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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія протидії витокам даних в організації на основі DLP»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

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

Виконав: здобувач вищої освіти групи БСДМ-61
БАГАЦЬКИЙ Сергій
(ПРІЗВИЩЕ, Ім'я)

Керівник: МАРЧЕНКО Віталій
д.ф., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DLP — Data Loss/Leak Prevention

SQL — Structured Query Language

XSS — Cross Site Scripting

MITM — Man in the middle

IDS/IPS — Intrusion Detection and Prevention System

SWG — Secure Web Gateway

SEG — Secure Email Gateway

CASB — Cloud Access Security Broker

ECM — Enterprise content management

PCI — Payment Card Industry

HIPAA — Health Insurance Portability and Accountability Act

GDPR — General Data Protection Regulation

IIS — Internet Information Services

ПК — Персональний комп’ютер

ВСТУП

Актуальність дослідження. У наш час, коли сучасні технології використовуються широкою масою організацій для зберігання та обробки величезних обсягів інформації, питання кібербезпеки та захисту даних стає надзвичайно актуальним. Загрози для конфіденційності та цілісності даних постійно зростають, охоплюючи атаки хакерів, внутрішні порушення безпеки, а також технічні та людські помилки. Виток конфіденційної інформації може призвести до серйозних наслідків, таких як втрата довіри клієнтів, фінансові втрати та юридичні проблеми.

Захист від витоку даних стає особливо важливим у контексті впровадження регуляторних вимог та законодавчих стандартів щодо конфіденційності інформації. Організації повинні дотримуватися строгих норм щодо захисту особистих даних своїх клієнтів і споживачів, що робить актуальність теми важливою для забезпечення відповідності та уникнення правових проблем.

Крім того, з розвитком технологій та збільшенням кількості з'єднаних пристроїв у бізнес-середовищі, поглиблюється потреба в комплексному та інтегрованому підході до захисту даних. Системи захисту повинні ефективно виявляти потенційні загрози, а також оперативно реагувати та запобігати витокам. Такий підхід стає стратегічною необхідністю для збереження репутації організації, її стійкості на ринку та довіри споживачів.

Вищенаведені аргументи актуалізують тему даної кваліфікаційної роботи, зміст якої становлять дослідження щодо технології захисту організації від витоку даних на основі технології DLP.

Об’єкт дослідження – процес забезпечення захисту інформації від витоку даних організації на основі DLP.

Предмет дослідження – технологія протидії витокам даних в організації.

Мета роботи – аналіз та розробка варіанту технології протидії витокам даних з використанням технології DLP в організаціях.

Наукові завдання:

- провести аналіз щодо необхідності безпеки організації від витоку даних;
- проаналізувати основні загрози та сценарії витоку даних в організації;
- проаналізувати методи та засоби захисту організації від витоку даних;
- розробити варіант розгортання технології протидії витокам даних в організації на основі DLP Safetica ONE та рекомендації щодо застосування даної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, законів України.

Практичне значення одержаних результатів полягає в розробці технології розгортання.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки» [1].

1 АНАЛІЗ ПРОБЛЕМИ ЗЕБЕЗПЕЧЕННЯ БЕЗПЕКИ ОРГАНІЗАЦІЇ ВІД ВИТОКУ ДАНИХ

1.1. Визначення та аналіз сценаріїв витоку даних

Витік даних — це випадки, коли кіберзлочинець пропускає та розкриває конфіденційні дані електронним або фізичним способом. Витік даних часто відбувається з внутрішніх пристроїв організації, таких як ноутбуки співробітників, зовнішні жорсткі диски, USB-накопичувачі, або в електронному вигляді через Інтернет або електронну пошту співробітників. У разі витоку даних кіберзлочинці виявляють витік даних і використовують знайдену інформацію в своїх цілях [2].

Порушення даних – це кібератака, при якій приватна та конфіденційна інформація розкривається неавторизованій особі. Важливі документи передаються, переглядаються та копіюються без дозволу власника. Зазвичай зловмисники використовують слабкі технології та необережну поведінку користувачів для проникнення в систему з метою крадіжки або перехоплення даних.

Методи атак для витоку даних

— Атака міжсайтового скриптингу (XSS)

Міжсайтовий скриптинг, або XSS - це атака, при якій кіберзлочинці впроваджують шкідливі скрипти на надійний сайт, який в іншому безпечний. Коли жертви відвідують пошкоджений сайт, вони стають вразливими до цієї атаки.

Це поширена техніка, що спостерігається під час витоку даних у охороні здоров'я. XSS використовується для крадіжки cookies, перехоплення сеансів користувачів, використання облікових записів, перехоплення та крадіжки конфіденційної інформації або доступу до геолокації, мікрофону, веб-камери, Bluetooth тощо. Вашого пристрою.

— Атака SQL Injection

SQL означає Structured Query Language (структурована мова запитів) - атака, коли зловмисники впроваджують шкідливі коди в існуючі елементи SQL для маніпулювання системами з метою надання доступу. Таким чином намагаються перехопити дані або знайти облікові дані адміністратора та повністю заволодіти системою.

— MITM-атака

MITM, або атака "людина посередині", - це атака з підслуховуванням, коли суб'єкти загрози порушують зв'язок та передачу даних між серверами відправника та одержувача.

Типові сценарії витоку даних та наслідки

Кібератака: Атака хакера на системи організації за допомогою шкідливого програмного забезпечення (малварь).

Наслідки: Несанкціонований доступ до конфіденційної інформації, можливість використання цих даних для викрадення грошей, витрати на відновлення безпеки.

Втрата фізичного носія даних: Втрата ноутбука, смартфона або USB-накопичувача, що містить конфіденційну інформацію.

Наслідки: Потенційний доступ до інформації особами, які знайшли втрачений носій даних.

Недбалість працівника: Працівник ненавмисно надає несанкціонований доступ до конфіденційної інформації (наприклад, надсилає невірному отримувачу поштову відправку, перехід на фішингове посилання).

Наслідки: Розголошення конфіденційної інформації, порушення довіри клієнтів або партнерів.

Фізичний доступ несанкціонованої особи: Несанкціонована особа отримує фізичний доступ до приміщення організації та отримує доступ до комп'ютерних систем.

Наслідки: Несанкціонований доступ до інформації та можливість використання її в своїх цілях.

Пошкодження або втрата даних через технічний збій: Несподіваний технічний збій призводить до втрати чи пошкодження конфіденційних даних.

Наслідки: Втрата доступу до важливої інформації, можливість порушити ділову діяльність.

Внутрішні порушення безпеки: Працівник або колишній працівник використовує свої привілеї для незаконного доступу до конфіденційної інформації.

Наслідки: Несанкціонований доступ та можливе розголошення конфіденційних даних.

1.2. Визначення категорій та типів конфіденційних даних

Конфіденційна інформація – (від англ. confidence — довіра) це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням.

Відповідно до статті 21 Закону України "Про інформацію", конфіденційна інформація разом із службовою та таємною інформацією належить до інформації з обмеженим доступом [3].

Інформація з обмеженим доступом – це така інформація, доступ до якої має лише обмежене коло осіб і оприлюднення якої заборонено розпорядником інформації відповідно до закону. Обмеження доступу до інформації здійснюється в інтересах національної безпеки або охорони законних прав фізичних та юридичних осіб. Важливо! Обмежується доступ до інформації, а не до документу. Відповідно, якщо в одному документі міститься відкрита і закрита інформація, то відкрита інформація може бути надана на ознайомлення зацікавленій особі у вигляді окремого документу.

За змістом статті 6 Закону України «Про доступ до публічної інформації» вбачається, що інформація з обмеженим доступом, може бути наступною [4]:

- конфіденційна інформація - інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може

поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.;

- таємна інформація – інформація, доступ до якої обмежується і розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу передбачену законом таємницю;

- службова інформація - що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню або прийняттю рішень; зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці [4].

До конфіденційної інформації, що є власністю держави і перебуває в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, не можуть бути віднесені відомості:

- про стан довкілля, якість харчових продуктів і предметів побуту;

- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

- стосовно стану справ із правами і свободами людини і громадянина, а також фактів їх порушень;

- про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

- щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов'язковому оприлюдненню відповідно до закону;

- інша інформація, доступ до якої відповідно до законів України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України [4].

Конфіденційні дані - це інформація, яка має важливий характер і призначена для обмеженого кола осіб. Ця інформація може включати особисті дані, фінансову інформацію, комерційну та конфіденційну інформацію компаній, медичну інформацію тощо.

Категорії та типи конфіденційних даних:

1. Особисті дані: ім'я та прізвище; адреса; номер телефону; адреса електронної пошти; соціальний номер (в США, наприклад, Social Security Number).

2. Фінансова інформація: карткові дані (номер картки, термін дії, CVV-код); банківські реквізити (реквізити рахунку, код банку); платіжні історії, фінансові звіти.

3. Медична інформація: історія захворювань; результати аналізів; інформація про прийом лікарських засобів; діагнози та лікування.

4. Комерційна та конфіденційна інформація компаній: бізнес-плани; фінансові документи; конфіденційні угоди та контракти.

5. Конфіденційна технічна інформація: патенти та реєстраційні дані; технічні специфікації; програмний код.

6. Державна інформація: військові стратегії; розвідувальні дані; класифіковані документи.

1.3. Оцінка наслідків витоку конфіденційної інформації для організації

Закон України «Про інформацію» дає наступне тлумачення поняття «інформації» - це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [3]. Ділова інформація в бізнесі в основному служить основою для прийняття рішень, але вона також використовується для ведення та підтримки бізнеспроцесів, полегшення спілкування між співробітниками і т. д.

На відміну від інших матеріальних активів, інформація в якості активу може мати різноманітні форми, бути дизайном продукту, технічними даними, інструкціями з управління, оперативними даними, знаннями співробітників, комп'ютерним програмним забезпеченням, робочими інструкціями, бізнес результатами і звітами, базою даних, системною документацією, керівництвом користувача, планами, засобами розробки та підтримки і т. д.

У бізнесі інформація є стратегічним ресурсом, який є ключовим для ведення бізнесу. Інформація є однією з найважливіших бізнес-цінностей, основним джерелом доходів і рушійною силою для створення нової цінності, для прийняття рішень, підвищення продуктивності, досягнення успіху на ринку і підтримки робочих процесів, засобом для комунікації. У кожному випадку інформація визначається як інструмент змін і інструмент формалізації та управління бізнес середовищем.

Оцінка наслідків витоку конфіденційної інформації для організації є важливою частиною управління ризиками та захисту даних. Вона допомагає розуміти потенційні втрати, які можуть виникнути в результаті такого витоку, і вжити відповідні заходи для їх запобігання чи пом'якшення.

Основні кроки у процесі оцінки наслідків витоку конфіденційної інформації включають [5]:

Визначення та ідентифікація витоку: Спочатку необхідно виявити, яка саме інформація була розкрита та які категорії даних були пошкоджені.

Оцінка важливості даних: Визначення, наскільки важливі ці дані для організації. Наприклад, особисті дані клієнтів чи фінансова інформація можуть мати вищий рівень важливості.

Оцінка потенційних втрат: Визначення можливих негативних наслідків для організації, таких як фінансові втрати, втрата довіри клієнтів, юридичні проблеми тощо.

Оцінка репутаційних втрат: Врахування можливих впливів на репутацію організації в результаті витоку конфіденційної інформації.

Оцінка впливу на ділову діяльність: Визначення, як витік конфіденційної інформації може вплинути на нормальний хід роботи організації та її бізнес-процеси.

Визначення заходів та стратегій: Розроблення плану дій для мінімізації потенційних втрат та запобігання подібним ситуаціям у майбутньому.

Оцінка відповідальності: Визначення, хто несе відповідальність за витік і які юридичні чи етичні наслідки можуть виникнути [6].

Комунікація та повідомлення сторонам зацікавленим: Якщо це вимагається законом, необхідно повідомити осіб, чий персональний чи конфіденційний матеріал був пошкоджений.

Моніторинг та вдосконалення: Важливо встановити механізми моніторингу та аналізу ефективності вжитих заходів та, в разі потреби, вносити корективи.

Важливо пам'ятати, що кожна ситуація може бути унікальною, тому конкретні кроки та заходи можуть відрізнятися в залежності від контексту та обставин.

Висновки до розділу 1

Отже, в розділі було проаналізовано проблеми забезпечення безпеки організації від витоку даних. Визначено методи атак та проаналізовано типові сценарії витоку даних та їх наслідки. Розглянуто ключові моменти нормативних документів, що відповідають за регулювання, визначення та відповідальність порушень, щодо конфіденційних даних. Проведено оцінку наслідків витоку даних організації.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВІД ВИТОКУ ДАНИХ

2.1. Аналіз існуючих методів та засобів безпеки від витоку даних

У зв'язку з постійним розвитком інформаційних технологій та зростаючою кількістю загроз для конфіденційності та цілісності даних, аналіз існуючих методів та засобів безпеки від витоку даних набуває особливої вагомості. Забезпечення безпеки даних стає завданням важливим не лише для запобігання потенційним витокам, але й для забезпечення довіри споживачів, дотримання вимог законодавства та забезпечення сталості бізнес-процесів.

Аналіз ключових методів та засобів захисту від витоку даних [7]

Шифрування даних: Шифрування конвертує звичайний текст в незрозумілий для сторонніх код за допомогою спеціального ключа.

Переваги: Зашифровані дані важко розгадати без відповідного ключа.

Недоліки: Потребує правильної реалізації та керування ключами.

Мережеві брандмауери: Фільтрують мережевий трафік, дозволяючи або блокуючи його відповідно до заданих правил.

Переваги: Захищають мережу від несанкціонованого доступу та атак із мережі Інтернет [7].

Недоліки: Важливо правильно налаштувати брандмауер та постійно оновлювати його правила.

Антивірусні програми та антишпигунські програми: Виявляють та блокують шкідливе програмне забезпечення, віруси та шпіонське ПЗ.

Переваги: Захищають від загроз, що можуть витекти чи навантажити систему.

Недоліки: Вимагають постійного оновлення для надання ефективного захисту.

Моніторинг та аналіз активності: Ведення журналів та аналіз подій для виявлення незвичайних або підозрілих активностей [7].

Переваги: Дозволяє вчасно виявляти можливі загрози та атаки.

Недоліки: Важливо правильно налаштувати та аналізувати журнали.

Двофакторна аутентифікація: Використання двох різних методів для підтвердження особи (наприклад, пароля та коду, отриманого на мобільний телефон).

Переваги: Додатковий рівень безпеки, навіть якщо пароль витік або був скомпрометований.

Недоліки: Може бути не так зручно для користувачів.

Системи виявлення та запобігання вторгненням (IDS/IPS): Моніторять мережевий трафік для виявлення невідомих чи підозрілих активностей та намагаються їх блокувати [7].

Переваги: Виявлення та блокування атак в реальному часі.

Недоліки: Вимагають правильної конфігурації та підтримки.

Регулярні навчання та нагадування працівникам: Навчання працівників щодо кращих практик щодо безпеки та свідомого відношення до конфіденційних даних.

Переваги: Підвищення обізнаності та запобігання людським помилкам.

Недоліки: Вимагає постійного нагадування та підтримки [7].

2.2. Визначення та основні принципи роботи DLP-систем

Запобігання втраті даних (DLP), згідно Gartner, можна визначити як технології, які виконують як перевірку вмісту, так і контекстний аналіз даних, надісланих через програми обміну повідомленнями, такі як електронна пошта та обмін миттєвими повідомленнями, у русі по мережі, у використанні на керованому кінцевому пристрої, і в стані спокою на локальних файлових серверах або в хмарних програмах і хмарних сховищах. Ці рішення виконують реагування на основі політики та правил, визначених для запобігання ризику ненавмисних або випадкових витоків або розголошення конфіденційних даних за межами авторизованих каналів [1,8].

