запланованих кібератак. Хоча витік даних і злом даних мають різне походження, обидва ці явища можуть призвести до компрометації конфіденційної інформації. Доступність до конфіденційної інформації підприємства або компанії часто передує використанню прогалин в системі безпеки і, таким чином, дає кіберзлочинцям можливість здійснювати масштабні кібератаки.

Надалі наведений список найпоширеніших проблем, що приводять до витоку даних:

1. Неправильна конфігурація програмного забезпечення

Неправильна конфігурація програмного забезпечення може призвести до витоку конфіденційної інформації клієнтів. Якщо прийняти програмне забезпечення широкого розповсюдження, мільйони користувачів можуть стати жертвами кібератаки.

2. *Соціальна інженерія.*

Кіберзлочинці недостатньо спричиняють витік даних, але коли це відбувається, то часто це результат тактичного обману за допомогою соціальної інженерії. Соціальна інженерія - це використання психологічних маніпуляцій для отримання конфіденційної інформації жертвою. Фішинг - найпоширеніший вид соціальної інженерії, який створюється в усній або електронній формі.

Прикладом вербальної фішингової атаки є ситуація, коли шахрай телефонує співробітнику і представляється IT-експертом. Зловмісник може вимагати облікові дані для входу в систему під виглядом отримання більшого доступу для вирішення критично важливої внутрішньої проблеми.

Компанія Experian зазначила витоку даних, що впровадив на 800 000 компаній через соціальну інженерію, зокрема, вербальні атаки. Кіберзлочинці, які видавали себе для клієнтів Experian, телефонували в сервісну службу підтримки, що призвело до витоку конфіденційних даних клієнтів. Хакери можуть використовувати вихідні дані для обходу IT-периметрів і завершення початкових етапів кібератаки. Фішингові атаки електронною поштою є більш розширеними, оскільки вони можуть швидше охопити більшу кількість жертв. Найпоширеніший

тип - це риболовля електронною поштою. Фішингові електронні листи виглядають як звичайні повідомлення від надійного джерела, але містять заражені посилання. Якщо користувач переходить за такими посиланнями, на його пристрої встановлюється шкідливе програмне забезпечення або завантажується розроблена веб-сторінка, призначена для крадіжки даних.

3. *Повторне використання пароля.*

Користувачі, як правило, вибирають один і той самий пароль для всіх своїх облікових записів, тому часто один скомпрометований пароль призводить до компрометації кількох цифрових активів. Оскільки викрадені дані клієнтів часто продаються на форумах у темному Інтернеті, це зловживання може призвести до значних витоків даних. Також часткова інформація про пароль класифікується як вік даних, останній решта паролів розкривається за допомогою грубої сили, якщо хакери потребують спеціального програмного забезпечення для введення паролів облікових записів. Наявність часткової інформації про пароль дозволяє кіберзлочинцям швидше досягти успіху, потім їм потрібно менше спроб, щоб ввести пароль.

4. *Фізична крадіжка пристроїв, що складається з конфіденційної інформації*

Пристрої компанії розробляють конфіденційну інформацію, і якщо ці пристрої відправляються до чужих рук, вони можуть бути використані для компрометації даних.

5. *Вразливість програмного забезпечення.*

Вразливості програмного забезпечення, такі як експлуатувати нульовий день, створюють зручні способи доступу до конфіденційних ресурсів. Це дозволяє зловмисникам оминути початкові етапи кібератаки і відразу перейти до фази ескалації привілей (по суті, до фази, що передує витоку даних).

6. Використання попередньо встановлених (за замовчуванням) паролів

Багато стандартних заводських облікових даних за замовчуванням, які постачаються з новими пристроями, широко відомі. У зв'язку з цим стандартні облікові дані за замовчуванням класифікуються як витік даних.

Пристрої IOT найбільше прогресують від цієї ситуації. Якщо ці пристрої

купуються, вони постачаються зі стандартною комбінацією для входу для швидкого налаштування [12].

Дані приклади є порушенням конфіденційності, цілісності та доступності чутливої інформації, тому для запобігання кіберінцидентам в систему безпеки інтегруються Data Leak Prevention (DLP) системи. Принцип DLP працює в безперервному аналізі потоків даних, які перетинають межі захищеної інформаційної мережі: DLP-система може відстежувати багато параметрів, таких як зв’язок, введення даних і передача файлів, а також час роботи пристроїв і запущених додатків [2].

Однак для того, щоб проаналізувати дані, система повинна спочатку отримати доступ до них. Це можна зробити двома способами. Серверний - система відстежує трафік на рівні сервера, де комп'ютер "спілкується" із зовнішнім світом. Агентський - на комп'ютері встановлена спеціальна програма-агент, яка надсилає дані для аналізу.

Метою даної роботи є використання рішення Symantec DLP від вендора Broadcom.

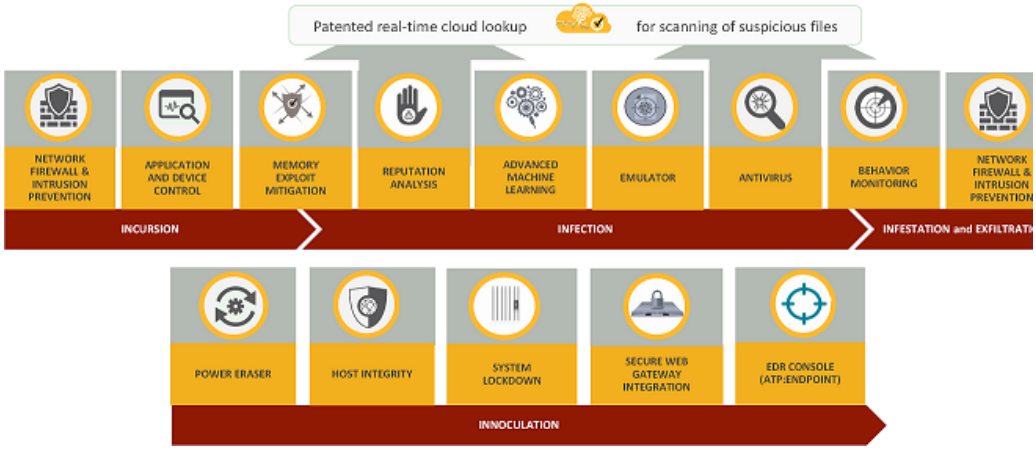

Рис.1.1. Портфель DLP рішення

В умовах стрімкого зростання кіберзлочинності та збільшення збитків від витоків даних, що сягнули рекордних показників, значення комплексних рішень для захисту інформації, таких як Symantec Data Loss Prevention від Broadcom, стає надзвичайно високим. Цей розділ підкреслює важливість інтегрованих систем захисту в контексті широкого спектру викликів безпеки, які охоплюють не тільки

технологічні аспекти, такі як неправильна конфігурація програмного забезпечення, вразливості та фізична крадіжка пристроїв, але й людський фактор, включаючи соціальну інженерію та повторне використання паролів.

Усвідомлення різноманітності загроз та розуміння, що витоки даних можуть мати різне походження та наслідки, підкреслює необхідність застосування рішень, які здатні не лише виявляти та блокувати потенційні витоки, але й аналізувати потоки даних для попередження кіберінцидентів. Symantec DLP пропонує такий комплексний підхід, забезпечуючи захист на рівні сервера та через агентське програмне забезпечення на кінцевих точках, тим самим відповідаючи на виклики сучасного кіберпростору.

Таким чином, враховуючи постійне зростання загроз та збитків від витоку даних, впровадження та ефективне використання рішень, таких як Symantec DLP, стає ключовим фактором для забезпечення безпеки конфіденційної інформації в організаціях різних масштабів, допомагаючи мінімізувати ризики та наслідки потенційних кібератак.

1.2 Аналіз інцидентів та причин витоків даних

За останніми даними 2022 року наймасштабнішими витоками даних були:

А) Crypto.com – 17 січня 2022 року

Crypto.com характеризував дану подію як "інцидент" і заперечив заяву про викрадання даних або коштів. Однак через кілька днів ситуація змінилася. Компанія визнала факт атак і компенсувала користувачам збитки на суму близько 33 доларів США.

Даний кіберінцидент включав в себе втрату доступу легітимних користувачів до 500 криптогаманців. За попередніми коментарями – потенційно шкідливе програмне забезпечення було розповсюджене на кінцевих точках, що і слугувало успіхом кіберзлочинців [3].

Б) Microsoft – 20 березня 2022 року

Скріншоти, опубліковані в групі Telegram Lapsus$, показують, що вони

зламали Microsoft і скомпрометували Cortana, Bing і кілька інших продуктів.
Даний кіберінцидент за офіційними даними включав в себе витік первинного коду, що дало можливість зловмисникам проникнути в систему компанії без використання методів підвищення привілеїв та ін.

В) МКЧХ – січень 2022

Конфіденційні дані тисячі людей були викрадені, значна частина даних жертви зникла або підтвердилася знищенням, і визнано, що можуть бути наступні витоки. Червоний Хрест блокував атаку і вимкнув свої сервери, щоб розслідувати це кричуще політичне порушення, але винуватці не були встановлені.
Даний кіберінцидент включає в себе отримання доступу з подальшим знищенням або передачею конфіденційних даних, що сигналізує про уразливості в системі безпеки без активного запобігання і протидії.

Г) FlexBooker – січень 2022

До злому була причетна хакерська група під назвою Uawrongteam. Група зламала AWS-сервери FlexBooker і встановила шкідливе програмне забезпечення, щоб отримати контроль над системами компанії. Даний кіберінцидент включає в себе поширення зловмисного програмного забезпечення на хмарних серверах компанії, що привело до повної втрати контролю, як результат – витік даних з метою перепродажу конкурентам.

Д) Cash App – квітень 2022

Зловмисник мав значний вплив на бізнес. Атака була спрямована на імена клієнтів, інформацію про торговельні дії, номери рахунків, вартісні портфелі та іншу конфіденційну фінансову інформацію. Даний кіберінцидент включає підготовчу стадію – розвідка, що і активно використалася для успіху кіберзлочинця [3]. З урахуванням та аналізом даних кіберінцидентів комплексний підхід до безпеки є критичним місцем у сучасному цифровому середовищі. Використання рішень забезпечення інформаційної безпеки може зменшити ризик виникнення нових кіберінцидентів. Велику роль відіграють системи запобігання втраті даних (DLP) у попередженні кіберінцидентів:

Виявлення та моніторинг конфіденційної інформації:

DLP-системи в режимі реального часу виявляють переміщення конфіденційної інформації та повідомлення, яке було переміщено в несанкціоноване місце або скопійовано.

Захист від витоку даних:

Політики DLP можуть бути впроваджені, щоб застосувати, як обробляється і передається конфіденційна інформація, запобігаючи ненавмисному або небажаному витоку.

Аналіз контенту:

Системи DLP виконують метод-аналіз контенту для виявлення конфіденційних даних, навіть якщо вони не вказані у вигляді конкретного шаблону або ключового слова.

Контроль доступу:

Правила контролю доступу, засновані на чутливості та класифікації даних, можуть бути встановлені, щоб обмежити доступ до конфіденційної інформації лише авторизованим користувачам.

Інтеграція з системами безпеки

DLP-системи можуть бути інтегровані з іншими системами безпеки, такими як антивірус і система виявлення вторгнень, щоб забезпечити комплексний захист від різних загроз.

Захист у хмарних середовищах.