Технології DLP загалом поділяються на дві категорії – Enterprise DLP та Integrated DLP. У той час як корпоративні рішення DLP є всеосяжними та упаковані в агентське програмне забезпечення для настільних комп'ютерів і серверів, фізичних і віртуальних пристроїв для моніторингу мереж і трафіку електронної пошти або програмних пристроїв для виявлення даних, Integrated DLP обмежено безпечними веб-шлюзами (SWG), безпечними шлюзами електронної пошти (SEG), продукти шифрування електронної пошти, платформи керування корпоративним контентом (ECM), інструменти класифікації даних, інструменти виявлення даних і брокери безпеки доступу до хмари (CASB) [1,8].

Розуміння відмінностей між усвідомленням вмісту та контекстним аналізом є важливим для повного розуміння будь-якого рішення DLP . Корисний спосіб подумати про різницю: якщо вміст – це лист, а контекст – це конверт. У той час як усвідомлення вмісту передбачає захоплення конверта та заглядання в нього для аналізу вмісту, контекст включає зовнішні фактори, такі як заголовок, розмір, формат тощо, усе, що не включає вміст листа. Ідея усвідомлення вмісту полягає в тому, що хоча ми хочемо використовувати контекст, щоб отримати більше інформації про вміст, ми не хочемо бути обмеженими одним контекстом [1,8].

Після відкриття конверта та обробки вмісту існує кілька методів аналізу вмісту, які можна використати для ініціювання порушення політики, зокрема:

На основі правил/регулярні вирази: найпоширеніша техніка аналізу, яка використовується в DLP, полягає в тому, що механізм аналізує вміст за певними правилами, такими як 16-значні номери кредитних карток, 9-значні номери соціального страхування в США тощо. Ця техніка є чудовою для першого проходу. фільтр, оскільки правила можна швидко налаштувати та обробити, хоча вони можуть бути схильні до високого рівня помилкових спрацьовувань без перевірки контрольної суми для визначення дійсних шаблонів.

Відбитки бази даних: також відомий як точна відповідність даних, цей механізм шукає точні збіги з дампа бази даних або живої бази даних. Хоча дампи бази

даних або активні підключення до бази даних впливають на продуктивність, це варіант для структурованих даних із баз даних.

Точна відповідність файлу: вміст файлу не аналізується; однак хеші файлів відповідають точним відбиткам. Забезпечує низьку кількість помилкових спрацьовувань, хоча цей підхід не працює для файлів із кількома схожими, але не ідентичними версіями [8].

Часткова відповідність документів: шукає повну або часткову відповідність у певних файлах, наприклад у кількох версіях форми, заповнених різними користувачами.

Концептуальний/лексикон: використовуючи комбінацію словників, правил тощо, ці політики можуть попереджати про абсолютно неструктуровані ідеї, які не піддаються простій категоризації. Його потрібно налаштувати для наданого рішення DLP.

Статистичний аналіз: використовує машинне навчання або інші статистичні методи, як-от байєсівський аналіз, щоб ініціювати порушення правил у безпечному вмісті. Для сканування потрібен великий об’єм даних, чим більше, тим краще, інакше можуть виникати помилкові спрацьовування та негативні результати.

Попередньо створені категорії: Попередньо створені категорії з правилами та словниками для поширених типів конфіденційних даних, таких як номери кредитних карток/захист PCI, HIPAA тощо [8].

Сьогодні на ринку існує безліч методів, які забезпечують різні види перевірки вмісту. Варто взяти до уваги одне: хоча багато постачальників DLP розробили власні механізми вмісту, деякі використовують технологію сторонніх розробників, яка не призначена для DLP. Наприклад, замість створення відповідності за шаблоном для номерів кредитних карток, постачальник DLP може отримати ліцензію на технологію від постачальника пошукової системи для зіставлення за шаблоном номерів кредитних карток. Оцінюючи рішення DLP, зверніть пильну увагу на типи шаблонів,

виявлених кожним рішенням у порівнянні з реальним масивом конфіденційних даних, щоб підтвердити точність механізму вмісту [8].

2.3. Архітектура та компоненти DLP-системи

П’ять типів запобігання втраті даних

1. Ідентифікація даних: це процес, за допомогою якого організації ідентифікують конфіденційну інформацію у своєму цифровому середовищі, незалежно від того, чи знаходиться вона в електронних листах, хмарних програмах для зберігання даних, програмах для співпраці чи в інших місцях.

2. Ідентифікація витоку даних: це автоматизований процес для виявлення та ідентифікації незаконно привласнених даних, незалежно від того, чи були вони викрадені чи неправильно розміщені в інфраструктурі організації.

3. Data-in-Motion DLP: коли дані передаються між місцями, мережева безпека DLP використовує низку заходів безпеки, щоб гарантувати, що дані надходять до місця призначення недоторканими [9].

4. Data-at-Rest DLP: цей тип захисту охоплює дані, які зараз не передаються і зазвичай зберігаються в базі даних або системі обміну файлами. Він використовує кілька методів для забезпечення безпечного зберігання даних локально та в хмарі, від захисту кінцевої точки до шифрування для запобігання будь-якому несанкціонованому використанню даних.

5. Data-in-Use DLP: Дані, якими зараз користуються особи в організації, мають бути захищені від будь-якого типу потенційно шкідливої взаємодії з даними, як-от зміна, захоплення екрана, вирізання/копіювання/вставлення, друк, або переміщення інформації. У цьому контексті DLP призначений для запобігання будь-якій несанкціонованій взаємодії або переміщенню даних, а також для виявлення будь-яких підозрілих шаблонів[9].

Існує три види DLP:

Мережевий DLP: відстежує та захищає всі дані, які використовуються, перебувають у спокої чи знаходяться в мережі компанії, включаючи хмару

Endpoint DLP: відстежує всі кінцеві точки , включаючи сервери, комп'ютери, ноутбуки, мобільні телефони та будь-які інші пристрої, на яких використовуються, переміщуються або зберігаються дані

Cloud DLP: підмножина Network DLP, яка спеціально розроблена для захисту тих організацій, які використовують хмарні сховища для зберігання даних.

Мережевий DLP

Відстежує та аналізує мережеву активність і трафік організації в традиційній мережі та хмарі; це включає моніторинг електронної пошти, обміну повідомленнями та передачі файлів, щоб виявити, коли критично важливі для бізнесу дані надсилаються з порушенням політики інформаційної безпеки організації

Створює базу даних, яка записує, коли доступ до чутливих або конфіденційних даних, хто має до них доступ і, якщо це можливо, куди дані переміщуються в мережі

Забезпечує команді інформаційної безпеки повну видимість усіх даних у мережі, включно з даними, які використовуються, знаходяться в русі чи в спокої.

Кінцева точка DLP

Відстежує всі кінцеві точки мережі, включаючи сервери, хмарні сховища, комп'ютери, ноутбуки, мобільні телефони та будь-які інші пристрої, на яких дані використовуються, переміщуються або зберігаються, щоб запобігти витоку, втраті або неправильному використанню даних [9].

Допомагає в класифікації нормативних, конфіденційних, приватних або важливих для бізнесу даних, щоб упорядкувати звітність і відповідність вимогам

Відстежує дані, що зберігаються на кінцевих точках як у мережі, так і поза нею

Хмарний DLP

Сканує та перевіряє дані в хмарі, щоб автоматично виявляти та шифрувати конфіденційну інформацію перед тим, як вона буде прийнята та збережена в хмарі

Зберігає список авторизованих хмарних програм і користувачів, які мають доступ до конфіденційних даних.

Попереджає команду інформаційної безпеки про порушення правил або аномальну діяльність [9].

Веде журнал доступу до конфіденційних хмарних даних та ідентифікації користувача

Встановлює наскрізну видимість для всіх даних у хмарі

Рішення DLP використовує комбінацію стандартних заходів кібербезпеки, таких як брандмауери, інструменти захисту кінцевих точок, служби моніторингу та антивірусне програмне забезпечення, а також передові рішення, такі як штучний інтелект, машинне навчання і автоматизація, щоб запобігти витоку даних.

Технології DLP зазвичай підтримують одну або кілька таких дій у сфері кібербезпеки:

Запобігання: слідкує за потоком даних у реальному часі та негайно обмежує підозрілу активність або неавторизованих користувачів.

Виявлення: швидко виявляє аномальну активність завдяки покращеній видимості даних і розширеним заходам моніторингу даних.

Реагування: оптимізовує дії з реагування на інциденти, відстежуючи та повідомляючи про доступ до даних і переміщення в межах підприємства.

Аналіз: контекстуалізовує підозрілу діяльність для команди безпеки, щоб посилити заходи запобігання[10].

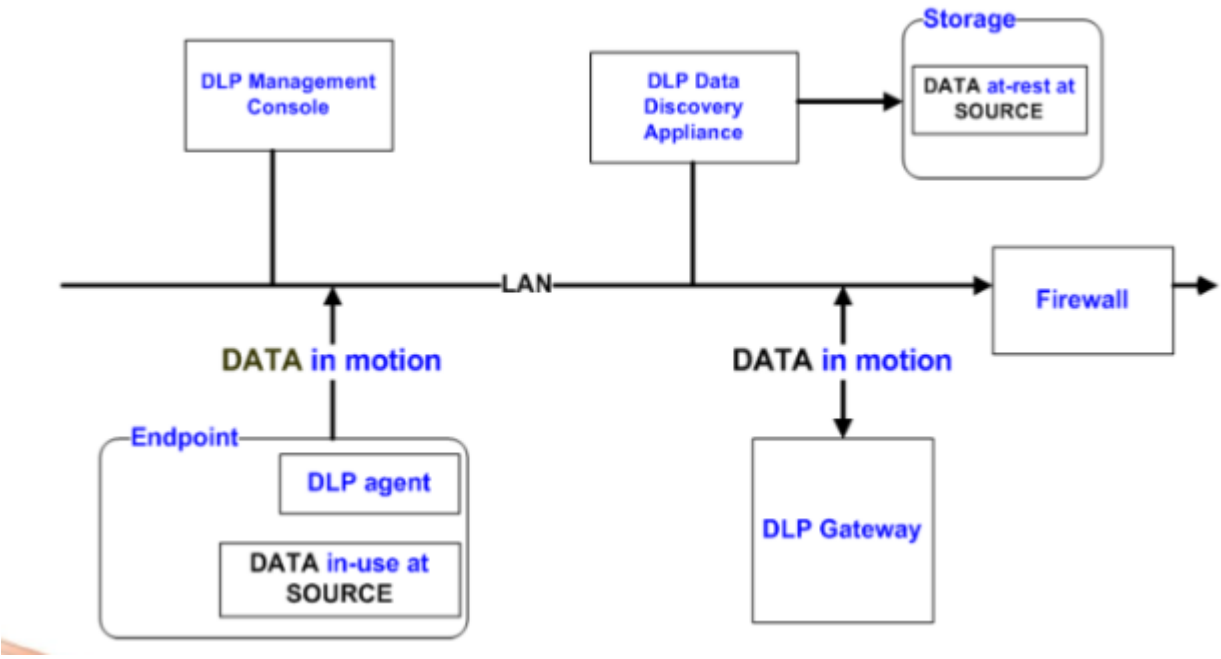

Рис. 2.1. Типова архітектура DLP системи [11]

Safetica ONE — це універсальне рішення для запобігання втратам даних та захисту від інсайдерських загроз, яке допомагає виявляти ризики безпеки, управляти потоком даних та захищати конфіденційні дані. Крім цього, Safetica ONE дозволяє легко дотримуватися будь-яких нормативних актів щодо захисту даних. Також, можна отримувати інформацію про інциденти безпеки за допомогою миттєвих сповіщень та детальних звітів. Safetica ONE проста у розгортанні та доступна для підприємств будь-якого розміру[12].

Safetica ONE – це рішення корпоративного рівня для захисту в даних від внутрішніх загроз. Воно охоплює всі сфери внутрішнього ризику та втрати даних. Також, захищає цінні дані від людського фактору та зловмисних намірів. DLP виявляє проблеми та активно запобігає витоку. Визначити свій захищений робочий простір і зменшити периметр можна за допомогою контролю додатків і веб-сайтів. Це допоможе запобігти небажаній поведінці у компанії та зменшить витрати на управління безпекою.

Безпека ніколи не повинна ставитися на шкоду продуктивності. Дане рішення не

створює зайвих клопотів для співробітників або IT-відділу, і його час-окупність є неперевершеною.

Автоматизація політик безпеки та інтеграція з IT-стеком допоможе захистити свої активи навіть у складних середовищах.

Це рішення «все в одному», яке легко інтегрується у існуючу систему безпеки, може захистити корпоративне середовище. Ось чому продукт захищає дані на всіх кінцевих точках, усіх пристроях, усіх основних операційних системах (Windows, macOS), а також у хмарі, периметрах і внутрішніх зонах.

Власна інтеграція з мережевими пристроями Microsoft 365 і Fortinet забезпечує розширений контроль над невідомими пристроями та створює надійне рішення для захисту від кінцевої точки до мережі.

Усі перевірені інциденти та журнали можна автоматично надсилати до рішень SIEM, наприклад Splunk, IBM QRadar, LogRhythm або ArcSight, для подальшого дослідження. REST API надає зібрані дані таким інструментам, як Power BI або Tableau, для розширеного аналізу (рис.2.2).

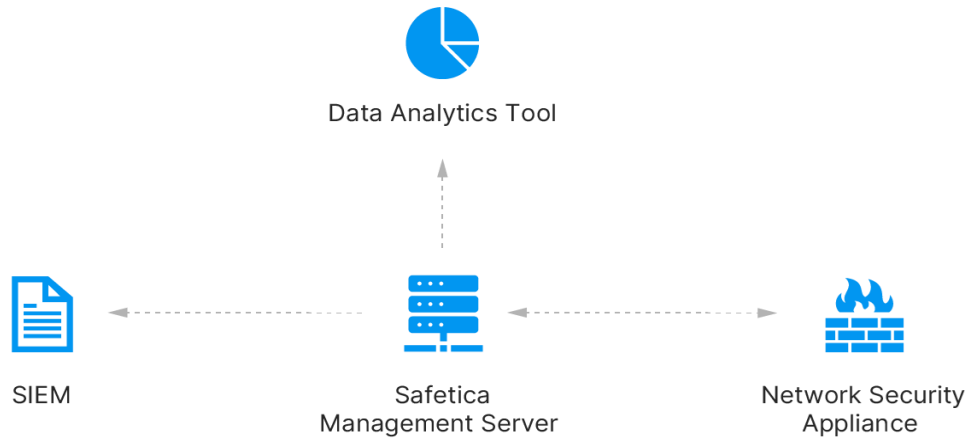

Рис.2.2. Схема надсилання звітів Safetica

Safetica захищає всі конфіденційні дані від витоку незалежно від того, де вони зберігаються:

- персональні дані;
- стратегічні документи;
- база даних клієнтів;
- дані щодо оплати, наприклад, номери кредитних карток;
- інтелектуальна власність;
- промислові зразки, комерційні таємниці та ноу-хау;
- контракти тощо.

Safetica дозволяє легко дотримуватися будь-яких нормативних актів щодо захисту даних у вашій галузі: GDPR, HIPAA, SOX, PCI-DSS, GLBA, ISO/IEC 27001, CCPA. Завдяки Safetica можливо навчити співробітників, як потрібно працювати з конфіденційними даними без змін у робочому процесі

Safetica розроблена таким чином, щоб її можна було швидко та легко розгорнути без потреби у висококваліфікованому персоналі чи додатковому апаратному забезпеченні. Важливі конфіденційні дані будуть захищені протягом кількох годин, необхідно лише визначити безпечні канали та обрати базові політики безпеки.

Safetica розпізнає потенційні ризики для конфіденційної інформації. Залежно від того, в якому режимі працює Safetica, рішення може заблокувати підозрілу діяльність, повідомити адміністратора або нагадати працівникам правила безпеки.