Рішення DLP може захистити конфіденційну інформацію в хмарних середовищах, де даними керує зовнішній постачальник послуг.

Виявлення та блокування небезпечних дій

Системи DLP можуть виявляти незвичайні шаблони або небажані дії, такі як спроби копіювання конфіденційних даних на зовнішніх пристроях, і автоматично блокувати або обмежувати ці дії.

Вивчення зашифрованого трафіку:

Деякі системи DLP можуть досліджувати зашифрований трафік, виявляти та відстежувати конфіденційну інформацію, яка міститься в зашифрованих повідомленнях.

Координація користувачів:

Ефективність системи DLP можна підвищити, ідентифікуючи користувачів, які мають доступ до конфіденційної інформації, та проводячи навчання та тренінги з питань безпеки.

Автоматизоване реагування:

Деякі системи DLP можуть автоматизувати реагування на ситуації ризику, що дозволяє швидше реагувати на виявлені загрози.

Завдяки даному функціоналу системи DLP виконують ключову роль у запобіганні потоку даних і забезпечують комплексний захист конфіденційної інформації в організаціях усіх типів.

Поєднання DLP з іншими системами інформаційної безпеки може підвищити ефективність заходів безпеки та знизити ризики.

Інтеграція DLP із системою SIEM (Security Information and Event Management) дозволяє централізовано аналізувати та відслідковувати події, пов’язані з витоком даних; SIEM може автоматично виявляти події, які порушують політику DLP, і допомагати реагувати на загрози.

DLP можна з’єднувати з брандмауерами та проксі-серверами для контролю передачі даних у мережі на різних рівнях. Він може блокувати спроби витоку конфіденційної інформації на мережевому рівні та захистити дані від несанкціонованого витоку.

Інтеграція DLP з антивірусними системами дозволяє виявляти та блокувати витоки даних, спричинені шкідливими програмами. Інтеграція з антивірусними системами дозволяє захистити інформацію від широкого спектру загроз.

Інтегруючи DLP з електронною поштою безпеки та системами шлюзів, можна побачити та запобігти витоку інформації через електронну пошту. Безпека електронної пошти може бути досягнута за допомогою контролю вкладень, фільтрації вмісту та виявлення конфіденційної інформації.

Інтеграція з системами контролю доступу може заборонити або обмежити доступ до конфіденційних даних користувачам без відповідного дозволу. Інтеграція з системами єдиного входу (SSO) також може покращити контроль

доступу та спростити процес автентифікації.

DLP можна з’єднувати з іншими системами, такими як системи виявлення вторгнення (IDS/IPS) і системи запобігання витоку інформації, щоб координувати дії та реагувати на інциденти в режимі реального часу. Ці комбіновані методи можна використовувати для створення комплексного підходу до захисту інформації, зниження ризику витоку даних і підвищення загального рівня безпеки організації.

Висновок до цього розділу підкреслює критичну необхідність комплексного підходу до забезпечення інформаційної безпеки в умовах сучасного цифрового середовища. Наведені приклади масштабних витоків даних в 2022 році, такі як інциденти з Crypto.com, Microsoft, МКЧХ, FlexBooker та Cash App, вказують на різноманітність загроз і методів, які використовують кіберзлочинці для отримання несанкціонованого доступу до конфіденційної інформації. Це підкреслює важливість впровадження систем запобігання втраті даних (DLP), які здатні виявляти, моніторити та захищати від потенційних витоків на різних етапах обробки інформації.

DLP-системи, інтегровані з іншими інструментами безпеки, такими як SIEM, антивірусні програми, системи контролю доступу та шлюзи електронної пошти, забезпечують багаторівневий захист від різних видів загроз. Це включає в себе не лише технічні заходи, як-от аналіз контенту і контроль доступу, але й адміністративні та організаційні заходи, такі як навчання користувачів та автоматизоване реагування на інциденти.

Таким чином, з огляду на складність та масштабність потенційних кіберзагроз, а також на прикладах значних фінансових та репутаційних втрат, які можуть виникати внаслідок витоку даних, впровадження та ефективне використання DLP-систем є необхідним елементом стратегії інформаційної безпеки кожної організації. Це дозволяє не лише попереджати витоки даних, але й забезпечує швидке виявлення та реагування на загрози, знижуючи таким чином потенційні збитки та сприяючи підтримці високого рівня довіри та безпеки в цифровому світі.

1.3 Оцінка ефективності та недоліків використання Symantec DLP

Symantec Data Loss Prevention (DLP) - це програмне забезпечення, призначене для виявлення та запобігання витоку конфіденційної інформації в компаніях і організаціях.

Рис.1.2. Symantec DLP

Дане програмне забезпечення є одним з найкращих на ринку через свою засвідчену ефективність та актуальність. Особливо варто звернути увагу на його ключові складові:

Виявлення та класифікація даних. Symantec DLP може виявляти конфіденційні дані за допомогою різних методів, зокрема аналізу контенту, контекстної класифікації та машинного навчання.

Можна встановити політику для виявлення та класифікації конфіденційної інформації. Задля покращення функціонування даної складової потрібна поточна налаштування та підтримка точності виявлення. Моніторинг і блокування потоку даних. Швидке реагування на зловживання або спроби витоку інформації, що дає групі з кіберзахисту підприємства чи організації можливість швидко встановлювати причини та виконавця даного порушення. Хоча в даному процесі може виникати велика кількість хибнопозитивних або хибнонегативних сигналів, у такому випадку конфігурація потребує оптимізації. Інтеграція та аналіз. Може бути інтегрована з іншими системами безпеки, такими як SIEM (Security Information and Event Management) задля підвищення рівня реагування на потенційні загрози. Надає звітність та аналітичні дані для покращення стратегій безпеки. Хоча сама процедура інтеграції є складною та може вимагати додаткових

зусиль і ресурсів. Інтерфейс користувача та адміністрування. Інтуїтивно зрозумілий інтерфейс для адміністраторів та користувачів. Зручна адміністративна панель для налаштування та моніторингу. Ресурсні витрати - ефективне використання ресурсів та масштабованість для великих організацій. Оптимізована продуктивність при обробці великих обсягів даних. Єдиним нюансом є високі витрати, які можуть бути проблемою для MSP (Manager Service Provider).

DLP-системи вибирають три методи ідентифікації: імовірний, детермінований і комбінований. Системи, засновані на першому методі, складаються на лінгвістичний контент-аналіз і цифрове дактилоскопіювання даних. Такі системи прості у впровадженні, але характеризуються недостатньою ефективністю та високим рівнем помилкових спрацьовувань. Системи, що вибирають детермінований підхід (файлові теги), дуже надійні, але негнучкі. Оптимальне рішення проблеми захисту конфіденційності інформації може забезпечити уніфікований підхід, коли метод розпізнавання підкріплений аудитом середовища зберігання та обробки даних [4].

Існує два основних підходи до контент-аналізу. Перший підхід базується на фільтрації контенту, що наповнює зміст інформації. Це означає, наприклад, що при перевірці конфіденційності стандартних офісних документів у форматі .doc система спочатку переводить їх у текстовий формат, а потім на основі попередньо підготовлених даних видає судження про цей текст. Контекстна фільтрація використовує принципово інший метод. Система використовує контекстну інформацію, в якій перевіряється інформація. Вона витягує теги файлів, вивчає їх розмір і аналізує поведінку користувачів.

Компанія Forrester Research розробила чотири критерії для оцінки DLP-продуктів.

- Перший критерій - багатоканальність: DLP-рішення не повинні зосереджуватися лише на одному каналі витоку. Це має бути комплексне рішення, яке охоплює максимальну кількість каналів, включаючи моніторинг електронної пошти, Інтернету, обмін миттєвими повідомленнями та файлові транзакції.

- Другий критерій - інтегроване управління. Зазвичай їх три: сервер

управління для зберігання групових політик користувачів, пристрій для моніторингу витоків у мережі та агенти для робочих станцій, серверів і файлових сховищ. Основна вимога другого критерію полягає в тому, що цими трьома компонентами можна керувати з єдиної консолі.

- Третій критерій - активний захист. Система повинна вміти фіксувати та запобігати старінню конфіденційної інформації. Четвертим критерієм є категоризація інформації відповідно до змісту та контексту. Вік чутливої інформації залежить не тільки від вмісту інформації, що передається, але й від контексту, в який вона передається (користування будь-яким протоколом, яка використовується програма, від вашого користувача, зв'язки тощо) [4].

Базуючись на даній інформації Symantec DLP може бути потрібним рішенням для захисту конфіденційної інформації через:

Уніфікований підхід. Symantec DLP використовує комбінований підхід до ідентифікації, включаючи ймовірні, детерміновані, та аудит збереження середовища та обробку даних. Це дозволяє системі бути більш гнучкою та адаптивною до різноманітних сценаріїв витоків даних.

Метод розпізнавання. Symantec DLP використовує лінгвістичний контент-аналіз та цифрове дактилоскопіювання даних, що дозволяє виявляти чутливі (персональні інформація, медичні записи, фінансові дані, банківські реквізити, соціальні номери, паспортні дані) дані та класифікувати їх. Це підсилює ефективність системи в процесах виявлених витоків.

Контекстний аналіз. Система використовує контекстну інформацію, що дозволяє більш точно визначити, коли і які дані можуть бути виявлені витокованими, зменшуючи кількість фальсифікаційних сигналів .

За критеріями, визначеними компанією Forrester Research, Symantec DLP можна визнати ефективним рішенням завдяки багатоканальності, інтегрованому управлінню та категоризації інформації.

У першому випадку система охоплює інші канали витоку, такі як моніторинг електронної пошти, Інтернету, обміну миттєвими повідомленнями та файлами транзакцій.

У другому випадку система забезпечує єдину консоль для керування сервером управління, пристроєм для моніторингу та агентами.

У тертьому випадку система може фіксувати та запобігати старінню конфіденційної інформації.

До того ж, завдяки категоризації інформації відповідно до змісту та контексту система враховує не лише вміст інформації, але й передає контекст.

З урахуванням проблем у захисті від витоків даних та особливостей Symantec DLP для їхнього вирішення - дана система може бути високоефективним інструментом для захисту конфіденційної інформації в організації [16].

Переваги Symantec Data Loss Prevention (DLP) охоплюють широкий спектр функціоналів, які роблять його надійним рішенням для захисту конфіденційної інформації в організаціях. Найважливішими перевагами є:

Гнучкість та адаптивність. Symantec DLP застосовує уніфікований підхід до ідентифікації даних, який включає імовірні, детерміновані методи та аудит середовища зберігання та обробки даних. Це дозволяє системі бути гнучкою та адаптивною до різноманітних сценаріїв витоків даних, забезпечуючи ефективний захист.

Продвинуті методи виявлення. Використання лінгвістичного контент-аналізу та цифрового дактилоскопіювання дозволяє системі ефективно виявляти та класифікувати чутливі дані. Такі методи значно підсилюють точність виявлення та класифікації конфіденційної інформації.

Зменшення хибних спрацьовувань. Контекстний аналіз інформації дозволяє системі більш точно ідентифікувати потенційні витоки, зменшуючи кількість хибнопозитивних та хибнонегативних спрацьовувань. Це забезпечує вищу ефективність моніторингу та відповіді на інциденти.

Багатоканальність. Система забезпечує захист через різні канали комунікації, включаючи електронну пошту, Інтернет, обмін миттєвими повідомленнями та файлові транзакції, що робить її комплексним рішенням для захисту інформації.