Аудит та виявлення з Safetica Discovery

Визначає способи використання корпоративних даних, незалежно від того, де вони перебувають та як переміщуються. Завдяки журналам аудиту дозволяє запобігти навмисному витоку інформації. Забезпечує огляд усіх внутрішніх процесів та допомагає організувати корпоративне середовище. Крім цього, Safetica Discovery дозволяє краще зрозуміти приховані ризики всередині вашої організації.

Навчання та захист із Safetica Protection

Safetica Protection створює безпечне середовище у компанії, навчає співробітників, визначає ризики та захищає корпоративні дані. Можливість

встановити політики для всіх каналів передачі даних. Можливість обрати потрібну дію для робочого процесу – від аудиту чи сповіщення до відхилення. Надає співробітникам впевненість під час роботи з конфіденційними даними - Safetica відображає сповіщення, коли користувач потенційно може порушити політику. Також можна застосувати точно визначений спосіб обробки цінних даних. Надає повний захист в режимі офлайн. У режимі офлайн забезпечується такий самий рівень захисту, як і в режимі онлайн. Усі зібрані записи синхронізуються одразу після відновлення з'єднання. Контролює всі підключені пристрої. Обмежує використання портативних пристроїв або несанкціоноване підключення медіаносіїв. Контролює корпоративні мобільні пристрої та відстежуйте дані, переміщені з хмарного середовища Office 365 (рис.2.3).

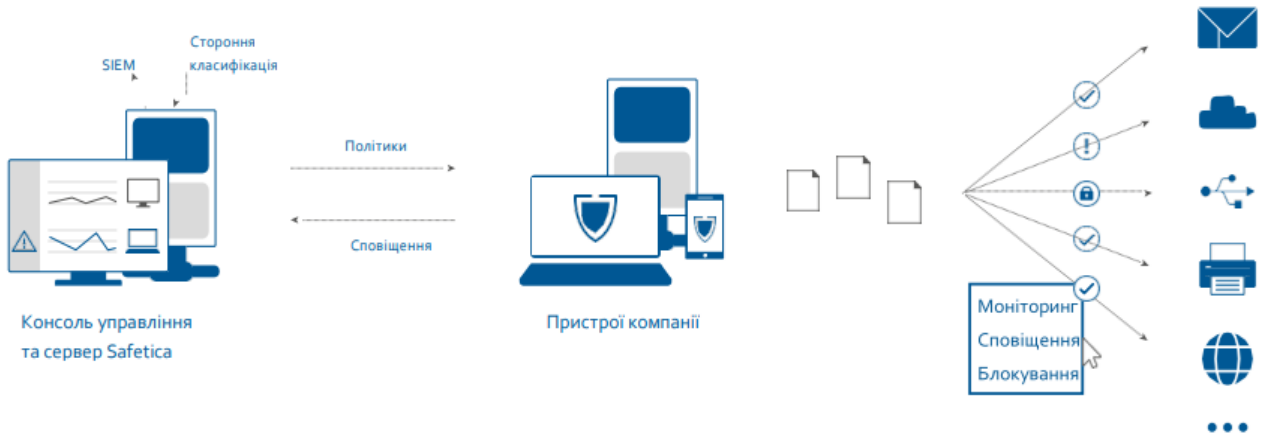

Рис.2.3. Схема роботи Safetica

Сервер Safetica запускає базу даних із робочими станціями та журналами безпеки. Консоль управління дозволяє користувачам управляти політиками безпеки та переглядати всю зібрану інформацію. Усі дії реєструються, а політики безпеки застосовуються на ПК, ноутбуках, планшетах та смартфонах із клієнтом Safetica.

Safetica захищає усі конфіденційні дані, перш ніж вони опиняться за межами компанії, незалежно від того, де вони зберігаються та як переміщуються (рис.2.4).

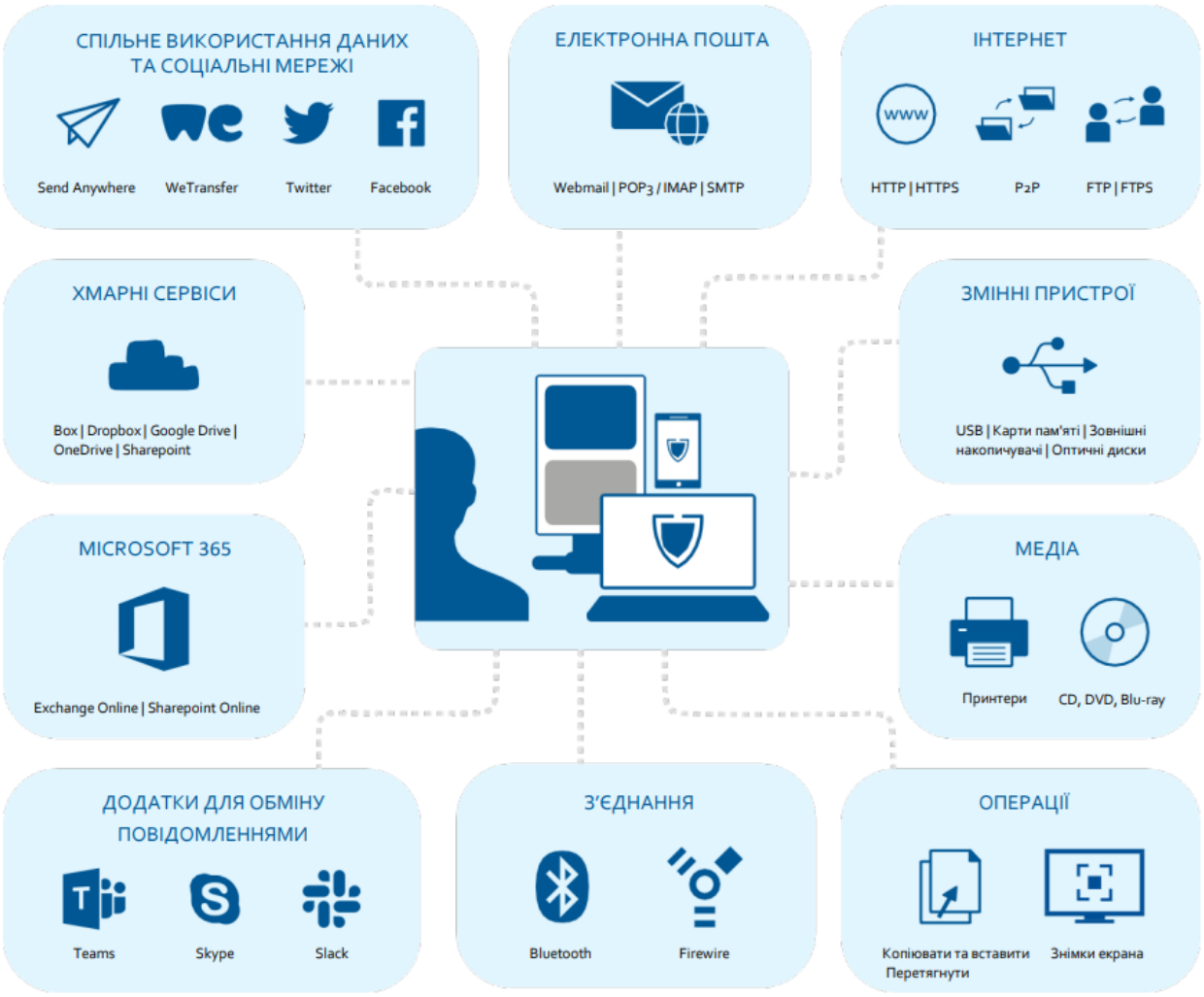

Рис.2.4. Канали переміщення інформації, з якими працює Safetica

Safetica забезпечує швидкий та легкий для розуміння огляд усіх можливих загроз з єдиної консолі. Ви маєте можливість отримувати повну інформацію у будь-який час та з будь-якого пристрою, навіть з вашого смартфона. Ви можете отримувати сповіщення про підозрілу поведінку за допомогою електронної пошти або SIEM, додавати будь-які дані на інформаційну панель та експортувати в формати XLS або PDF для подальшого аналізу[13].

Safetica є DLP-рішенням, яке зможе задовольнити потреби різних організацій. При правильному впровадженні даної системи, можливо домогтися повного захисту

від витоку даних. Також, система може допомогти у проведенні аудиту для визначення конфіденційної інформації в організації. А грамотно налаштовані політики допоможуть зберегти інформацію всередині корпоративної мережі і не дати зловмисникам скористатися нею.

На рис. 2.5 проілюстровано архітектуру DLP Safetica ONE де:

1. Комп'ютери та ноутбуки з Safetica Endpoint client: здійснюється запис дій і впровадження політики через додаток клієнта.

2. Safetica management services і бази даних SQL: дані автоматично передаються із мережевих комп'ютерів до сервера разом із синхронізованими даними ноутбука при підключенні до мережі. Налаштування клієнта синхронізується в зворотному порядку.

3. Safetica management console з налаштуваннями та результатами: всі дані доступні для перегляду в додатку керування, де також можуть бути змінені будь-які параметри.

4. Сервери Safetica management services в інших відгалудженнях: Safetica підтримує декілька відгалуджень із допомогою єдиної консолі керування.

Рис. 2.5. Архітектура рішення Safetica ONE

Управління усіма функціями та компонентами Safetica (клієнтами, серверами, базами даних) здійснюється за допомогою веб- або настільної консолі. У ній також відображаються дані моніторингу, статистична інформація та графіки. Після його запуску консолі потрібно увійти до облікового запису користувача. Елементи, які можна переглянути або встановити в окремих функціях Safetica, залежать від прав

користувача в Safetica.

Після запуску консолі Safetica ви побачите наступний інтерфейс (рис.2.6):

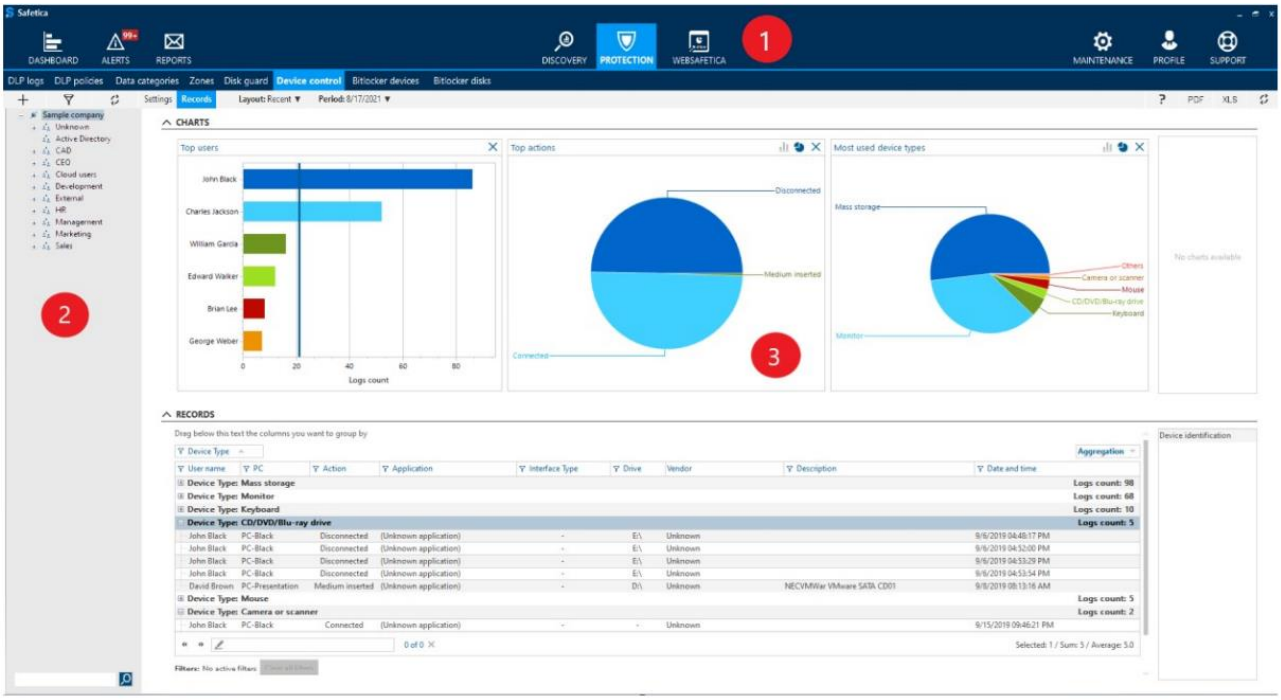

Рис. 2.6. Інтерфейс консолі управління

1. Головне меню

В головному меню можна змінювати функції та компоненти Safetica. На сірому банері у верхній частині екрана є перемикач, який використовується в деяких функціях Захисту (Protection) та Обслуговування (Maintenance) для перемикання між режимами Налаштувань (Settings) і Записів (Records). У розділі Discovery використовується лише режим Записів:

• Режим налаштувань – можна встановлювати налаштування для груп, користувачів або комп'ютерів виділених у дереві користувачів. Зміни в налаштуваннях застосовуються лише після збереження за допомогою кнопки у верхньому правому кутку. Зміни також можна скасувати.

• Режим записів – у цьому режимі можна переглядати записані дані, підсумкові звіти, діаграми та статистичні дані для функцій Safetica. Дані про групи, користувачів і комп'ютери, виділені в дереві користувачів, відображаються протягом певного

періоду часу.

Ліворуч є значки, за допомогою яких можна перейти до різних оглядів із підсумковою інформацією:

• Панель інструментів (Dashboard) — огляд даних, зібраних з усіх активних функцій.

• Сповіщення (Alerts) — автоматичне налаштування сповіщень.

• Звіти (Reports) — налаштування відправки регулярних зведених звітів.

У центрі розташовані значки, які використовуються для перемикання між основними модулями Safetica:

• Discovery;

• Protection;

• WebSafetica.

Праворуч є значки, які використовуються для доступу до управління компонентами Safetica та довідки.

• Обслуговування (Maintenance) — управління та налаштування компонентів Safetica.

• Профіль (Profile) — основні налаштування облікового запису, зокрема підключення до сервера, а також налаштування консолі управління.

• Підтримка (Support) — доступ до бази знань Safetica.

Під верхньою панеллю інструментів з елементами управління консолі є список функцій. Список змінюється залежно від модулів, які використовуються — Discovery, Protection або Обслуговування.

2. Дерево користувачів

Дерево користувачів знаходиться на лівій стороні консолі під верхньою панеллю інструментів. Всі сервіси Safetica, з якими ви з'єднані, відображаються в дереві. Нове підключення до сервера можна налаштувати в розділі Профіль (Profile). Кожен сервер в дереві містить користувачів та комп'ютери, які до нього підключені. Вибрані елементи у дереві, параметри або дані, отримані за допомогою відповідних функцій,

відображаються в області відображення або перегляду (розділ 3 на малюнку).

3. Область відображення (перегляду)

Область відображення або область перегляду використовується для візуалізації даних та налаштування окремих функцій. Зміст області перегляду змінюється залежно від функції, яку переглядають та поточного режиму (налаштування або записів). Щоб переключитися між окремими функціями, потрібно натиснути на один з модулів у головному меню, а потім обрати необхідну функцію[14].

Висновки до розділу 2

В розділі проаналізовано та приведені методи та засоби захисту від витоку даних. Було визначено основні принципи роботи DLP-систем та загальна архітектура. Описано архітектуру, основні компоненти та функціональні можливості DLP Safetica ONE, що дозволяє легко інтегруватися з різноманітними системами безпеки для кращого захисту даних від витоку чи несанкціонованого доступу до них.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ПРОТИДІЇ ВИТОКАМ ДАНИХ В ОРГАНІЗАЦІЇ НА ОСНОВІ DLP

3.1. Налаштування та встановлення DLP та її компонентів

Safetica встановлюється за допомогою універсального інсталятора, який включає всі необхідні компоненти. Після його запуску можна вибрати один із двох способів інсталяції:

• Автоматичну інсталяцію – автоматичне встановлення всіх компонентів на комп'ютер.

• Інсталяція вручну (Експертна установка та витяг компонентів) – інсталяція окремих компонентів Safetica вручну.