Інтегроване управління. Централізоване управління дозволяє

адміністраторам легко налаштувати політики безпеки, моніторити події та вживати заходів щодо захисту даних через єдину адміністративну панель.

Активний захист - здатність фіксувати та запобігати старінню конфіденційної інформації забезпечує активний захист даних, зменшуючи ризики пов’язані з витоком інформації.

Завдяки цим перевагам Symantec DLP стає високоефективним інструментом для організацій, які прагнуть захистити свою конфіденційну інформацію від небажаних витоків.

Незважаючи на значні переваги Symantec Data Loss Prevention (DLP), існують певні недоліки та виклики, пов'язані з впровадженням та використанням цього рішення. Перш за все, складність налаштування та управління системою може стати великим бар'єром для організацій з обмеженими технічними ресурсами або знаннями. Потреба в детальному розумінні внутрішніх процесів для ефективного налаштування політик може вимагати значних зусиль і часу від адміністраторів. Крім того, процес інтеграції Symantec DLP з іншими системами безпеки може бути складним і вимагати додаткових зусиль і ресурсів для забезпечення сумісності та оптимального функціонування.

Ще одним важливим недоліком є висока вартість ліцензій та необхідність вкладення в апаратне забезпечення, що може стати значним фінансовим навантаженням для малих та середніх підприємств. Вартість може особливо швидко зростати для великих організацій з великим обсягом даних для моніторингу та аналізу.

Висока чутливість системи може призвести до великої кількості хибнопозитивних сигналів, що, у свою чергу, вимагає додаткових ресурсів для перевірки та корекції. Це може призвести до збільшення навантаження на команду з кібербезпеки та зниження загальної продуктивності.

Окрім того, незважаючи на різноманітність функцій, можуть виникати випадки, коли специфічні потреби підприємства не повністю покриваються можливостями Symantec DLP, що вимагає пошуку додаткових рішень або кастомізації існуючої системи.

Таким чином, попри значні переваги Symantec DLP у захисті конфіденційних даних, важливо ретельно оцінювати згадані вище недоліки та виклики при розгляді цього рішення для впровадження в організації.

Symantec Data Loss Prevention представляє собою комплексне рішення для захисту конфіденційної інформації в компаніях та організаціях, надаючи потужні інструменти для виявлення, моніторингу, блокування потоку даних та їх класифікації. Завдяки гнучкості, адаптивності, продвинутим методам виявлення та контекстного аналізу, Symantec DLP забезпечує високий рівень захисту інформації. Система охоплює різноманітні канали витоку даних і забезпечує інтегроване управління через єдину адміністративну панель, що значно спрощує моніторинг та відповідь на потенційні загрози. Однак, слід зазначити, що висока вартість, складність управління та інтеграції, а також потенціал високої кількості хибнопозитивних сигналів можуть стати викликами для організацій при впровадженні та експлуатації системи. Важливо ретельно зважити ці недоліки поряд з перевагами Symantec DLP, щоб забезпечити ефективне використання ресурсів і максимальну користь від впровадження системи для захисту важливих даних.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВІД ВИТОКУ ДАНИХ НА ОСНОВІ SYMANTEC DLP

2.1 Дослідження інцидентів витоку даних та атак на системи зберігання даних

Витік інформації є серйозною загрозою для організацій та користувачів, оскільки він може призвести до різних негативних наслідків. Витік інформації може стати причиною втрати конфіденційності даних, порушення правил та нормативів, втрати довіри клієнтів та партнерів, фінансових втрат і репутаційних збитків. Це може також призвести до втрати конкурентного переваги, порушення законодавства та накладення штрафів, а також втрати важливої інформації, що може бути використана зловмисниками для здійснення шкідливих дій. Тому захист від витоку інформації є важливою складовою інформаційної безпеки для будь-якої організації.

Атаки на системи зберігання даних - це спроби несанкціонованого доступу до інформації або зміни її, здійснювані зловмисниками з метою заволодіння цією інформацією або завдання шкоди організації. Ці атаки можуть приймати різні форми, включаючи хакерські атаки, віруси, фішинг, DDoS-атаки та інші. Атаки на системи зберігання даних можуть мати серйозні наслідки, такі як втрата конфіденційної інформації, втрата фінансових активів, порушення нормативних вимог, втрата репутації та інші негативні наслідки. Тому необхідно вживати заходів для захисту систем зберігання даних від таких атак, включаючи застосування відповідних технологій та політик безпеки, регулярне оновлення програмного забезпечення та виконання інших профілактичних заходів.

Витоки даних та атаки на системи зберігання даних є серйозною загрозою для інформаційної безпеки. Ці інциденти можуть призвести до втрати конфіденційної інформації, порушити конфіденційність користувачів і спричинити значні збитки як для компаній, так і для приватних осіб. Для запобіганню даних інцидентів коректним є побудова надійної системи захисту баз даних, яка включає

в себе сукупність методів, програмних засобів, процесів, програм і технік, що застосовуються для захисту інформації, яка зберігається, і запобігання несанкціонованому електронному доступу, модифікації, випадковому розкриттю, пошкодженню, знищенню або копіюванню [5]. Найчастішими атаками задля отримання конфіденційних даних виступають:

Фішинг є формою соціально-інженерної атаки, де зловмисники користуються маніпуляцією та обманами, щоб отримати конфіденційну інформацію від користувачів. Цей вид атаки ґрунтується на психологічних та технічних методах введення наявних жертв в оману, щоб вони надали доступ до своїх облікових даних.

Malware, або шкідливе програмне забезпечення, представляє собою код, який розроблено з наданням завдати шкоди або здійснити незаконний доступ до системи. Це може включати в себе віруси, трояни та інші форми атак, які інфікують системи для збереження конфіденційної інформації або завдання інших шкідливих наслідків.

Витік даних часто виникає через дефіцит заходів безпеки, таких як недостатнє управління доступом, неактуалізовані заходи безпеки, слабкі паролі або недостатнє шифрування. Аналіз недоліків у системах безпеки є ключовим для запобігання подібним інцидентам.

Соціальна інженерія використовує психологічні та маніпулятивні методи для отримання конфіденційної інформації. Атаки цього типу можуть включати в себе використання довіри або створення обманливих сценаріїв для здійснення атаки.

Ransomware – це форма шкідливого програмного забезпечення, яке шифрує дані або блокує доступ до систем, а злочинці вимагають викупу для їх відновлення. Це залежить від ефективності шифрування та можливої декриптації.

Інсайдерські загрози викликають, коли особа всередині організації починає дії, спрямовані на шкоду даним чи системам. Це може бути через недобросовісних працівників або недостатній контроль доступу.

DDoS-атаки:

Атаки на перевантаження мережевих ресурсів, відомі як DDoS, створюють

неспроможність системи обслуговувати легітимний трафік через переповнення або сервер мережі.

Злам паролів:

Brut-force або давні паролі включають в себе спробу отримати доступ до системи, перебираючи паролі або використовуючи викрадені облікові дані.

Дані атаки є доволі поширеними в інформаційному просторі, деякі організації та підприємства відчули на собі їх вплив:

У 2016 році фішери використовували фішингові електронні листи, замасковані під повідомлення Google, для реєстрації облікових даних користувачів. Список містив посилань на фальшиві веб-сайти для введення логіна та пароля. У результаті було скомпрометовано облікові записи для подальшого продажу персональних даних.

Під час атаки на Sony Pictures у 2014 році хакери використовували шкідливий код для отримання конфіденційної інформації, в тому числі невиданих фільмів, електронних листів та облікових записів. У результаті більшість фільмів було розповсюджено на піратських джерелах, дані користувачів розміщені на чорному ринку.

У 2017 році недостатні заходи безпеки в Equifax призвели до витоку персональних даних європейських користувачів, включаючи номери соціального страхування та інші дані конфіденційності. Через недотримання політик безпеки було виявлено зловмисниками уразливості в системі, що привело до масштабного витоку.

Cambridge Analytica використовувала соціальну інженерію та обман, щоб отримати доступ до даних більшої кількості користувачів Facebook і створити політичні профілі виборців [15]. Через слабке уявлення користувачів про можливі пастки в інформаційному просторі зловмисники отримали доступи до облікових записів популярної соціальної мережі для виконання політичного замовлення.

Під час атаки WannaCry у 2017 році комп’ютерні дані були зашифровані, а для їх відновлення вимагали викуп. В даному інциденті використовувався шкідливий програмний код, що включав в себе шифрувальник з асиметричним

шифруванням та вимагач, що дало зловмисниками отримати певну кількість грошового забезпечення без повернення користувачам можливості отримання доступу до власних персональних даних.

Едвард Сноуден, колишній співробітник Агентства національної безпеки США (АНБ), надав у ЗМІ конфіденційну інформацію про стеження за інтернет-користувачами. Через порушення Non-disclosure agreement (NDA) співробітник поширив у мережу інформацію, яка може бути використаною зловмисниками у майбутньому.

Під час атаки Mirai у 2016 році ботнет зі зламаних пристроїв перевантажив сервери і зробив багато веб-сайтів недоступними. Використання DDoS- атак є доволі частим через їхню успішність, чому слугує доволі повільна реакція команди з реагування на кіберінциденти та також недотримання політик безпеки для пристроїв в інфраструктурі підприємтсва або організації.

У 2012 році LinkedIn зазнав витоку даних, коли в результаті атаки на базі даних були викрадені хеші паролів користувачів. У даному інциденті було втрачено конфіденційну інформацію користувачів, що надає можливості зловмисникам отримати доступ до облікового запису, якщо додатково буде проведено підбір логіну з використанням інструментів Brut-force.

Задля попередження і мінімізування ризиків від даних інцидентів велику роль відіграють DLP-системи

- аналіз вихідного трафіку електронної пошти та веб-сайтів для виявлення надто підозрілих або фішингових повідомлень. Дана функція дозволяє заблокувати доступ до шкідливих посилань та завершити спробу атаки ще до того, як користувачі нададуть дані свого облікового запису.

- виявляння аномального трафіку та активність шкідливого коду, вчасно виявляючи та блокуючи атаки. Також можуть установлюватися правила для блокування вихідних шкідливих файлів чи обмеження передачі конфіденційних даних.

- встановлення політики щодо регулювання типів даних, що можуть бути передані або збережені. Дана функція дозволяє виявляти та блокувати

ненормативні передачі чутливих даних, запобігаючи витокам даних через недоліки в безпеці.

- аналіз тексту повідомлень та комунікацій для виявлення можливих ознак соціальної інженерії, таких як спроба отримати дані конфіденційності.

Автоматичне виявлення та блокування таких спроб може бути реалізовано через DLP.

- визначення та фільтрування трафіку, з метою ідентифікації атаки на перезавантаження та забезпечити доступ лише легітимним користувачам. Дана функція може допомогти у запобіганні відмові в обслуговуванні внаслідок DDoS-атак.

-використання аналізу поведінки та моніторингу активності для виявлення надто агресивних або перевірених спроб введення паролів. Також можна визначати та блокувати злам паролів через брутфорс атаки.

Інтеграція систем DLP у комплексну стратегію інформаційної безпеки може ефективно знизити ризик втрати даних та забезпечити високий рівень захисту від різноманітних загроз.

Загрози витоків даних та кібератак на системи зберігання даних становлять серйозний ризик для інформаційної безпеки. Ці інциденти можуть призвести до втрати конфіденційної інформації та нанести значні збитки компаніям і приватним особам. Для запобігання таким інцидентам важливо вживати надійні заходи безпеки даних, включаючи побудову комплексної системи захисту баз даних та інтеграцію DLP-систем. Через функціонал таких систем можна виявляти та блокувати різноманітні загрози, такі як фішингові атаки, шкідливе програмне забезпечення, витоки даних через недоліки в безпеці, соціальна інженерія та програми здирники. Інтеграція DLP у комплексну стратегію інформаційної безпеки може ефективно знизити ризики втрати даних та забезпечити високий рівень захисту від кіберзагроз.

2.2 Налаштування та аналіз основних інструментів Symantec DLP

Компанія Symantec присутня на ринку DLP протягом багатьох років і є загальновизнаним світовим лідером на ринку DLP. Рішення Symantec вже багато років поспіль займаються лідируючі позиції в дослідженнях Gartner в області запобігання втраті даних, чутливих до контексту. Рішення Data Loss Prevention (DLP) від Symantec призначене для використання в організаціях практично будь-якого розміру, від малого бізнесу (100+ користувачів) до великих підприємств (10 000+ або 100 000+ користувачів). Найбільше розгортання Symantec DLP відбулося в компаніях з більш ніж 300 000 співробітників, але, на жаль, назви цих компаній не розголошуються. Найбільш відкритим користувачем є консалтингова компанія Deloitte з приблизно 180 000 співробітників [6].

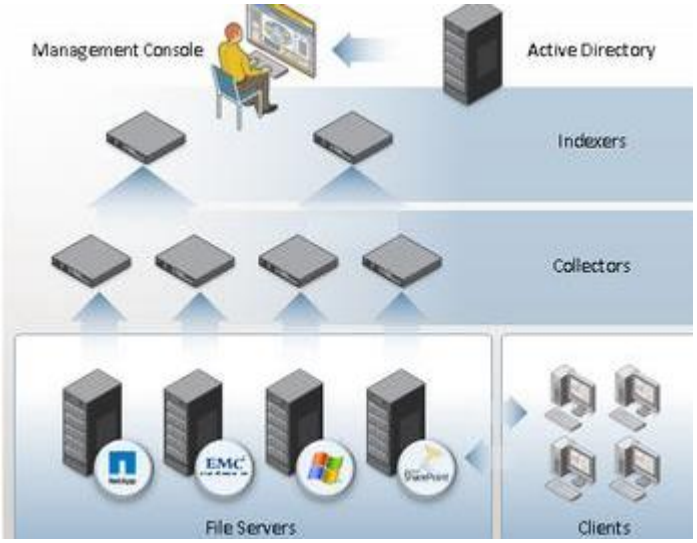

Рис. 2.1. Прикладне використання DLP в компаніях

Дане рішення спеціалізується на таких основних функціях:

1) Виявлення конфіденційної інформації у відкритих доступних файлових сховищах, веб-серверах, базах даних, електронних поштових системах документообігу;

2) Захист конфіденційної інформації на робочих станціях, ноутбуках, у тому числі за межами внутрішньої мережі;

3) Управління електронною поштою, відправленою та отриманою через

мобільний додаток, хмарні веб-сервіси.

Symantec DLP є розподіленою модульною комплексною системою, склад якої наведено нижче в таблиці 2.1.

Таблиця 2.1

Складові рішення Symantec DLP

Група модулів	Функціональна складова	Призначення
Enforce platform	Symantec DLP Enforce server	Центральна платформа керування Symantec DLP
	Oracle Database for Symantec DLP	База даних для збереження звітності, інцидентів, конфігурації та налаштувань системи
Endpoint	Symantec DLP Endpoint Discover	Виявлення конфіденційних даних на локальних дисках робочих станцій та ноутбуків
	Symantec DLP Endpoint Prevent	Контроль та запобігання витокам даних з робочих станцій ноутбуків
	Symantec DLP Network Discover	Виявлення конфіденційних даних, які розташовані на корпоративних сховищах інформації
	Symantec DLP Data Insight	Відстеження використання інформації, яка розміщена на сховищах, контроль прав доступа, визначення

Storage		власників даних
	Symantec DLP Self-Service Remediation portal	Залучення власників до виправлення помилок розміщення конфіденційної інформації на файлових серверах та порталах Sharepoint
	Symantec DLP Network Protect	Автоматичне виправлення розміщення конфіденційної інформації на файлових серверах та порталах Sharepoint
	Symantec DLP Classification Server	Класифікація електронної пошти при розміщенні в архіви та журнали Symantec Enterprise Vault
Network	Symantec DLP Network Monitor	Контроль переміщення конфіденційних даних по мережевим каналам зв’язку (пасивний)
	Symantec DLP Network Prevent for Web	Контроль переміщення конфіденційних даних по мережевим каналам зв’язку(активний з можливістю блокування та аналізу шифрованого трафіку)
	Symantec DLP Network Prevent for Mail	

Mobile	Symantec DLP Mobile Prevent	Контроль інформації, що відправляється з мобільних пристроїв
	Symantec DLP Mobile Email Monitor	Контроль інформації, що завантажується на мобільні пристрої через пошту
Symantec Management Platform	Symantec DLP IT Analytics	Додатковий модуль для розширеної звітності
	Symantec DLP Integration Component	Інструмент автоматичного розгортання агентів та контролю їх роботи

На відміну від інших рішень, які запроваджуються як програмно-апаратні комплекси, Symantec DLP є набором програмного забезпечення, який готовий до встановлення. Усі модулі можливо встановити на будь-яке апаратне забезпечення, що відповідає системним вимогам, особливо на віртуальні сервери.

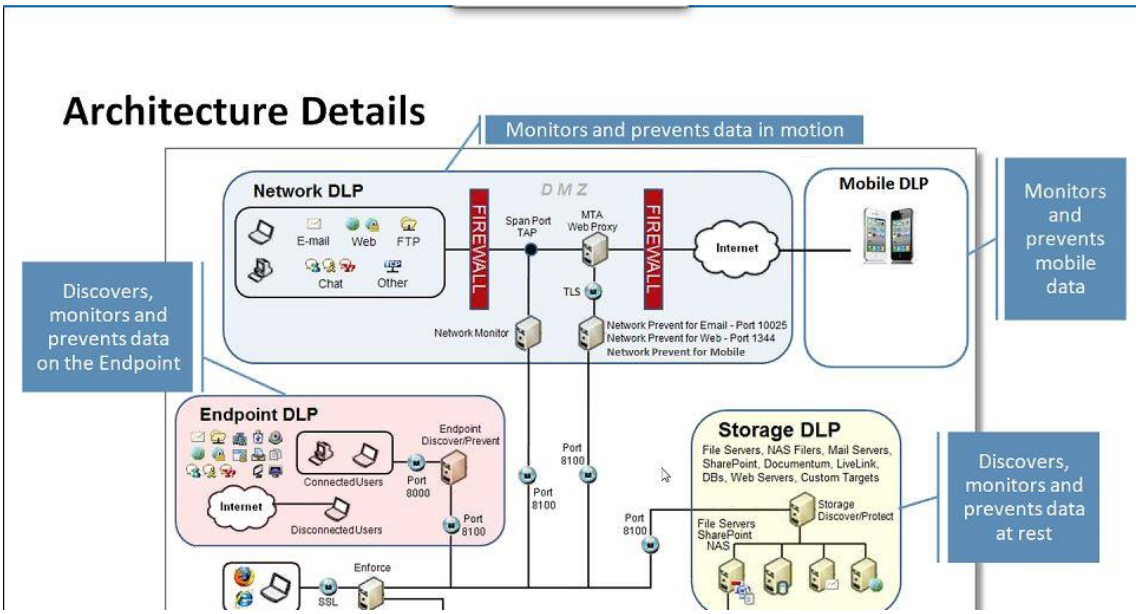

Рис.2.2. Схема роботи Symantec DLP

Функціональні можливості рішення включать в себе вирішення двох основних задач:

А) виявлення та блокування передачі конфіденційної інформації, яка зберігається в повідомленнях з пошти, веб-трафіку, при копіюванні в буфер обміну, при записі на локальні або компакт диски, в документах в інтернеті. Для вирішення даної задачі DLP-система включає в себе декілька технологій виявлення конфіденційної інформації: Described Content Matching (DCM), Exact Data Matching(EDM), Indexed Document Matching(IDM), Vektor Machine Learning (VML).

Б) оперативне реагування на події, які пов’язані з обміном, передачею або виявленням конфіденційної інформації на заборонених ресурсах відповідно до політик. Для їх створення можливо використовувати готові шаблони, які можна використати без змін або змінювати відповідно до поточних потреб. У випадку спрацювання політики – потенційного або реального інциденту ІБ, Symantec DLP вмикає механізм повідомлення та контролю розслідування інцидентів. Завдяки використанню вбудованих засобів для візуалізації інциденту аналітики чітко розуміють причини виникнення, місце виникнення та хто ініціював дане сповіщення від системи безпеки.

Часто для покращення базового функціоналу рішення використовують інші продукти вендора задля забезпечення безпеки від витоку даних та їх коректного збереження:

- Symantec Backup Exec System Recovery для сканування образів резервних копій на вміст конфіденційної інформації.

- Symantec Endpoint Encryption для примусового шифрування даних на основі політик при копіюванні файлів на знімні носії в режимі реального часу.

- Symantec FileShare Encryption для розшифрування та аналізу тексту в зашифрованих документах.

- Symantec Mobile Management для використання параметрів VPN на мобільних пристроях, відправки попередження при спробі зміни профілю пристрою.

Також розробники додали можливість інтегрувати дане рішення зі сторонніми такими як:

- Мережеві каталоги LDAP (Microsoft Active Directory).
- Поштові сервіси (Microsoft Exchange).
- Проксі-сервери (McAfee Web Gateway, Microsoft TMG).
- SIEM-системи (при використанні листів, syslog-повідомлень, repoting API).

Щодо системних характеристик за основу взято середнє підприємство, на якому розгортається DLP-система, приблизно 1000-10000 хостів. Платформа керування Enforce та Oracle встановлюється на один сервер, кожен сервер виявлення встановлюється окремо на свій сервер, який може бути або фізичним, або віртуальним:

1) Сервер Enforce+СУБД Oracle: 2xCPU 3,0 ГГц 1 ядро, 6-8 ГБ ОЗУ, 500 ГБ HDD Raid 1+0 або Raid 5, 1 NIC Ethernet 100/1000 мідний або оптичний.

2) Сервери виявлення: 2xCPU 3,0 ГГц 1 ядро, 6-8 ГБ ОЗУ, 140 ГБ SSD, 1 NIC Ethernet 100/1000 мідний або оптичний (2 NIC для модуля Network Monitor).

3) Параметри сервера для аналітиків DLP-системи зазвичай – 2 або 4 ядерний процесор, 8-16 ГБ ОЗУ та 300-500 ГБ SSD.

Основними операційними системами для серверів є: Microsoft Windows Server 2019 Enterprise Edition, Standard Edition, Data Center Edition та Red Hat Enterprise Linux [6].