Інсталяція вручну:

1. Перед інсталяцією потрібно перевірити, чи відповідає мережа умовам розгортання.

2. Встановити сервер на вибраних комп'ютерах. Під час інсталяції обрати, яка база даних буде використовуватися сервером для зберігання даних.

3. Встановити консоль управління або WebSafetica на ПК, з якого буде налаштоване управління Safetica.

4. Використовуючи консоль, підключити до сервера і виконати початкове налаштування Safetica.

5. Інсталювати агент на робочі станції.

6. Використавши консоль, щоб встановити клієнт на робочих станціях (встановлення клієнта через консоль можлива тільки на комп'ютерах з інстальованим агентом).

Після розгортання всіх компонентів та перевірки правильності встановлення, можна почати роботу з Safetica[14].

Автоматична інсталяція

Детально розглянемо лише Автоматичну інсталяцію, яка встановлює серверний компонент, адміністративні консолі, включаючи WebSafetica, IIS вебсервер і сервер баз даних Microsoft SQL Server Express на поточному комп'ютері. Клієнти встановлюються під час першого запуску Safetica після інсталяції. Необхідно переконатися, що комп'ютер має достатню обчислювальну потужність для роботи з базою даних, сервером, а також WebSafetica (Детальні умови стосовно вимог див. Install Manual на офіційному сайті Safetica One [12-14]).

Після запуску універсального інсталятора Safetica необхідно виконати наступні дії:

1. Обрати мову інсталятора (рис.3.1).

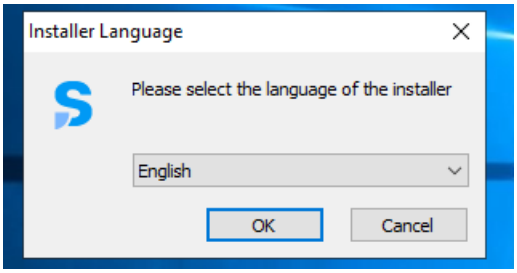

Рис. 3.1. Вікно вибору мови інсталятора

2. Натиснути кнопку «Автоматична інсталяція» (рис.3.2).

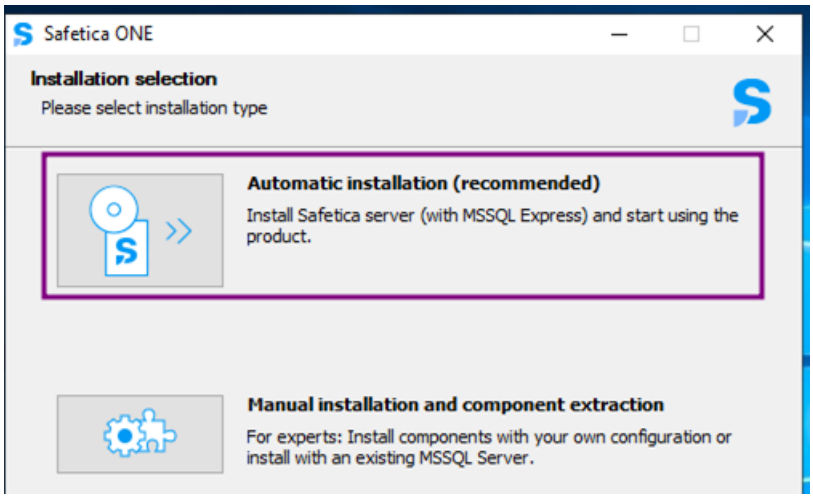

Рис. 3.2. Вікно вибору Автоматичної інсталяції

3. Натиснути «Далі», щоб підтвердити, що обране середовище відповідає

вимогам до апаратного забезпечення (рис.3.3).

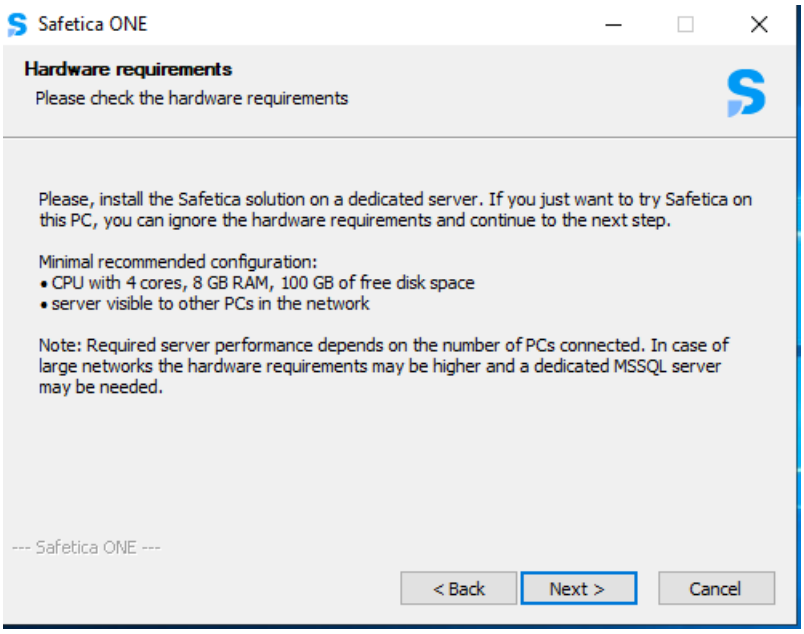

Рис. 3.3. Вимоги апаратного забезпечення

4. Ввести надійний пароль для облікового запису адміністратора. За замовчуванням пароль safetica. Підтвердіть умови ліцензійної угоди на сервері SQL і запустити інсталяцію, натиснувши кнопку «Інсталювати» (Install) (рис.3.4 – 3.8).

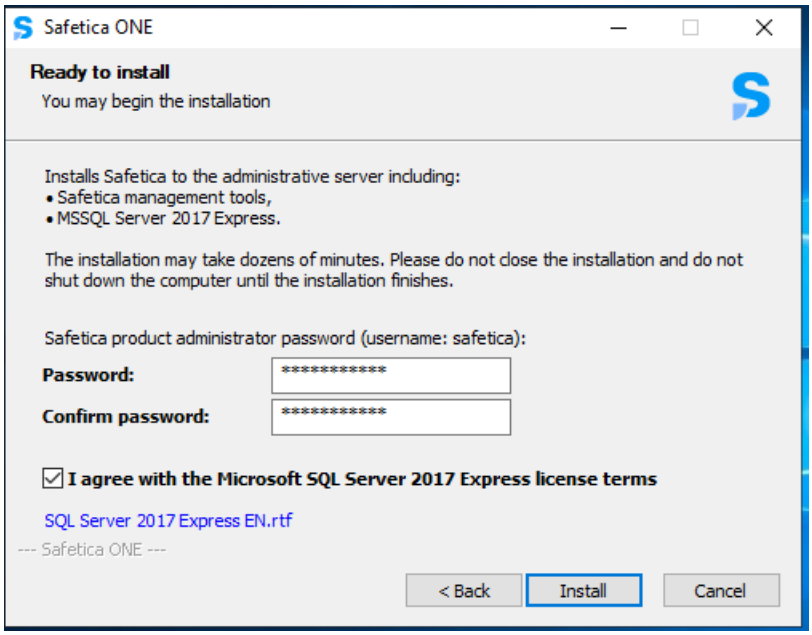

Рис. 3.4. Вікно створення паролю адміністратора

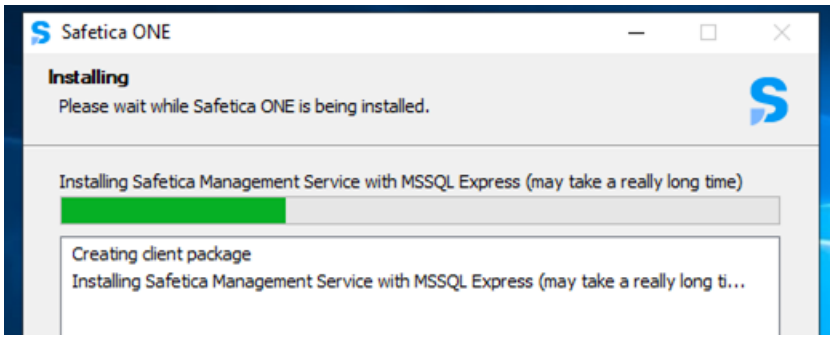

Рис. 3.5. Вікно встановлення Safetica Management Service

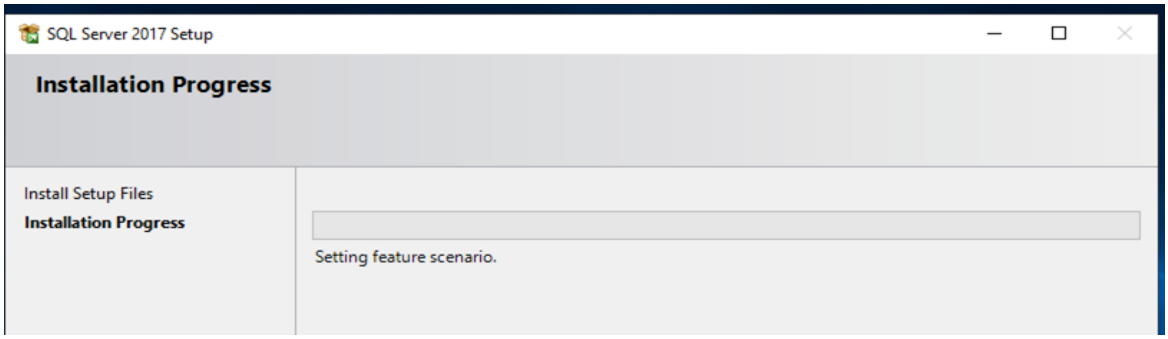

Рис. 3.6. Вікно встановлення SQL Server

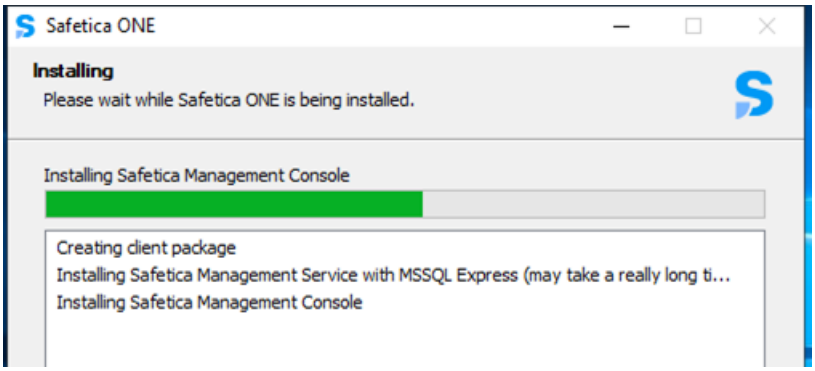

Рис. 3.7. Вікно встановлення Safetica Management Console

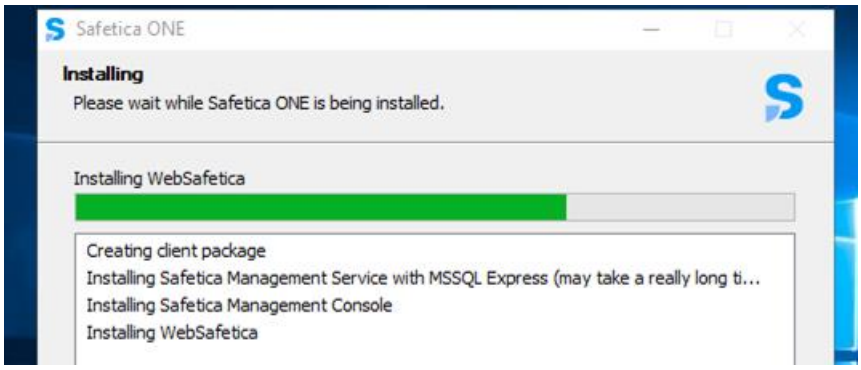

Рис. 3.8. Вікно встановлення WebSafetica

5. Щоб підтвердити успішну інсталяцію серверної частини натиснути «ОК» (рис.3.9).

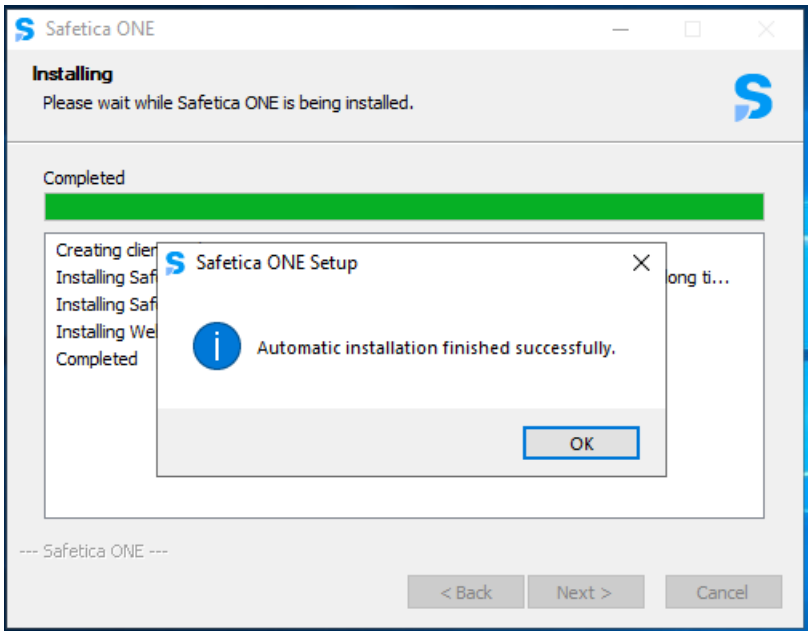

Рис. 3.9. Вікно підтвердження інсталяції

6. Після успішної інсталяції консолі управління Safetica та сервера, вся система повинна бути налаштована належним чином, перед тим як розпочати встановлення агента та клієнта Safetica на комп'ютерах. Управління та налаштування здійснюється за допомогою консолі управління Safetica (рис.3.10).

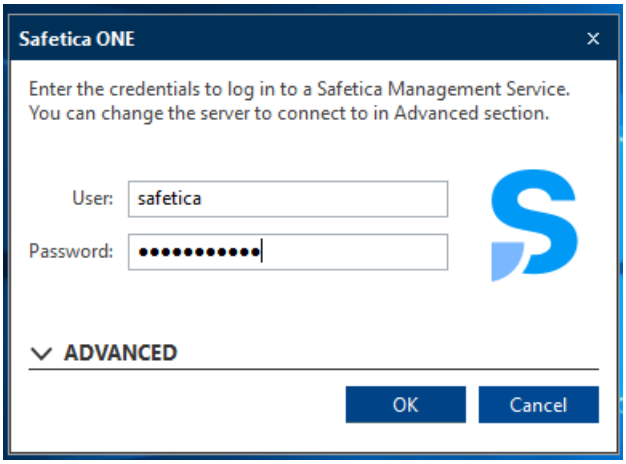

Рис. 3.10. Вікно входу в консоль управління

7. Після запуску консолі управління Safetica відкриється майстер початкового

налаштування. Під час другого етапу можна додати сервер SMTP-сервер, на який Safetica буде надсилати сповіщення та звіти. Можна пропустити дане налаштування і вказати дані пізніше (рис.3.11).