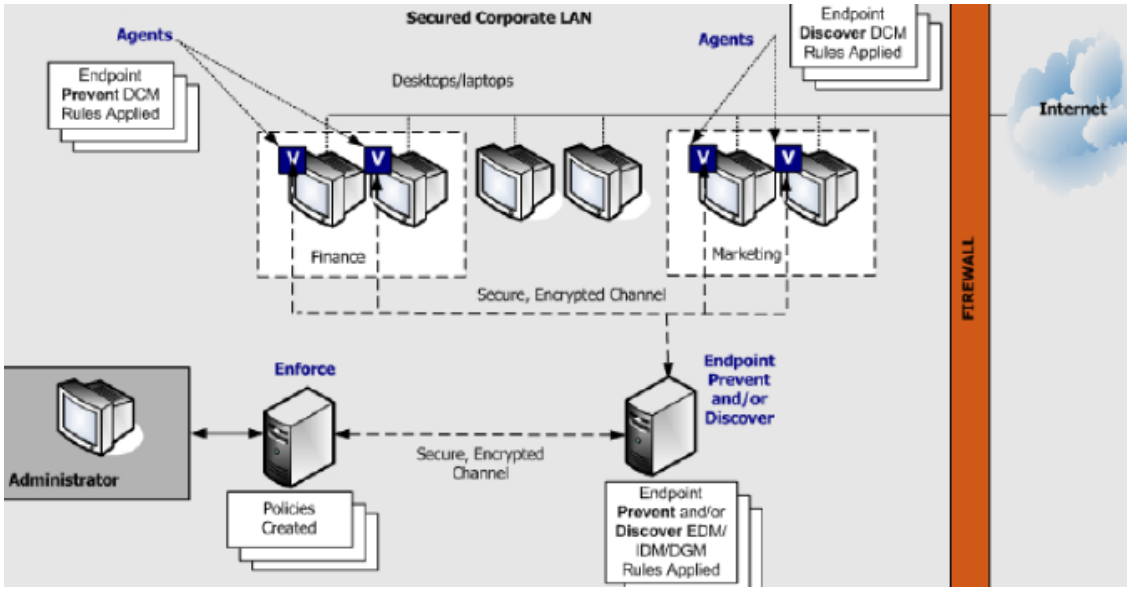

Рис. 2.3. Схема підключення модулів Symantec DLP Endpoint Discover& Prevent

Після виконання процедур з розгортання системи, його зустрічає вікно веб консолі (рис. 2.4).

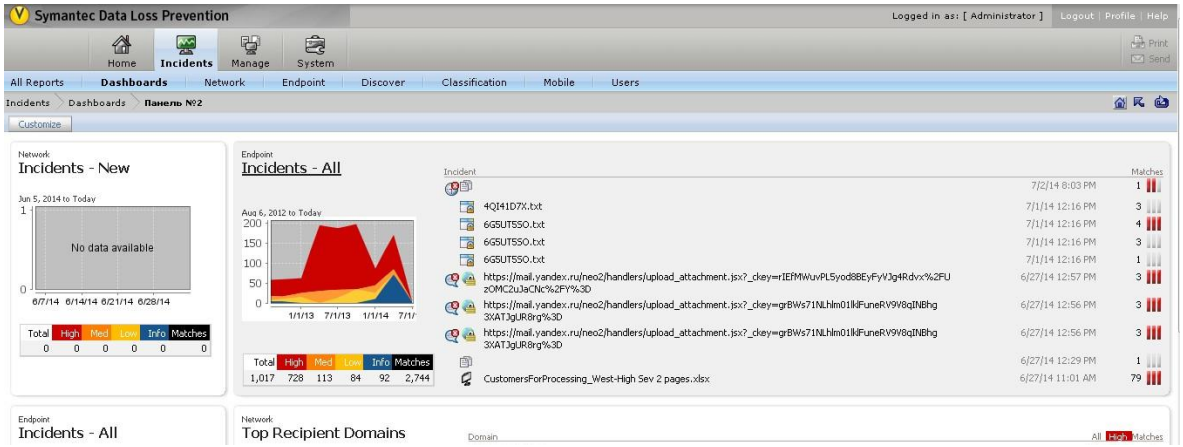

Рис. 2.4. Веб-консоль

Для прикладу, поєдання модулів було використано варіант підключення Symantec DLP Mobile Email Monitor шляхом налаштування нового серверу, налаштування проксі-серверу, налаштування режиму відповіді на проксі-сервері, додавання цифрового сертифікату, налаштування облікових записів пошти, створення політики безпеки для Mobile Email Monitor.

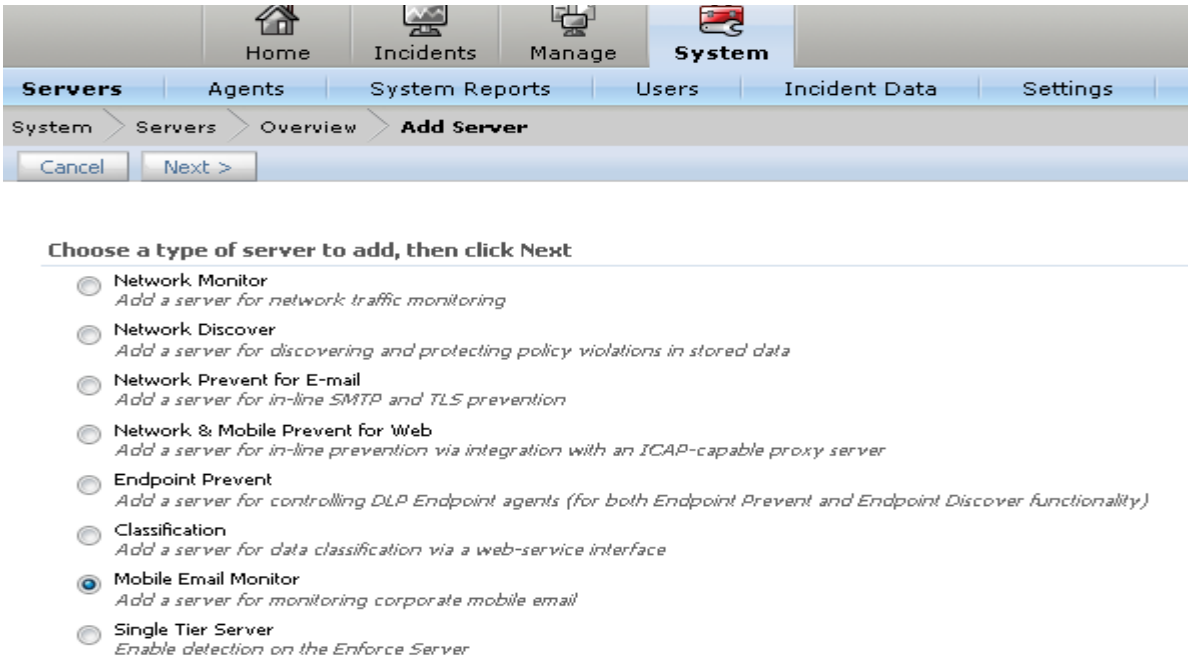

Рис. 2.5. Підключення серверу з використанням консолі керування

Після підключення серверу наступним кроком є використання розширених налаштувань задля коректного функціонування відповідно до вимог політик безпеки.

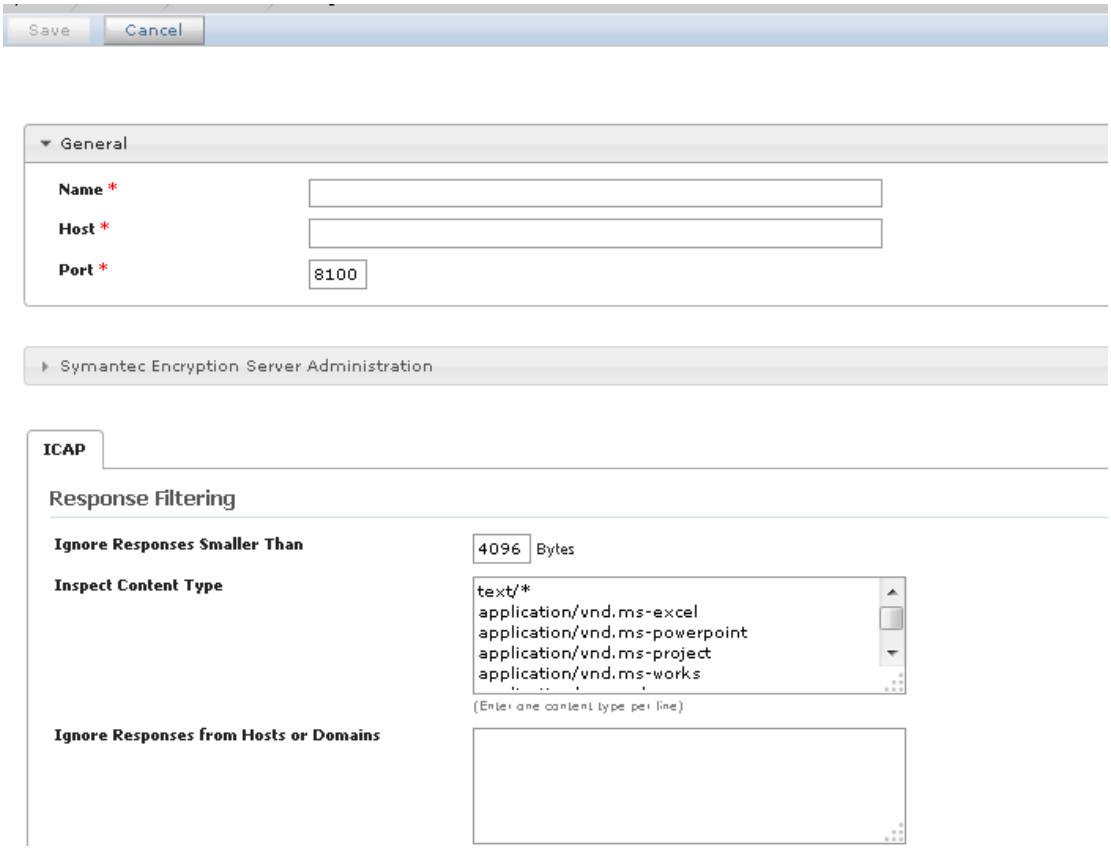

Рис.2.6. Додаткові налаштування в сервері

Для коректного функціонування всіх складових та модулів в системі створюються політики, які включають в себе набір правил детектування контенту, контексту та відповідних дій. Можуть бути користувацькими або на основі шаблонів. При створенні політик треба обов’язково звертати увагу на важливість компонентів. Нижче в таблиці 2.2 наведено компоненти та їх тлумачення.

Таблиця 2.2

Компоненти політик в Symantec DLP

Компонент	**Необхідність**	**Пояснення**
Ім'я політики	Обов'язково	Повинно бути унікальним
Група політики	Обов'язково	Повинна бути призначена
Правила політики та виключення	Обов'язково	Політика повинна включати правила, які визначають хоч одну умову збігу
Профілі даних та виключення	Може бути потрібним	Профілі даних необхідно задавати в політиці, якщо методи виявлення в політиці їх потребують
Група користувачів та виключення	Може бути потрібним	Вказання групи користувачів необхідне, якщо групові методи в політиці потребують цього
Опис політики	Опціональне	Для полегшення адміністрування
Правила реагування та виключення	Опціональне	Потрібні за умови реагування системи на інцидент при спрацюванні політики

Звітність по інцидентам формується за більшістю складових інциденту. Загалом існує 5 видів звітів в системі:

- перелік інцидентів – список інцидентів, які включають інформацію про важливість, застосовану політику, кількість збігів та статус;

- загальна статисика – відображає інформацію про всі інциденти, окрім архівних;

- звіти, доступні для поточної ролі користувача;

- звіти, які відповідають окремим серверам виявлення;

- користувацькі звіти.