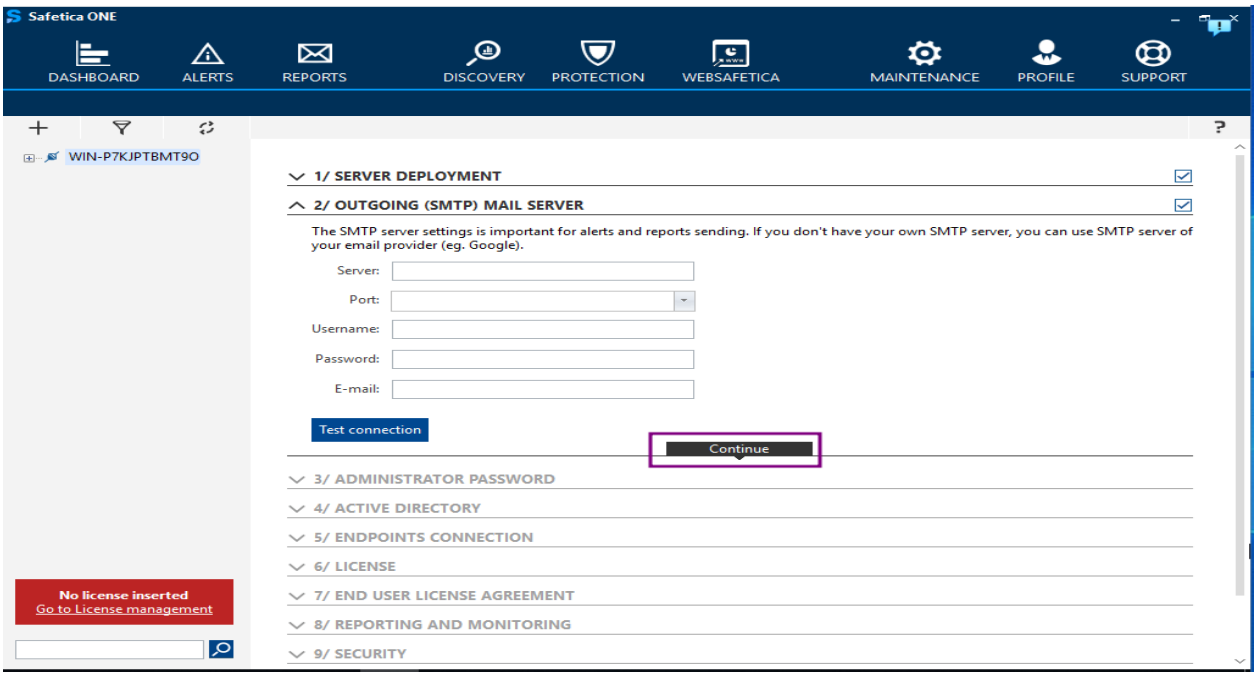

Рис. 3.11. Вікно налаштування підключення до поштового серверу

8. Під час наступного етапу можна імпортувати структуру Active Directory в компанії. Це можливо, якщо комп'ютер з сервером Safetica в домені (рис.3.12).

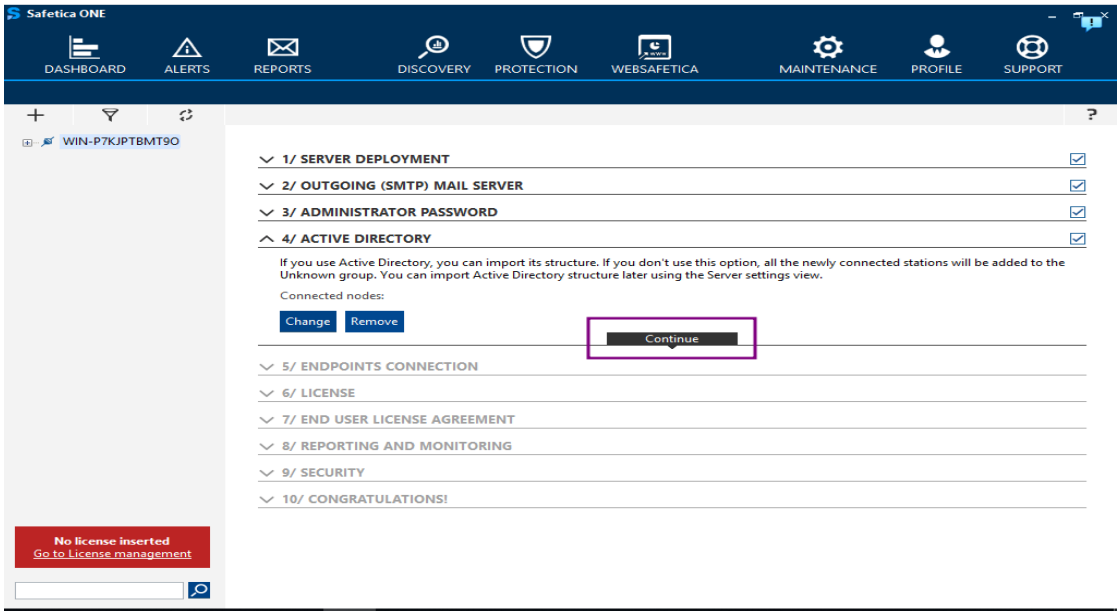

Рис. 3.12. Вікно налаштування підключення до Active Directory

9. Наступний крок — це завантаження агенту Safetica, щоб підключити робочі станції. Після натискання на кнопку «Get Downloader Agent» генерується файл інсталяції з агентом, який можна встановити на робочих станціях (рис.3.13).

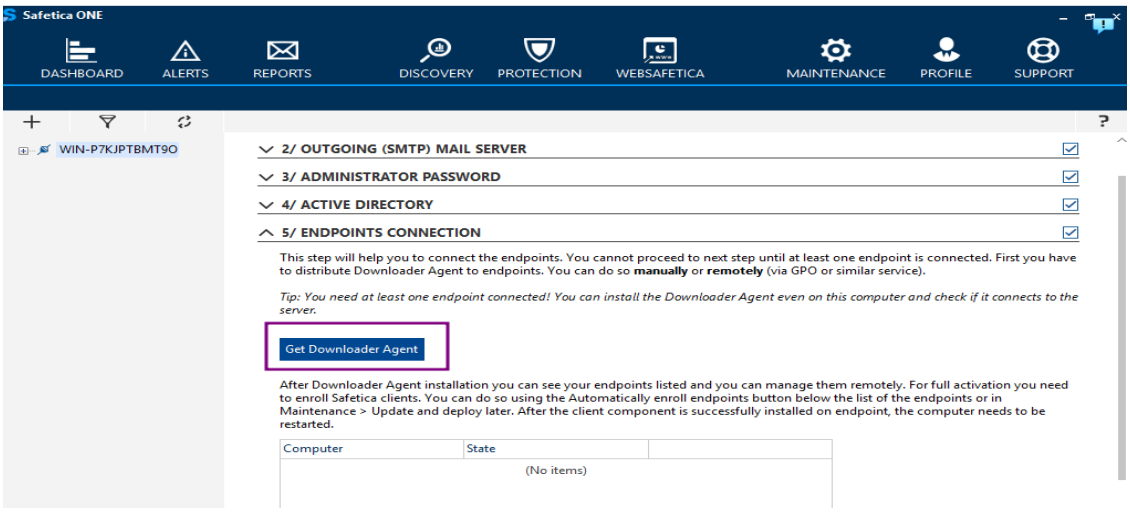

Рис. 3.13. Вікно для завантаження агента

10. Обираємо, куди завантажити інсталятор агента та натискаємо «Save» (рис.3.14 та рис.3.15).

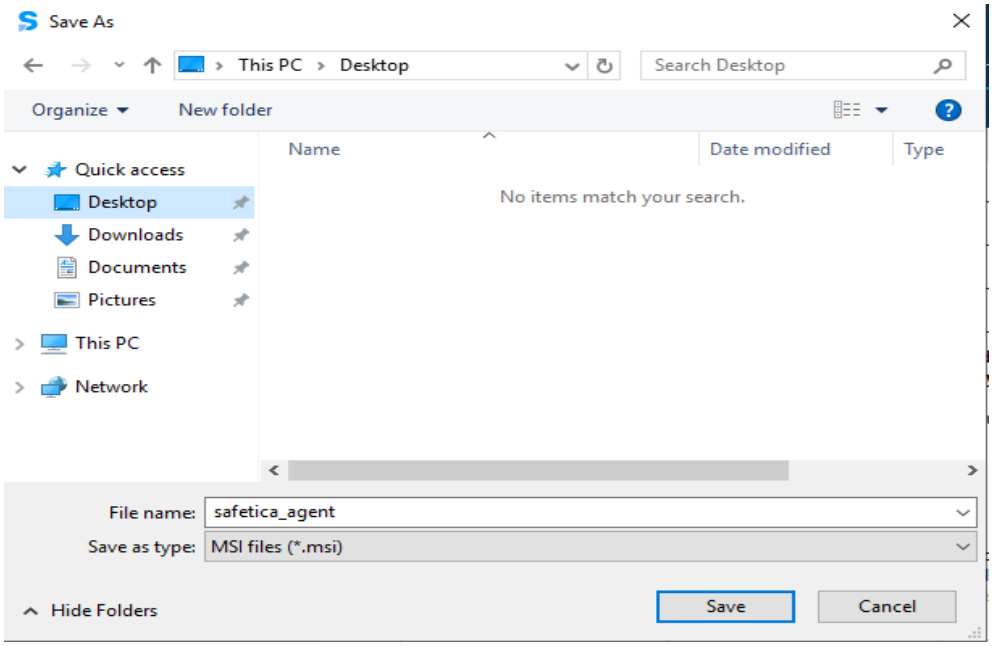

Рис. 3.14. Вікно вибору шляху завантаження

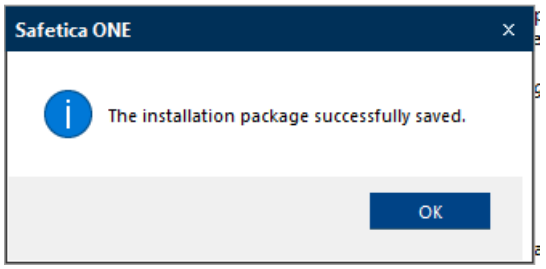

Рис. 3.15. Вікно успішного завантаження інсталятора агентам

11. Далі потрібно ввести ліцензійний ключ (рис.3.16).

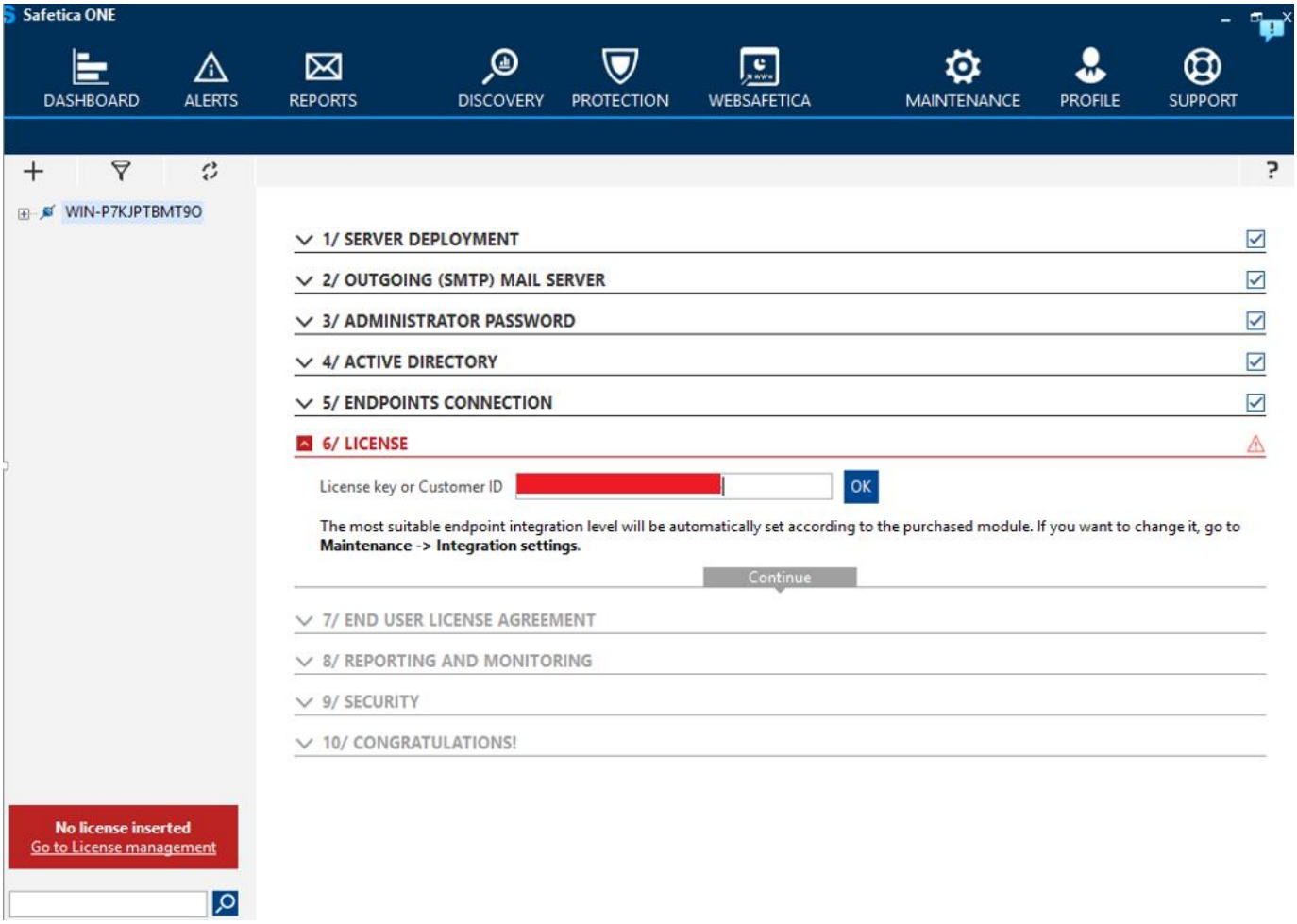

Рис. 3.16. Вікно вводу ліцензійного ключа

12. Вводимо дані адміністратора системи та погоджуємося з Safetica EULA (рис.3.17).

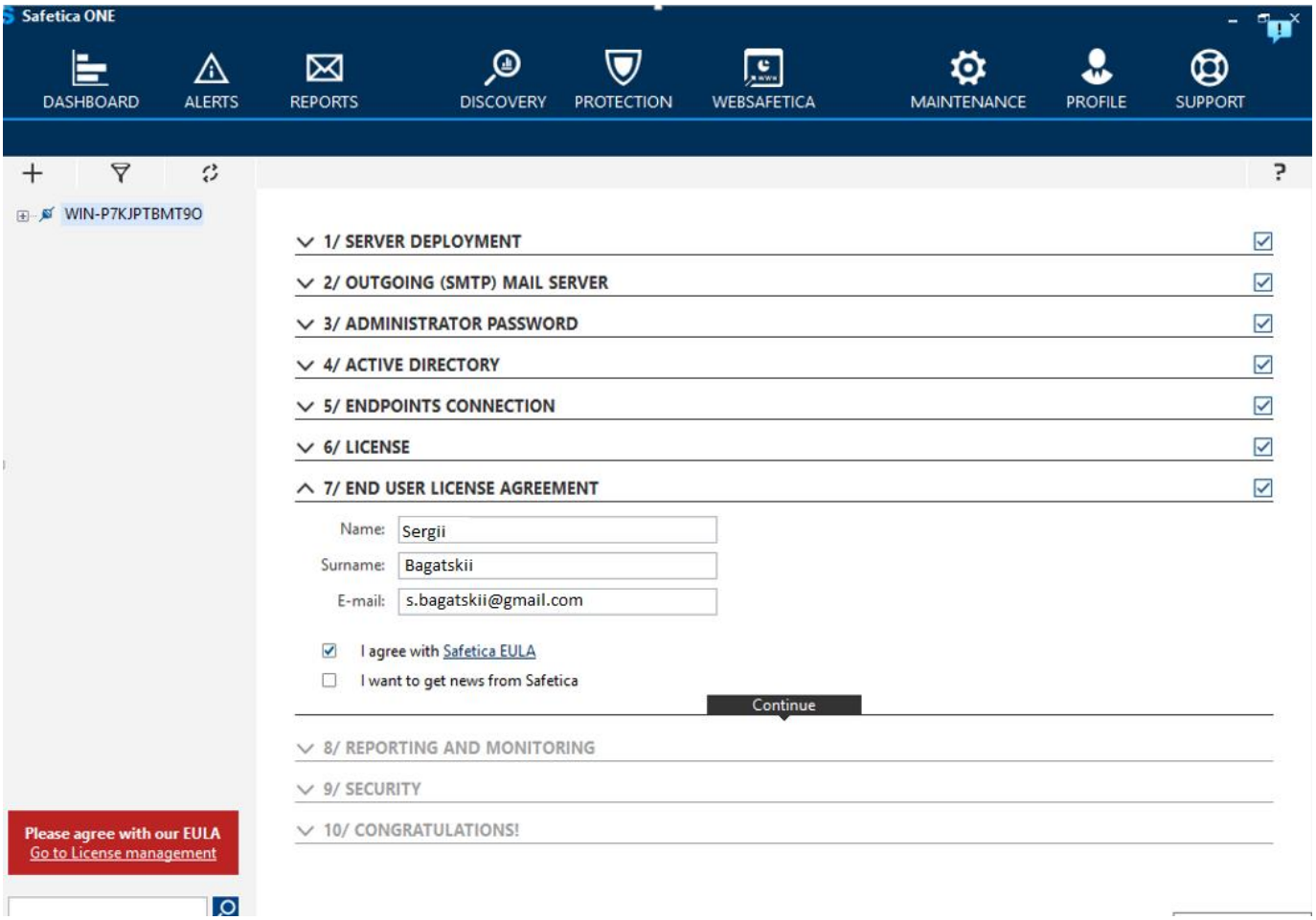

Рис. 3.17. Вікно вводу даних адміністратора

13. На даному етапі можна обрати доменну зону для електронної пошти компанії, встановити правила вмісту для опису конфіденційних даних. Після введення необхідної інформації натискаємо «Continue» (рис.3.18).