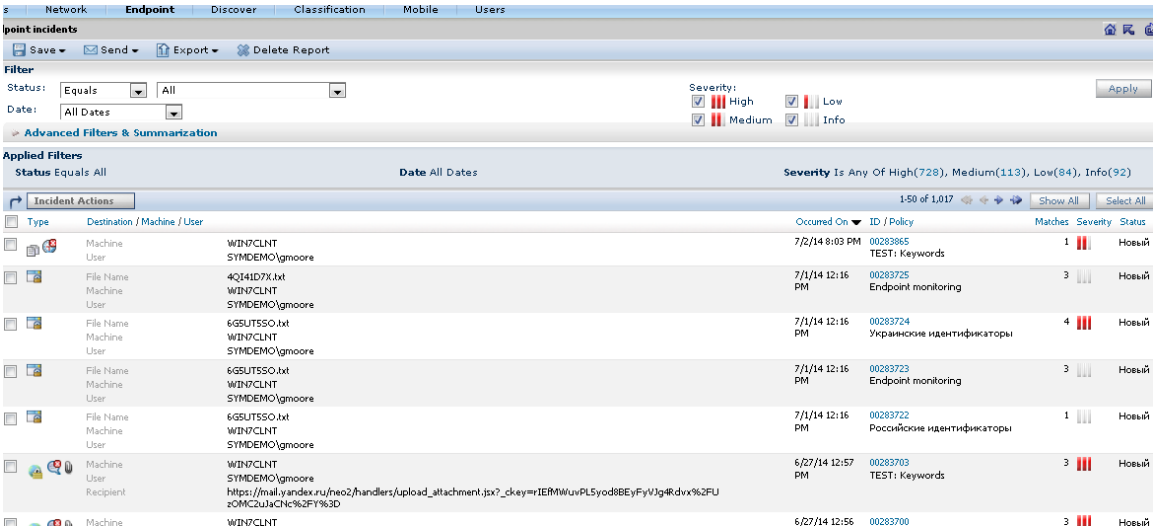

Рис. 2.7. Приклад звіту за інцидентами

Додатковою відмінністю Symantec DLP від інших є додаткові допоміжні модулі для кожної функції. Для покращення звітності використовується модуль Symantec DLP IT Analytics.[14] Його основною допоміжною функцією є проведення аналізу статистики і побудова різних звітів в графічному вигляді. Дані можливо вивести в форматах: CSV, TIF, PDF, XLSX [6].

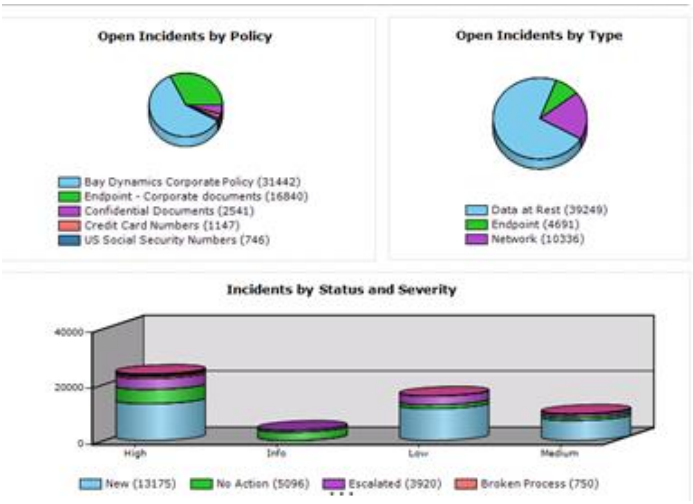

Рис. 2.8. Приклад звіту з використанням модуля IT Analytics

Symantec DLP - сучасна багатокомпонентна система запобігання витоку даних, яка не тільки контролює рух інформації, але й розгортання агентів, розширені звіти та взаємодію з власником даних. Це продукт корпоративного класу, який забезпечує повний наскрізний захист даних для підприємства або організації з урахуванням сучасних загроз інформаційній безпеці [13].

Symantec DLP є визнаним лідером на ринку захисту від витоків даних. Його комплексна система забезпечує виявлення, захист та управління конфіденційною інформацією на різних рівнях інфраструктури організацій будь-якого розміру. Рішення Symantec DLP вирізняється модульністю та готовністю до встановлення на різні апаратні платформи, що робить його універсальним і ефективним засобом захисту від кіберзагроз.

2.3 Методи підвищення ефективності використання Symantec DLP

Зазвичай кожен продукт має свої певні складові, які потребують покращення або зміни. Symantec DLP відповідає наступним методам підвищення ефективності:

Стратегічне планування та структурування. Ретельно розробка стратегії використання Symantec DLP з урахуванням бізнес-процесів і чутливості даних. Визначення типів конфіденційних даних, способи їх використання та місця зберігання, а також правила та політику DLP, які відповідають потребам підприємства або організації.

Навчання та підтримка. Проведення навчання з метою допомогти зрозуміти Symantec DLP і його можливості. Надання постійної підтримки користувачам і адміністраторам для вирішення проблем і оптимізації системи.

Постійні оновлення та моніторинг. Відстеження оновлення системи для нових випусків Symantec DLP, а також нові функції та виправлення вразливостей. Впровадження системи моніторингу для аномалій і своєчасного реагування на інциденти.

Інтеграція з іншими системами безпеки. Інтеграція Symantec DLP з іншими системами безпеки (наприклад, ідентифікацією та автентифікацією користувачів,

управлінням інцидентами та іншими рішеннями), щоб максимально підвищити ефективність і координацію.

Політика тестування та оптимізації. Політика в контексті Symantec DLP - це набір правил, процедур і параметрів, які визначають, як система має виявляти, моніторити і обробляти дані з точки зору їхньої конфіденційності і захисту. Правило - це конкретна інструкція або умова, яка вказує системі, як реагувати на певні дії або події з даними. Наприклад, правило може вказувати, що якщо співробітник намагається відправити електронний лист з великим обсягом конфіденційних даних за межі корпоративної мережі, система має перешкодити відправцю і повідомити адміністратора.

Ретроспективне навчання - це процес аналізу попередніх інцидентів і подій для виявлення закономірностей, тенденцій і слабких місць у системі. На основі цього аналізу система може вносити корективи в свою роботу, оптимізувати політику та правила, щоб уникнути подій витоку даних у майбутньому.

Широке застосування політики та правил. Політика визначає широкий спектр правил, які охоплюють різні методи, за якими може бути порушена конфіденційність інформації. Деякі з цих правил можуть бути налаштовані для різних відділів організації з урахуванням їхньої специфіки або результатів розслідування.

Впровадження технології запобігання витоку даних. Використання таких технології, як шифрування, анонімізація та архівація для додаткового захисту конфіденційних даних.

Впровадження політик DLP для запобігання неочікуваним витокам.

Аудит та звітність. Створення механізму аудиту та звітності для розслідування подій, дій та інцидентів, а також для того, щоб знати, як використання Symantec DLP.

Регулярне проводення аудиту і звітування, щоб підвищити продуктивність і перевірити аналіз слабких місць в системі безпеки.

Гнучка сегментації та диференційовані права доступу. Сегментуйтування користувачів і груп, позначаючи різні права доступу на основі ролей і обов'язків.

Визначення кастомізованої політики DLP на основі рівня чутливості даних і впровадження політики за допомогою диференційованих прав доступу.

Також додатково можна поєднати з Data Insight, який тісно інтегрований з продуктами Symantec DLP. Це двонаправлена інтеграція, Data Insight використовує DLP вмісту, а DLP використовує аналіз прав, власність, дозволи і дії над даними, можливе відновлення та оцінку ризиків [7]. Також вендор Broadcom додає певну інструкцію щодо підвищення ефективності відпрацювання системи:

1) переконайтеся, що системні вимоги до комп'ютера відповідають або перевищують системні вимоги до хост-комп'ютера.

2) перезавантажте комп'ютер, щоб переконатися, що проблема не пов'язана з одним сеансом входу.

3) переконайтеся, що агент DLP внесено до білого списку в антивірусній програмі відповідно до найкращих практик: агенти кінцевих точок, захищені від вірусів. Інші активні програми безпеки та/або інші програми, які не повинні контролюватися, такі як програми резервного копіювання та відновлення, повинні бути внесені в білий список на розсуд організації.

4) перевірте, чи є у агента дамп пам'яті/дамп збоїв. Якщо так, надішліть їх до служби підтримки Symantec.

5) переконайтеся, що опція "Локальний диск" увімкнена на вкладці "Канал", де ви вибираєте кінцеву точку і місце призначення (канал) для моніторингу. Моніторинг "локального диска" може спричинити проблеми з продуктивністю, оскільки DLP почне моніторинг усіх файлів, створених на локальному диску. Якщо вам потрібно контролювати файли на локальних дисках, рекомендується використовувати Endpoint Discover [8].

Використовуючи низку технологій і правил Symantec DLP, компанії можуть забезпечити високий рівень безпеки даних, мінімізуючи ризик витоку конфіденційної інформації. Завдяки використанню низки технологій і правил Symantec DLP компанії можуть забезпечити високий рівень безпеки даних і звести до мінімуму ризик витоку конфіденційної інформації. Це робить Symantec DLP незамінним інструментом для організацій, які хочуть захистити критично важливі

дані та відповідати новітнім стандартам безпеки.

Отже, ці методи дозволяють максимально ефективно використовувати Symantec DLP для захисту конфіденційної інформації в організації. Їх впровадження і вдосконалення може позитивно позначитися на безпеці даних та загальній продуктивності організації.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ВІД ВИТОКУ ДАНИХ НА ОСНОВІ SYMANTEC DLP

3.1 Тестування та оптимізація системи захисту від витоку даних з використанням Symantec DLP в реальному часі

Кількість викрадених даних зростає з кожним роком. 60-70% витоків даних стають надбанням громадськості, що негативно впливає на репутацію компанії, а часто і на її прибуток; 84% IT-лідерів вважають, що для віддалених працівників це ще більш складний виклик. Кожні 11 секунд компанії піддаються атакам, а кількість кібератак зростає. Середній збиток від витоку даних у США оцінюється в 9,44 мільйона доларів США, DLP вирішує три ключові проблеми IT-безпеки для організацій: захист/відповідність персональних даних, захист інтелектуальної власності та прозорість даних [9].

Захист даних: організації, які збирають і зберігають персональні, медичні та платіжні дані, швидше за все, підтримують під дію таких нормативних актів, як HIPAA та GDPR. Це означає, що вам потрібно буде вжити заходів для захисту конфіденційної інформації ваших клієнтів.

Захист інтелектуальної власності: Якщо ваша компанія володіє цінною інтелектуальною власністю, комерційною або державною таємницею, втрата або крадіжка таких даних може поставити вашу компанію під загрозу. Рішення DLP, яке вимагає контекстну класифікацію, може класифікувати інтелектуальну власність як у структурованій, так і в неструктурованій формі. Політики та заходи захисту запобігають витоку даних.