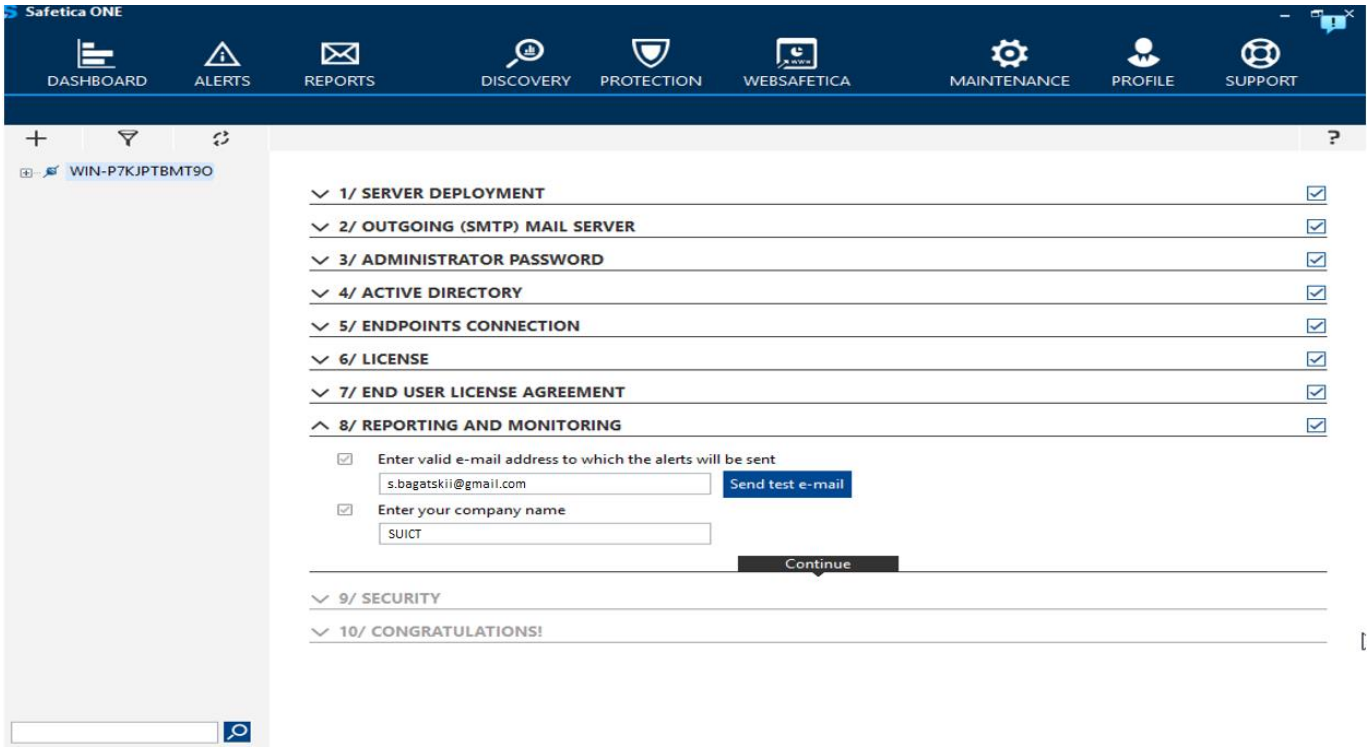

Рис. 3.18. Вікно для вводу назви компанії

14. Всі налаштування введені коректно і можна починати захист даних (рис.3.19).

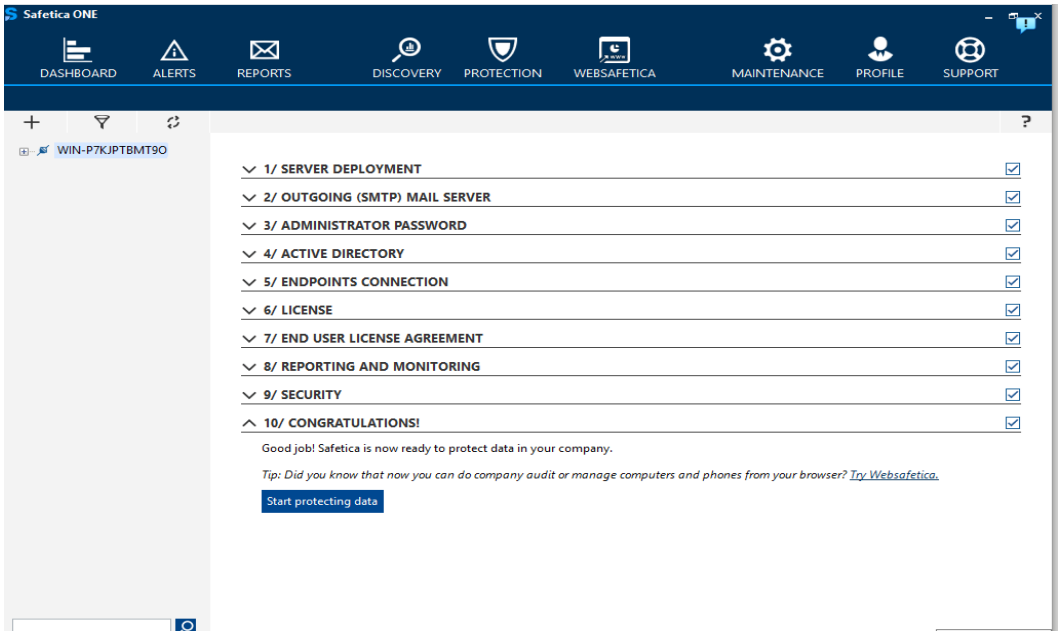

Рис. 3.19. Вікно підтвердження успішного налаштування системи

3.2. Оптимізація та підвищення ефективності DLP-системи

Успішна інтеграція будь-якого продукту в систему – це лише перший крок у використанні його функцій. Рішення Safetica DLP має інтерфейс, достатньо зрозумілий для адміністраторів безпеки. Safetica допомагає класифікувати дані та створити необхідні політики для запобігання витоку інформації.

Рішення Safetica DLP складається з двох основних модулів: Discovery (виявлення) та Protection (захисту).

Розділ Discovery містить огляд потенційних проблем безпеки та дозволяє краще зрозуміти процеси безпеки. З його допомогою можна перевіряти конфіденційні файли, витік яких може становити загрозу безпеці.

За допомогою аудиту апаратного забезпечення можна побачити, на які пристрої доставляються, як використовуються принтери та які файли завантажуються в корпоративну мережу. Даний модуль допомагає проаналізувати систему, щоб використати ці дані для налаштування політик. Він запише, які програми використовують працівники, які сайти відкривають в браузерах, з якими файлами працюють і куди можуть їх переносити чи надсилати. Вся ця інформація потрібна, щоб проаналізувати систему та працівників, провести аудит у організації та мінімізувати ризики витоку даних.

Розділ Protection забезпечує захист конфіденційних корпоративних даних від несанкціонованого використання, та таким чином дозволяє запобігти фінансовим втратам та шкоді репутації. На основі інформації отриманої з розділу Discovery, можна класифікувати відповідні дані та створити відповідні політики запобігання втратам даних. Для створення безпечних каналів передачі даних використовуються зони. В зонах створюються набори довірених та заборонених зовнішніх пристроїв, принтерів, IP-адрес, мережевих шляхів та електронних адрес.

Існує кілька послідовностей, як налаштувати захист DLP в розділі Protection. Для початку потрібно визначити, які саме дані вважати конфіденційними. Для цього

потрібно провести відповідний аудит всередині організації та вирішити, які будуть ступені захищеності файлів. Safetica пропонує декілька видів класифікацій конфіденційних даних, щоб потім використовувати їх під час створення політик:

• На основі конфіденційного вмісту (Based on content (Sensitive content)) — основний, найпростіший та рекомендований метод DLP-захисту, який використовує глибокий аналіз вмісту. Конфіденційні дані визначаються на основі їх вмісту за допомогою словників, алгоритмів, ключових слів або регулярних виразів.

• На основі тегів сторонніх програм (Існуюча класифікація) (Based on data tagging by thirdparty applications (Existing classification)) — інший варіант DLP-захисту, створений на основі існуючих тегів метаданих, які виконуються, наприклад, іншою програмою класифікації. Цей підхід можна використовувати для захисту даних, яким уже присвоєно певну класифікацію або рівень безпеки (наприклад, внутрішні, конфіденційні тощо).

• На основі контексту (Based on context (Context rules)) — DLP-захист на основі контексту. Це означає, що дані захищені залежно від того, хто з ними працює, де вони зберігаються, куди передаються, в яких програмах використовуються тощо. Конфіденційні дані захищені тегом Safetica. Цей метод можна використовувати для захисту даних, які не можна класифікувати на основі вмісту. Його складніше реалізувати та підтримувати, ніж інші варіанти. Він вимагає більш глибокого знання Safetica, а також детального аналізу та відповідності корпоративним процесам роботи з даними.

• На основі властивостей файлу (Based on file properties (File properties)) – категорії даних властивостей файлу дозволяють захищати файли на основі їх властивостей, таких як розширення файлів, незалежно від їх вмісту чи класифікації. Наприклад, ви можете захистити всі вихідні файли .pdf або .cad. Ці категорії також можуть розширювати існуючі політики DLP для захисту файлів, які не можна перевірити на предмет класифікації або конфіденційних даних (наприклад, зашифрованих файлів)[14].

Після проведення аналізу та прийняття рішення стосовно класифікації файлів потрібно обрати, під який саме класифікатор в Safetica підпадають ті чи інші дані. Створити відповідні категорії даних, для подальшого їх використання. У розділі Категорії даних можна створити необмежену кількість категорій даних. Категорії даних використовуються для класифікації файлів на різні групи залежно від того, хто, де і як може з ними працювати. Після створення категорій даних для них створюються різні DLP-політики і таким чином захищаються класифіковані дані.

Safetica використовує політики DLP для захисту даних на робочих станціях та для контролю поведінки програм. Політиками блокується переміщення інформації несанкціонованими шляхами, щоб запобігати потенційним витокам конфіденційної інформації. Є два типи політик: політика для збору журналів та політика блокування. В залежності від потреб можна створити будь-яку кількість політик. Вони допомогають попередити можливі витоки даних та зменшують збитки від можливого людського фактору працівників.

Створення політики з розпізнавання IBAN та номерів карток

Створення категорії даних потрібно починати з розуміння того, що необхідно захистити від витоку. Отже, перше, що захищаємо — це номери IBAN та кредитних карток. Вони можуть знаходитися в бухгалтерських документах та списках, наприклад, клієнтів чи робітників. В такому випадку потрібно використати категорію даних Sensitive content.

Необхідно відкрити Safetica Management Console та перейти в розділ Protection. Обрати підрозділ Data categories та натиснути «New data category» (рис.3.20).

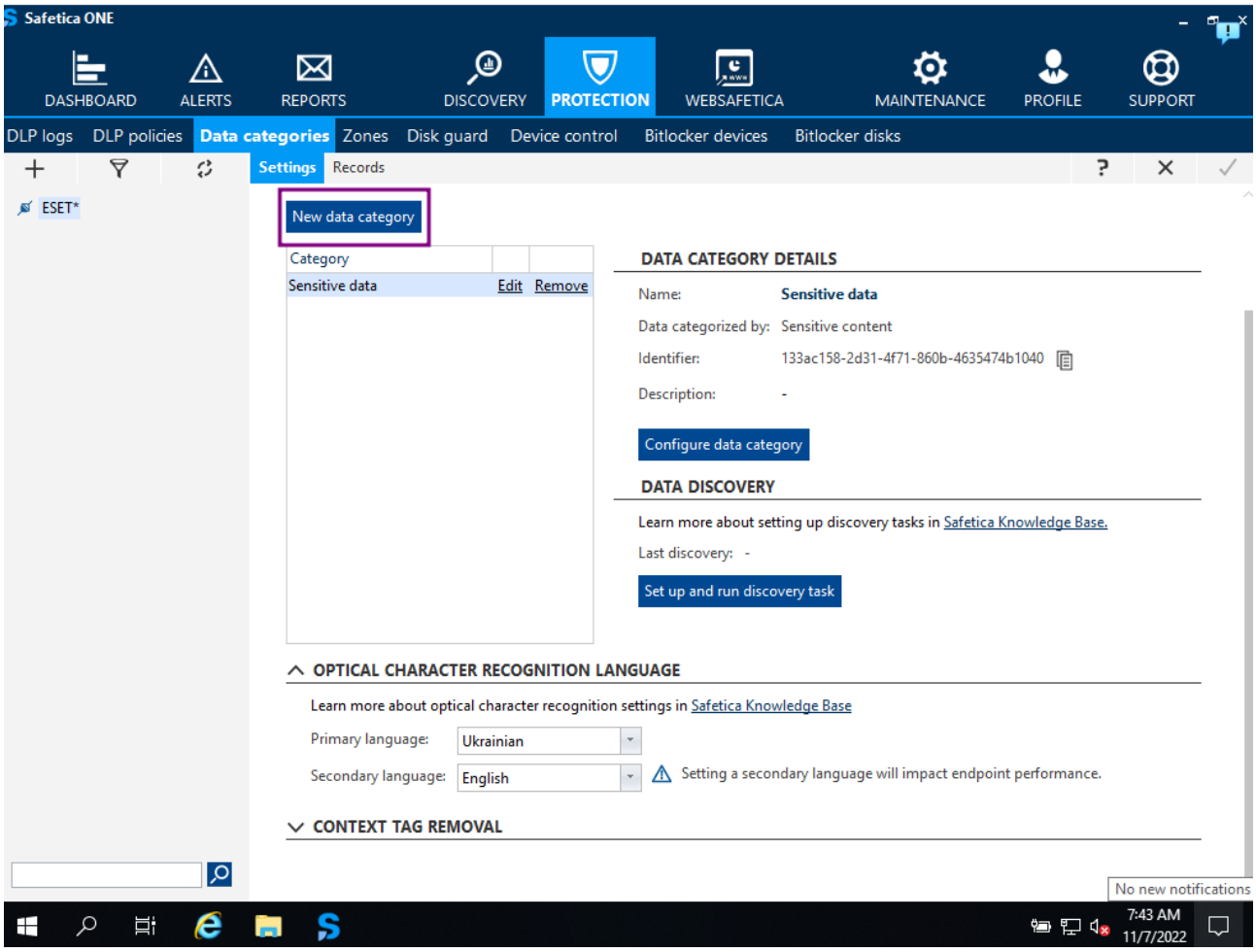

Рис. 3.20. Вікно підрозділу Data categories

Далі обирати тип категорії даних Sensitive content та ввести її назву. І натиснути «ОК» (рис.3.21).