Видимість даних: комплексні корпоративні DLP-рішення забезпечують видимість і моніторинг даних на кінцевих точках, у мережах і хмарах. Ви можете побачити, як користувачі вашої організації маніпулюють даними. Рішення DLP також ефективно запобігає несанкціонованим діям користувачів, захищає дані Office 365, аналізує поведінку користувачів і компанії та захищає від комплексних загроз. Задля підвищення якості вирішення проблем інформаційної безпеки

організації або підприємства системи DLP повинні проходити постійні процедури перевірок на відпрацювання вбудованих модулів та функцій – тестування та оптимізації. Дані процедури включать в себе наступні складові:

1) Аналіз витоків даних та визначення критичних об’єктів інформаційної безпеки: задля підвищення стійкості системи захисту проводяться аудити, щоб визначити ключові загрози та виявити вразливості. Наявним прикладом є проведення аналізу обміну електронними листами та виявлення можливих точок витоку конфіденційної інформації через невірно налаштовані правила в модулі Symantec DLP Network Prevent for Mail.

2) Встановлення правил для категоризації конфіденційної інформації: дана складова включає в себе налаштування правил у модулях системи з метою коректного і вчасного відпрацювання. Наявним прикладом є налаштування модуля Symantec DLP Endpoint Discover на розпізнавання конфіденційних номерів кредитних карток у текстових документах та електронних листах. Такі дані мають відстежуватися та блокуватися в режимі реального часу відповідно до встановленим політикам безпеки організації або підприємства.

3) Налаштування політики безпеки: дана складова включає в себе написання правил задля обмежень певних дій користувачів в системах з метою попередження витоку. Наявним прикладом є налаштування політик у модулі Symantec DLP Endpoint Prevent для блокування виведення конфіденційних даних клієнтів у файли та заборони копіювання на зовнішніх пристроях. Як можливий варіант - запобігання витоку планів домовленостей з замовникамиза проекти через зовнішні флеш-накопичувачі.

4) Тестові сценарії в реальному часі: дана складова включає в себе виконання операцій в системі користувачем задля викликання алертів про порушення правил. Наявним прикладом є імітація спроби співробітника передати конфіденційні дані несанкціонованим мережевим каналом та подальше спрацювання модуля Symantec DLP Network Protect.

5) Оптимізація правил і політики: дана складова іключає в себе аналіз з метою подальшого виявлення та виправлення помилкових спрацювань і хібних

спрацювань. Наявним прикладом є написання правил для модуля Symantec DLP Network Discover щодо оптимізації для усунення помилкових спрацьовувань при роботі із зашифрованими документами в мережі організації або підприємтсва.

6) Моніторинг і аудит: будь-які зразки подій повинні бути задокументовані і в режимі реального часу відстежуватися з використанням модулів Symantec DLP для виявлення невідомих загроз. Навяним прикладом є реагування на несанкціоноване копіювання конфіденційних файлів на локальних комп'ютерах з використанням Symantec DLP Network Prevent for Web.

7) Навчання персоналу: дана складова включає в себе написання посадових та технічних інструкцій задля правильного використання та реагування на зразки сповіщення Symantec DLP. Наявним прикладом є інструкції щодо використання електронної пошти та передача даних безпеки.

8) Звітність та аналіз результатів: важливим етапом в забезпеченні інформаційної безпеки є підготовка звітів про кількість виявлених витоків інформації, ефективність запобігання та рекомендації щодо підвищення безпеки. Наявним прикладом є аналіз частоти витоків даних за певний час та розробка стратегій для усунення виявлених вразливостей та занесення даної інформації до Oracle Database for Symantec DLP.

При виконанні даних процедур Symantec DLP, разом із систематичним тестуванням та оптимізацією, можна використовувати для створення ефективних механізмів запобігання витоку даних у реальному часі, які відповідають найсучаснішим вимогам кібербезпеки.

Отже, реалізація та оптимізація системи захисту від витоку даних з використанням Symantec DLP в реальному часі є критично важливою для забезпечення безпеки даних у сучасному інформаційному середовищі. Системи DLP не лише допомагають виявляти та запобігати витокам даних, але й забезпечують захист персональних даних, інтелектуальної власності та забезпечують видимість даних в організації.

Для ефективного використання системи Symantec DLP у реальному часі необхідно проводити постійні процедури тестування та оптимізації, що включають

аналіз витоків даних, встановлення правил категоризації конфіденційної інформації та вдосконалення стратегій захисту. Тільки таким чином можна гарантувати високий рівень захисту даних і вчасну реакцію на потенційні загрози безпеці.

3.2 Інтеграція з існуючими системами безпеки та ймовірність фальсифікаційних сигналів

Поєднання Symantec Data Loss Prevention (DLP) з існуючими системами безпеки є необхідним і стратегічним кроком у впровадженні ефективної стратегії кібербезпеки в організації. Цей процес спрямований на створення інтегрованої взаємопов'язаної екосистеми безпеки, в якій Symantec DLP взаємодіє та взаємодіє з іншими системами безпеки, щоб забезпечити належну та скоординовану реакцію на наявні загрози витоку даних. Унікальна технологія Symantec дозволяє швидко автоматизувати навчання. При зміні рівня знань в компанії рішення DLP може бути швидко перенавчено/перекваліфіковано. Може бути інтегровано з функціональними системами компанії (наприклад, ERP, CRM, HR). Таким чином, завдання запобігання витоку інформації можна об'єднати з наступними регулярними процесами[10]. Вони були консолідовані:

1. Включення конфіденційної інформації у всі пристрої компанії.

2. Керування розміщенням конфіденційної інформації та безпечним зберіганням даних на всіх пристроях компанії, включаючи мобільні пристрої, які регулярно залишають мережу компанії.

3. Управління та контроль доступу використання конфіденційної інформації співробітниками компанії.

4. Управління життєвим циклом конфіденційної інформації та забезпечення її безпеки, включаючи процедури обробки та зберігання інформації.

5. Контроль передачі конфіденційної інформації всіма каналами (електронна пошта, веб, мережа, локальні порти та пристрої) відповідно до встановлених політик.

6. Блокування незаконних дій, включаючи друк на мережевих та локальних принтерах, автоматичне видалення, друк на принтері та автоматичне видалення конфіденційної інформації.

7. Надання розрахунків зі зниження ризиків у рамках завдань, які виконуються Symantec DLP відповідно до стандартів чинного законодавства.

На додаток до функціональності DLP, він забезпечує інтеграцію з іншими системами безпеки і системами управління інформаційною безпекою (СУІБ):

- Інтеграція з продуктами PGP/ERM/DRM для посилення захисту конфіденційної інформації з використанням шифрування у випадку розташування на небезпечних ресурсах [10].

- Автоматична зміна привілеїв користувачів відповідно до політики безпеки.

- Побудова процесів роздільного зберігання і обробки конфіденційної інформації.

- Зміна статусу ресурсу у випадку виявлення конфіденційної інформації на ньому.

- Інтеграція в системи IT-аналітики для розширення звітності, контролю ключових ідентифікаторів ефективності та консолідації інформації від різних систем інформаційної безпеки.

Інтеграція Symantec DLP з існуючими системами безпеки створює ключову роль у вдосконаленні загального безпечного ландшафту організації. Відповідно до останніх досліджень виділено декілька прикладних варіантів інтеграції:

А) інтеграція з системами ідентифікації та автентифікації. Метою даної інтеграції є поєднання Symantec DLP з Active Directory для автоматичного визначення та управління правами доступу. Запобігає ситуації, коли користувач отримує підвищений рівень доступу в Active Directory (наприклад, отримує адміністраторські права), Symantec DLP автоматично забезпечує ефективні правила захисту для цього користувача, забезпечуючи більш жорсткий контроль над конфіденційними даними.

Б) інтеграція з системою управління подіями та інцидентами (SIEM). Метою даної інтеграції є централізований моніторинг та аналіз подій.

Підтвердження виявлення поточного витоку даних у Symantec DLP автоматично передається в SIEM-систему. Це дозволяє аналізувати виявлені загрози в контексті інших безпекових подій, швидко реагувати на інциденти та досліджувати відповідні заходи.

В) інтеграція з системою контролю доступу (IAM). Метою даної інтеграції є покращення адміністрування прав доступу та забезпечення єдиного інтерфейсу управління. Після інтеграції Symantec DLP із системою IAM адміністратор може використовувати єдиний інтерфейс для налаштування прав доступу, включаючи ті, які стосуються заходів захисту від витоку даних. Це спрощує управління та знижує ймовірність помилок у конфігурації. Іноді при моніторингу та аналізу дій користувачів можуть виникати фальсифікаційні сигнали. Мінімізація ймовірності фальсифікаційних сигналів є аспектом досягнення ефективності та точності системи Symantec DLP. Фальсифікаційні сигнали можуть виникати внаслідок наступних причин:

Таблиця 3.1

Причини фальсифікаційних сигналів

Причини	**Значення**
Недостатній контекст	Symantec DLP може виявляти певні дії в системі як загрозливі, але без детального контексту не визначити зміст взаємодії користувача з даними
Наявність шумових даних	Засмічення даними, які не є конфіденційними, але можуть мати вигляд аномалії провокує до ложнопозитивних сигналів
Неактуальність моделей машинного навчання	Якщо модель машинного навчання не оновлюється, можлива втрата актуальності в контексті нових типів атак

Продовження таблиці 3.1

Причини фальсифікаційних сигналів

Причини	**Значення**
Некоректна конфігурація правил та Політик	Недостатнє налаштування чутливості або невірний вибір правил для конкретного типу даних може спричинити ефективне визначення загрози.
Нестандартні сценарії взаємодії	Нестандартні, але легітимні сценарії взаємодії з даними можуть викликати сигналізацію виявлення загрози, яка не є дійсно витоком даних

За даних умов аналітик інформаційної безпеки отримує додаткову інформацію про події, що не несуть загрози захищеності інформаційного простору організації або підприємства, але змушують реагувати відповідно до прописаних політик безпеки, тому для зменшення хибних сигналів потрібно:

- Регулярно оновлювати правила та політики з урахуванням останньої інформації про нові загрози.
- Налаштувати рівень чутливості до кожного типу даних та контексту.
- Використовувати контекстуальний аналіз для більш точного визначення загроз.
- Моніторинг та аудит системи, що включає в себе аналіз хибних спрацювань для вдосконалення алгоритмів та виправлення некоректних налаштувань.
- Інтеграція з системами SIEM, що включає в себе централізований моніторинг та аналіз подій для виявлення аномалій з подальшим вдосконаленням алгоритмів виявлення [11].

Отже, інтеграція Symantec Data Loss Prevention (DLP) з існуючими системами безпеки є стратегічно важливим етапом у впровадженні ефективної стратегії

кібербезпеки в організації. Цей процес дозволяє створити інтегровану екосистему безпеки, в якій Symantec DLP взаємодіє з іншими системами, забезпечуючи координацію реакції на загрози витоку даних.

Використання унікальних технологій Symantec сприяє швидкому автоматизованому навчанню системи, а також її інтеграції з іншими функціональними системами організації, такими як ERP, CRM та HR. Це дозволяє об'єднати завдання запобігання витоку інформації з регулярними процесами аудиту та оптимізації.

Завдяки інтеграції Symantec DLP з існуючими системами безпеки досягається кілька ключових цілей, включаючи включення конфіденційної інформації у всі пристрої компанії, управління доступом, контроль передачі даних та побудову різноманітних процесів безпеки.

Інтеграція Symantec DLP з існуючими системами безпеки забезпечує зростаючий рівень захисту даних та ефективний контроль над їх витоком, що є важливим для забезпечення безпеки організації в умовах зростаючих загроз кібербезпеки.

3.3 Рекомендації щодо забезпення захисту ІКС від витоку даних на основі Symantec DLP

Після завершення аналізу функціоналу та розгортання системи для запобігання втраті даних на кінцевих точках рішення Data Loss Prevention (DLP) від Symantec було визначено його високоефективним і передовим інструментом, який включає в себе передові можливості та вирішує основні питання інформаційної безпеки у питанні витоку даних на кінцевих точках. Це рішення обґрунтовується на ключових особливостях, які відрізняють його від аналогів і підкреслюють його видатну ефективність.

Таблиця 3.2

Переваги рішення серед аналогів

Особливості системи	**Значення**
Комплексний підхід	Рішення пропонує комплексний набір інструментів для виявлення, моніторингу та управління витоками даних на всіх рівнях інфраструктури
Розширена визначеність політик	Рішення дозволяє деталізовано налаштовувати політики виявлення витоків, що дозволяє адаптувати їх під конкретні потреби та особливості бізнес-процесів
Машинне навчання та аналітика	Система використовує технології машинного навчання та аналітики для створення точних та ефективних алгоритмів виявлення витоків, зменшуючи ймовірність хибних сигналів
Інтеграція зі сторонніми системами безпеки	Легко інтегрується з іншими системами безпеки, такими як системи ідентифікації та автентифікації, SIEM, що дає змогу створювати повноцінний комплекс захисту
Спрощений моніторинг та звітність	Symantec DLP надає зрозумілі засоби моніторингу та звітності, що полегшує відслідковування та аналіз інцидентів витоку даних
Гнучкість та розшарування	Гнучко адаптується до різних бізнес-сценаріїв та розмірів компаній, надаючи різні рівні захисту та розширюючись від невеликих підприємств до великих корпорацій

Також було досліджено та розраховано ризик витоку даних з використанням DLP рішення в системі інформааційної безпеки підприємтсва або організації.

Таблиця 3.3

Поширені джерела витоку інформації з кінцевих точок

Джерело витоку інформації	Без використання додаткових рішень по запобіганню витокам	З використанням рішення Symantec DLP
Веб-джерела	Високий	Низький
Електронні поштові сервіси	Високий	Низький
Копіювання на зовнішні носії інформації	Високий	Низький
Злом баз даних	Високий	Низький
Шпигуни	Високий	Середній

За результатами дослідження було визначено, що потенційні та найчастіші джерела витоку інформації знаходяться під активним моніторингом з боку DLP системи, лише від методів соціальної інженерії присутня певна ймовірність витоку. Основуючись на даному детальному аналізі системи з запобігання та витоків даних було надано наступні рекомендації для захисту ІКС від витоків даних на кінцевих точках:

1. Налаштування та підтримка точності виявлення. Встановлення політик для виявлення та класифікації конфіденційної інформації є основоположним етапом. Для забезпечення надійного функціонування необхідна поточна налаштування системи та регулярні оновлення для підтримки точності виявлення. Це допоможе зменшити кількість хибнопозитивних та хибнонегативних сигналів, що є критично важливим для зменшення навантаження на команду кібербезпеки.

2. Моніторинг і блокування потоку даних. Symantec DLP має забезпечувати постійний моніторинг і блокування несанкціонованих спроб передачі конфіденційної інформації. Важливо налаштувати систему для швидкого реагування на зловживання або спроби витоку, що дозволяє групі з кіберзахисту оперативно встановлювати причини та виконавців порушень.

3. Інтеграція з іншими системами безпеки. Symantec DLP може бути інтегрована з іншими системами безпеки, такими як SIEM (Security Information and Event Management), що підвищить рівень реагування на потенційні загрози. Інтеграція з антивірусними системами, системами контролю доступу та шлюзами електронної пошти допоможе забезпечити багаторівневий захист від різних видів загроз.

4. Інтуїтивно зрозумілий інтерфейс для адміністраторів та користувачів є важливим аспектом для забезпечення ефективного управління системою. Зручна адміністративна панель для налаштування та моніторингу дозволить адміністраторам легко керувати політиками безпеки, моніторити події та оперативно реагувати на інциденти.

5. Ефективне використання ресурсів та масштабованість для великих організацій є ще одним ключовим аспектом. Symantec DLP оптимізує продуктивність при обробці великих обсягів даних, що робить його придатним для використання в організаціях з різними масштабами діяльності. Однак, важливо врахувати, що висока вартість ліцензій та необхідність вкладення в апаратне забезпечення можуть стати значним фінансовим навантаженням для деяких підприємств.

6. Автоматизоване реагування та зменшення хибних спрацьовувань. Використання методів контентного та контекстного аналізу для виявлення конфіденційних даних дозволяє зменшити кількість хибнопозитивних сигналів. Автоматизоване реагування на інциденти дозволить швидше реагувати на загрози та знижувати ризики.

Впровадження Symantec Data Loss Prevention (DLP) забезпечує комплексний підхід до захисту кінцевих точок від витоку даних. Ключові рекомендації включають налаштування точності виявлення, моніторинг і блокування потоку даних, інтеграцію з іншими системами безпеки, ефективне використання ресурсів та інтуїтивно зрозумілий інтерфейс для адміністраторів. Автоматизоване реагування та зменшення хибних спрацьовувань також сприяють підвищенню ефективності системи. Виконання цих рекомендацій допоможе мінімізувати

ризики витоку даних та забезпечити високий рівень захисту інформації в організації.

ВИСНОВКИ

В даній кваліфікаційній роботі було проведено дослідження проблеми витоку даних на кінцевих точках підприємства або організації, визначено його мету та завдання. Зі стрімким розвитком технологій все більше і більше з'являється нових загроз інформаційній безпеці. Все більша кількість світових аналітиків безпеки зазначає на зростанні ризиків для безпеки та захисту кінцевих точок підприємств або організацій, які посилюються недостатнім рівнем знань та інструментів до їх протидії новим загрозам за допомогою існуючих рішень для захисту від витоку даних на кінцевих точок.

Проведено аналіз та порівняння існуючих сучасних рішень для захисту від витоку даних кінцевих точок підприємства або організації. Рішення DLP забезпечує функції активного моніторингу і збору даних із кінцевих точок для виявлення потенційних порушень інформаційної безпеки в системи та швидкого реагування на кіберінциденти. Тому, DLP відіграє визначальну роль у загальній системі забезпечення безпеки інформаційної системи організації.

- Виявлення та захист від витоків;
- Моніторинг та контроль користувачів;
- Шифрування та захист даних під час транспортування;
- Адаптивна правила та аналітика.

Отже, в контексті сучасних загроз інформаційної безпеки та загрози витоку даних, Symantec Data Loss Prevention (DLP) виступає як інструмент для захисту кінцевих точок підприємства або організації.

Рішення дозволяє класифікувати та маркувати дані, забезпечуючи їх чітку ідентифікацію та контроль. Крім того, використання адаптивних правил, аналітики та інтеграції з іншими системами безпеки робить його комплексним рішенням для ефективного виявлення, реагування та запобігання витокам даних. Symantec DLP лише надає технологічні можливості для захисту від сучасних загроз, але й активно сприяє збільшенню рівня свідомості персоналу та навчанню їх впровадженню найкращих практичних заходів безпеки. Його гнучкість та здатність адаптуватися

до змін у бізнес-процесах із використанням ключових елементів Symantec DLP у сфері захисту від витоків даних.

Як підсумок, реалізація Symantec Data Loss Prevention (DLP) є стратегічним рішенням для організацій, які прагнуть максимально ефективно захистити свої кінцеві точки від ризиків потоку даних. Впровадження цієї системи в синергії з іншими заходами забезпечення безпеки створює надійний оборонний щит, здатний ефективно протидіяти сучасним та майбутнім загрозам інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Витік даних чи злам – у чому різниця. URL: https://10guards.com/ua/articles/whats-the-difference-between-a-data-leak-and-a-data-breach/ (дата звернення: 26.03.2023).

2. Впровадження DLP (ДЛП) системи і Криптозахисту інформації. URL: https://netwave.ua/direction/kryptozahyst-ta-zapobigannya-vytoku-danyh/#:~:text=DLP%20(Data%20Loss%20Prevention)%20%E2%80%93,%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8E%D1%8E%D1%87%D0%B8%20%D1%82%D0%B0%20%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D1%83%D1%8E%D1%87%D0%B8%20%D0%BF%D0%BE%D1%82%D1%96%D0%BA%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85.(дата звернення: 26.11.2023).

3. Витік даних. Визначення та приклади у 2024. URL: https://gridinsoft.ua/data-breaches (Accessed December 3, 2023).

4. Захист від витоку інформації - Integrity Systems URL: http://integritysys.com.ua/security/dlp/(дата звернення: 26.11.2023).

5. Шифрування та захист баз даних - iIT Distribution URL: https://iitd.com.ua/shifruvannja-ta-zahist-baz-danih/#:~:text=%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%20%D0%B1%D0%B0%D0%B7%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85%20%E2%80%94%20%D1%86%D0%B5,%2C%20%D0%BF%D0%BE%D1%80%D1%83%D1%88%D0%B5%D0%BD%D0%BD%D1%8F%2C%20%D0%B7%D0%BD%D0%B8%D1%89%D0%B5%D0%BD%D0%BD%D1%8F%2C%20%D0%BA%D0%BE%D0%BF%D1%96%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F.(дата звернення: 26.11.2023).

6. Огляд Symantec Data Loss Prevention 12.5 URL: https://ukrbezpeka.com/symantec_dlp-11/(дата звернення: 28.11.2023).

7. ERC Content. Захищайте та відновлюйте URL: https://erc.ua/upload/uploaded_files/114/64da1f16309cc_erc_n_4_-83-

_2022_web.pdf(дата звернення: 26.11.2023).

8. Improve the DLP Endpoint Agent Performance. URL: https://knowledge.broadcom.com/external/article/176182/improve-the-dlp-endpoint-agent-performan.html(дата звернення: 26.11.2023).

9. Що таке запобігання втраті даних (Data Loss Prevention або DLP)?. URL: https://www.kingston.com/ua/blog/data-security/data-loss-prevention-dlp(дата звернення: 26.11.2023)

10. Запобігання витокам інформації. URL:https://quadrosoft.by/images/pdf/baza_znanij/Symantec%20DLP%2012.0.pdf

11. Атака на відмову в мережі інтернет. URL:https://core.ac.uk/download/pdf/38468786.pdf

12. Що таке Інтернет речей (IoT) і які його наслідки? URL:https://www.iotworlds.com/uk/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D1%96%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%80%D0%B5%D1%87%D0%B5%D0%B9-iot-%D1%96-%D1%8F%D0%BA%D1%96-%D0%B9%D0%BE%D0%B3%D0%BE-%D0%BD%D0%B0%D1%81%D0%BB/

13. Шифрування даних та автентифікація користувачів за допомогою рішень Symantec. URL: https://www.softkey.ua/ua/useful/webinars/shifrovanie-dannykh-i-autentifikatsiya-polzovateley-posredstvom-resheniy-symantec/

14. Symantec IT Analytics Solution for DLP. URL:https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/symantec-it-analytics-solution-for-dlp/2-9-1.html

15. Витік даних: Cambridge Analytica припиняє своє значення. URL:https://rubryka.com/2018/05/02/vytik-danyh-cambridge-analytica-prypynyaye-svoye-isnuvannya/

16. Впровадження DLP систем. URL:https://techexpert.ua/it-services/implementation-of-dlp-systems/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)