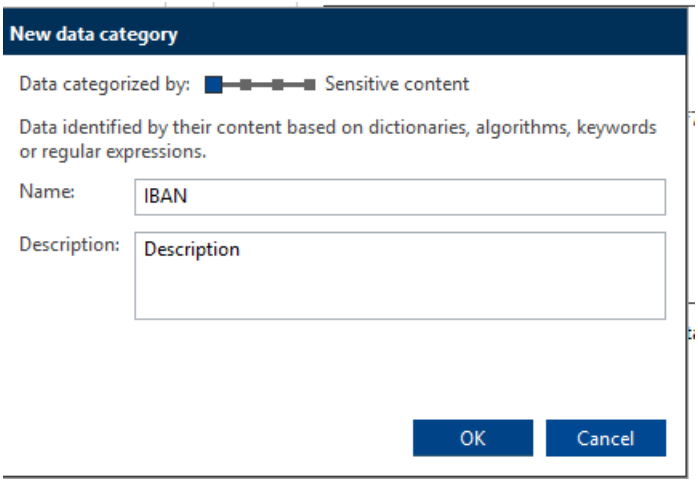

Рис. 3.21. Вікно вибору типу категорії даних

Повернувшись до попереднього вікна, обрати створену категорію даних та натиснути «Configure data category» (рис.3.22).

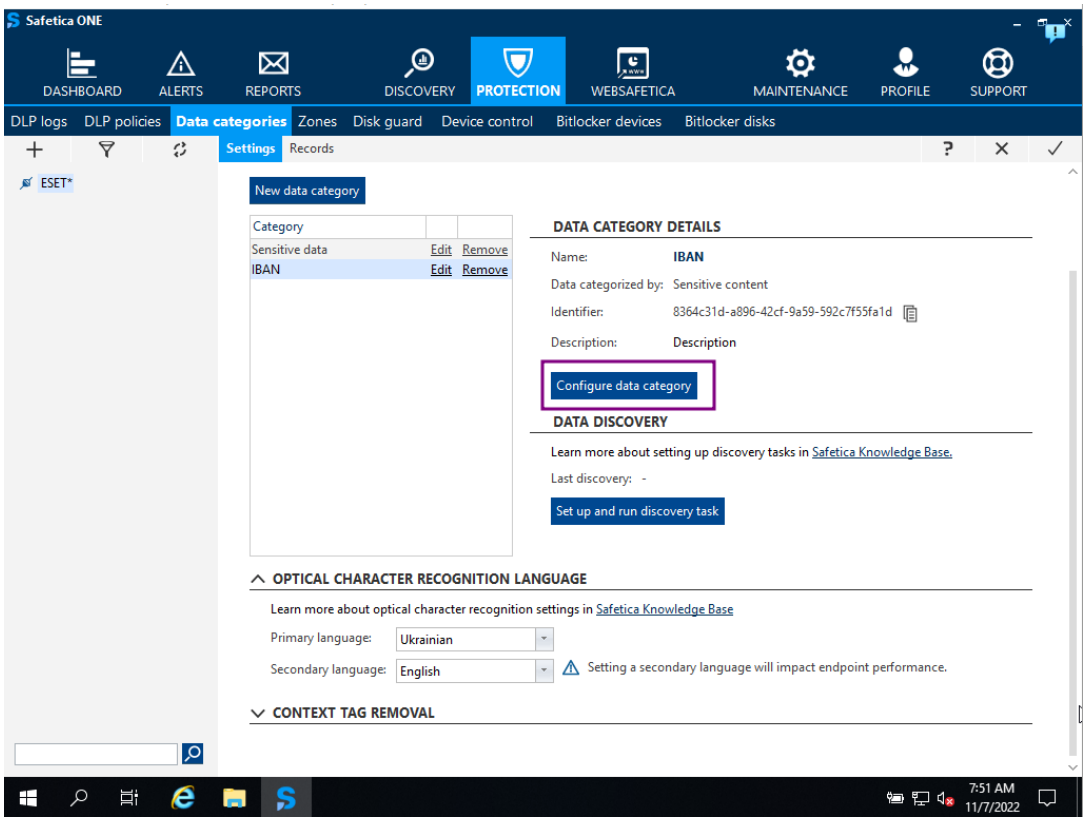

Рис. 3.22. Вікно вибору налаштування категорії даних

У наступному вікні потрібно обрати правило розпізнавання для категорії даних. Та натиснути «New detection rule» (рис.3.23).

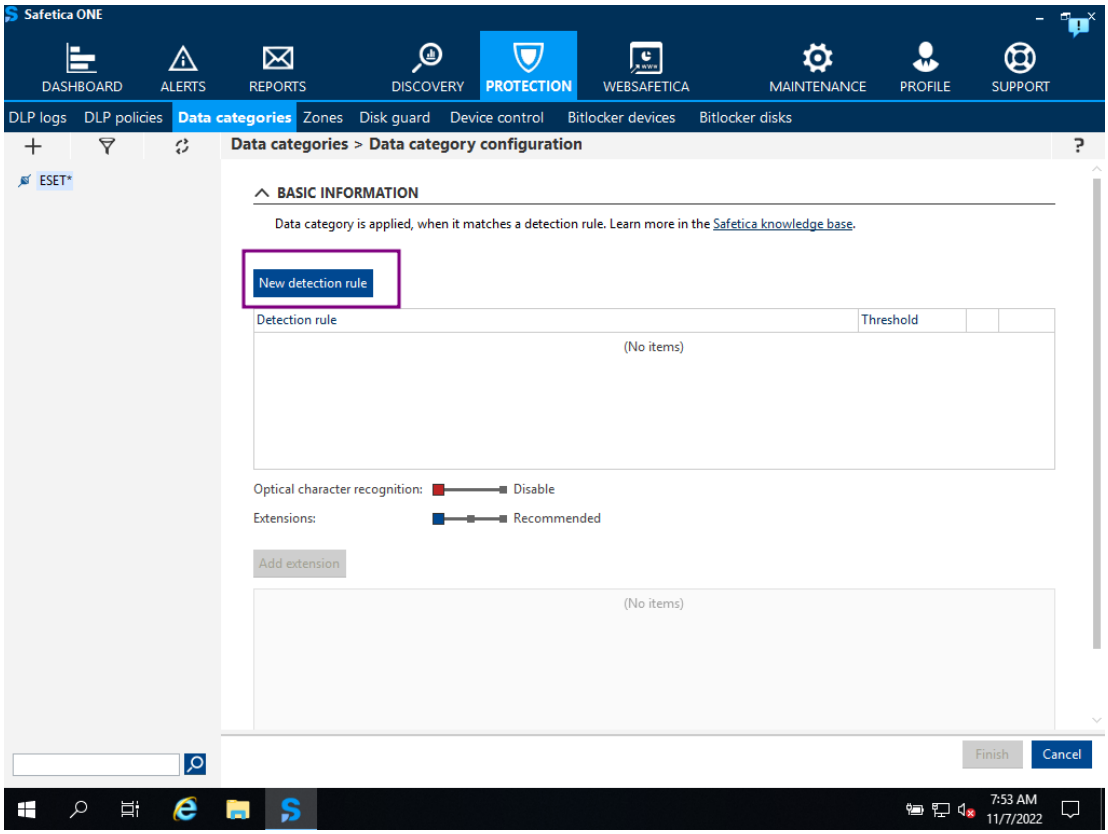

Рис. 3.23. Вікно налаштувань категорії даних

В новому вікні потрібно налаштувати правило розпізнавання. В першому розділі обрати кількість повторів обраної інформації в одному документі. В наступному розділі обрати інформацію, яку потрібно шукати в документах. Оберемо номери IBAN та натиснемо «ОК» (рис.3.24).

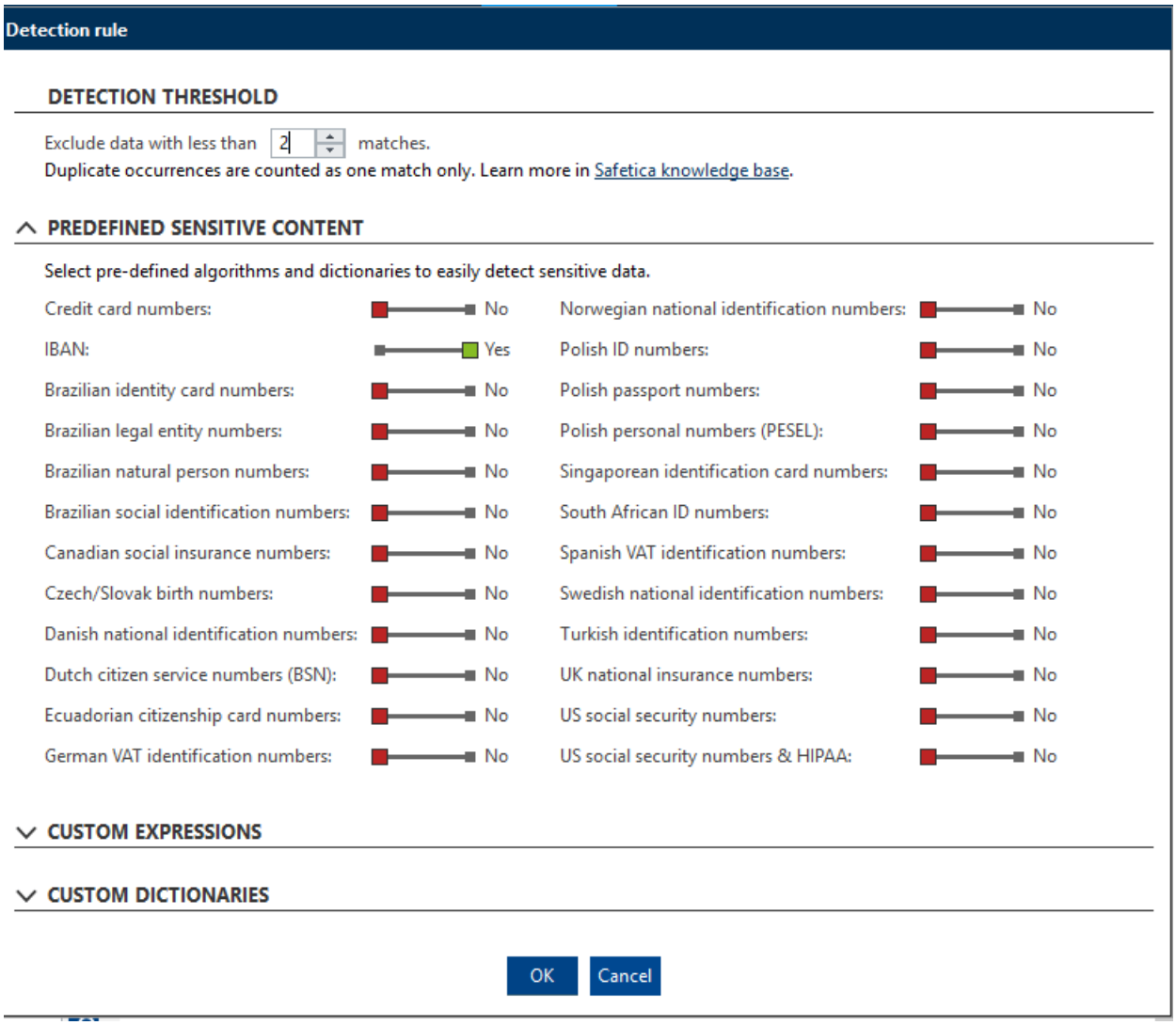

Рис. 3.24. Вікно створення правила розпізнавання IBAN

Аналогічним чином створити правило розпізнавання номерів кредитних карток. Після цього є можливість обрати розширення файлів. Якщо ви знаєте, які розширення найчастіше використовуються, то можете їх ввести вручну або обрати відповідну категорію розширень файлів. Натиснути «Finish» (рис.3.25).

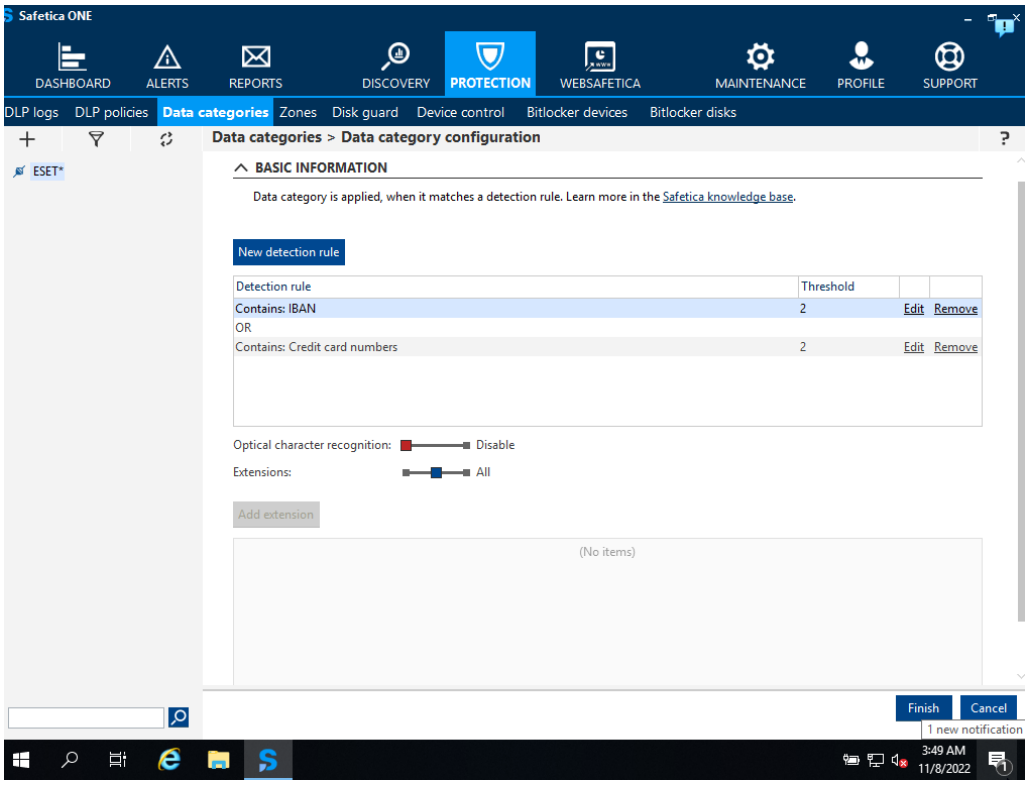

Рис. 3.25. Вікно створеного правила розпізнавання

Наступний крок - це створення політики. Для цього переходимо в підрозділ DLP policies. (рис.3.26).

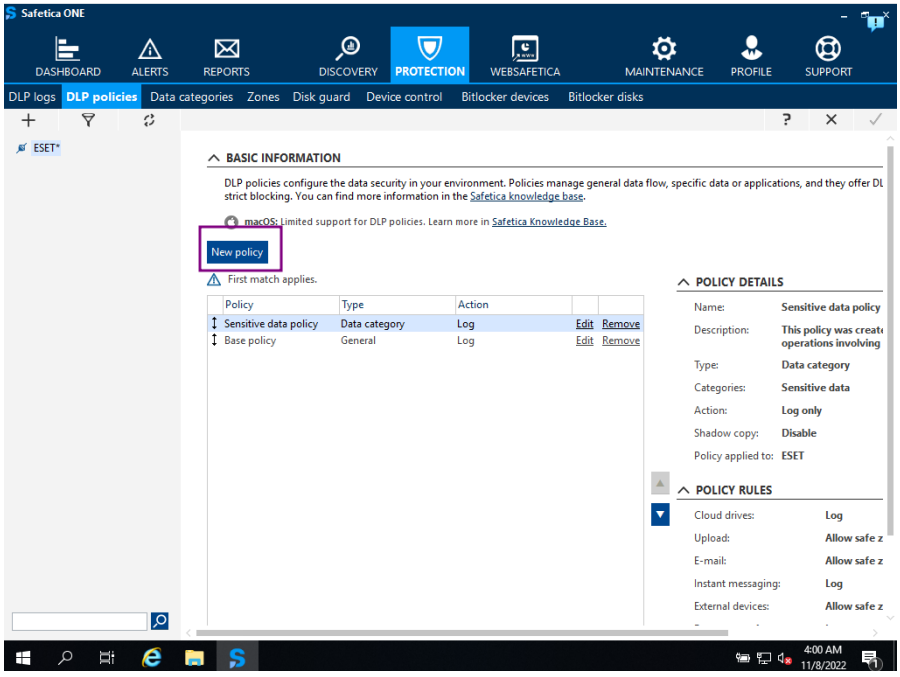

Рис. 3.26. Вікно підрозділу DLP policies

У новій вкладці потрібно обрати тип політики, яку необхідно створити. Потрібно обрати тип Data та обрати категорію даних, яку попередньо створили. Далі «Next» (рис.3.27).

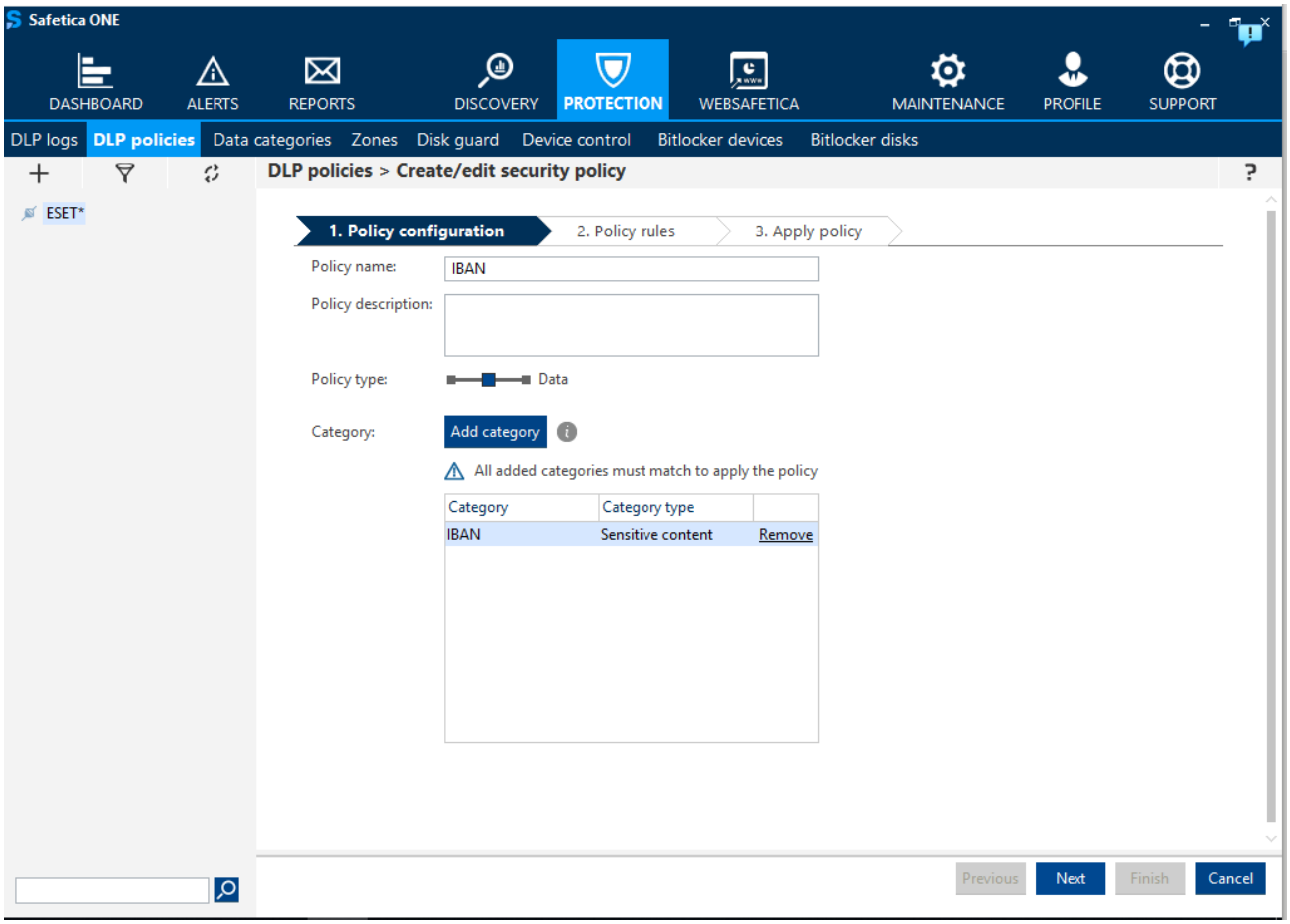

Рис. 3.27. Вікно вибору типу політики

Далі потрібно обрати дію, яку буде виконувати політика (логування або блокування). Обирати дію Log and block. Щоб переглянути доступні правила політики DLP, необхідно натиснути «Customize». Доступні правила будуть розміщені у списку. Для створення нових DLP-політик також можна використовувати шаблони політик - заздалегідь визначені групи правил (рис.3.28).

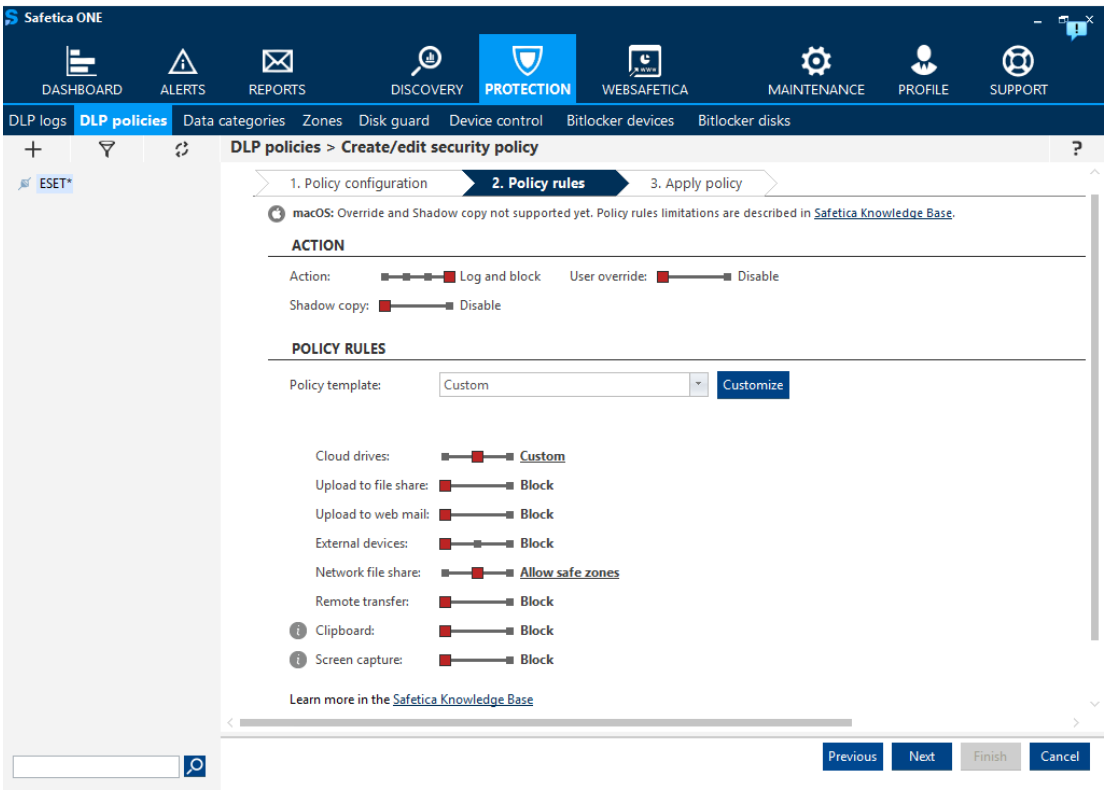

Рис. 3.28. Вікно вибору налаштувань політики

В наступному вікні обрати ПК чи користувача до якого буде застосовано політику (можна обрати відразу всю організацію, тоді політика буде застосовуватися до всіх ПК та користувачів). Далі «Finish» (рис.3.29).

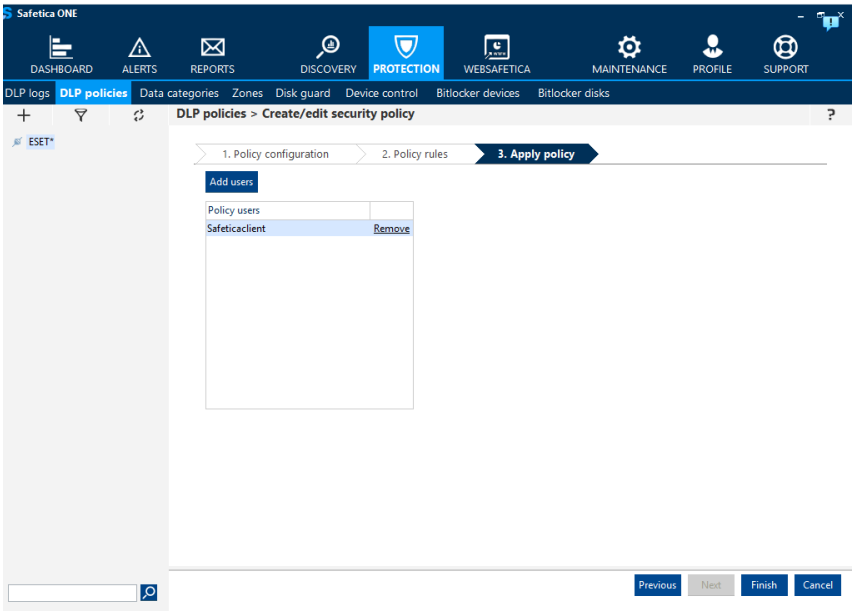

Рис. 3.29. Вікно вибору ПК чи користувачів

Зберігаємо налаштування в підрозділі DLP policies.

Створення політики з використанням тегів

Наступна категорія даних доступна, якщо помістити документ у відповідну папку. Тобто після перегляду всі документи сортуються за важливістю, а потім поміщаються в папки з відповідними правами доступу. Щоб мінімізувати ризик витоку такої важливої інформації, потрібно використовувати контекстні категорії даних правил. З відповідними налаштуваннями призначаються відповідні теги кожному документу на основі файлової системи. Кінцеві користувачі не можуть видалити або змінити цю мітку, усі ці дії виконуються лише в консолі адміністратора. Тег залишається в документі, і якщо розширення перейменовано або змінено розширення, тег залишається на місці, навіть якщо відповідний документ заархівовано, оскільки він призначений на основі файлової системи [12-14].

Для того, щоб створити категорію даних Context rules необхідно відкрити Safetica Management console та перейти в розділ Protection. Обирати підрозділ Data categories та натиснути «New data category», щоб створити відповідну категорію даних. У вікні вибору типу категорії даних обирати Context rules та ввести її назву. Після цього натиснути «ОК» (рис.3.30).

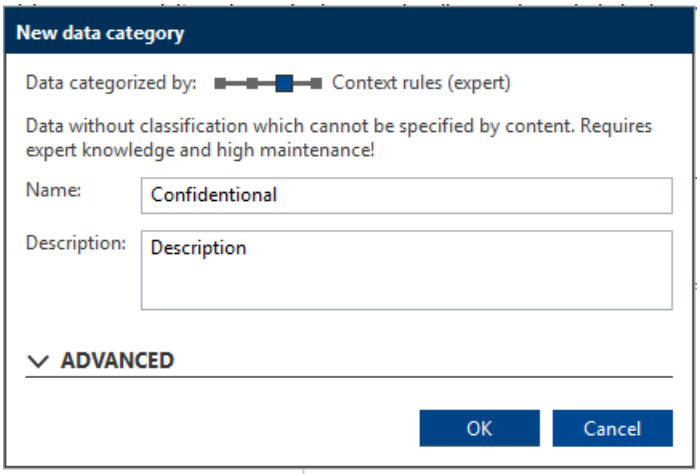

Рис. 3.30. Вікно вибору типу категорії даних

Обрати щойно створену категорію даних та натиснути «Configure data category», щоб налаштувати її. У новому вікні знаходимо розділ Path rules. В даному розділі створити правило тегування файлів за шляхом до відповідної теки. Натиснути «Add» (рис.3.31).

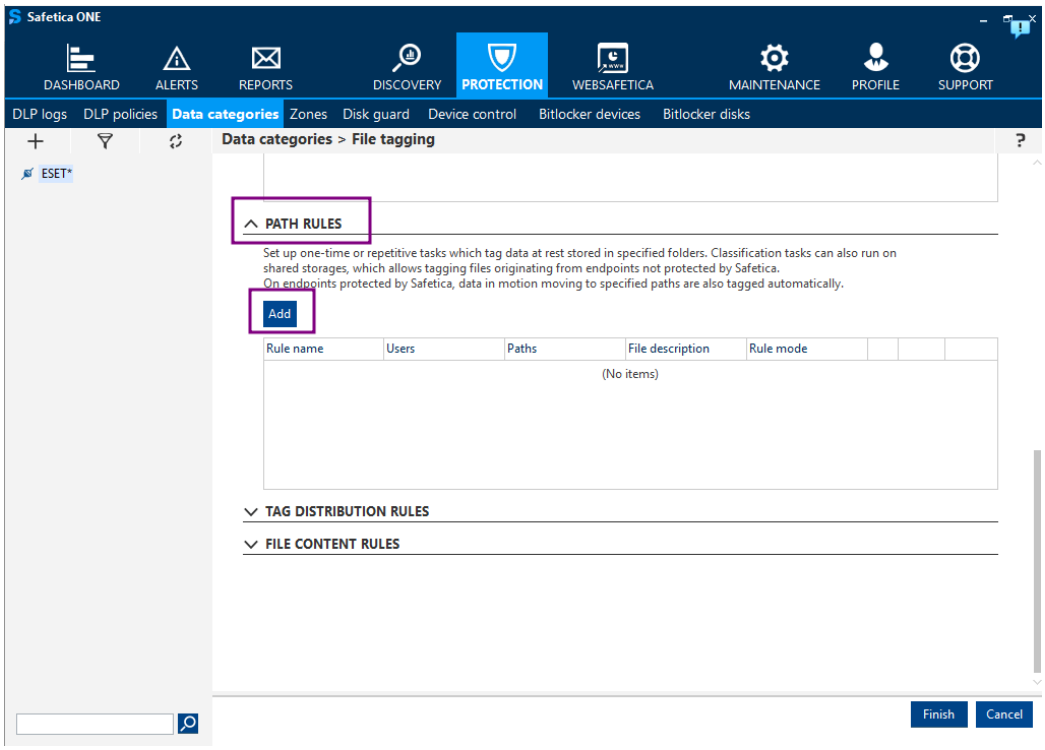

Рис. 3.31. Вікно створення правила тегування

У новому вікні потрібно налаштувати відповідне правило тегування. Спочатку потрібно ввести назву правила. Потім поставити правило тегування. Далі обрати ПК, де буде застосовуватися правило (можна обрати всю організацію, якщо є доступ до теки в локальній мережі). Після цього ввести шлях до відповідної теки з конфіденційним вмістом. Далі обрати розширення. Після введення всієї необхідної інформації натиснути «Finish» (рис.3.32).

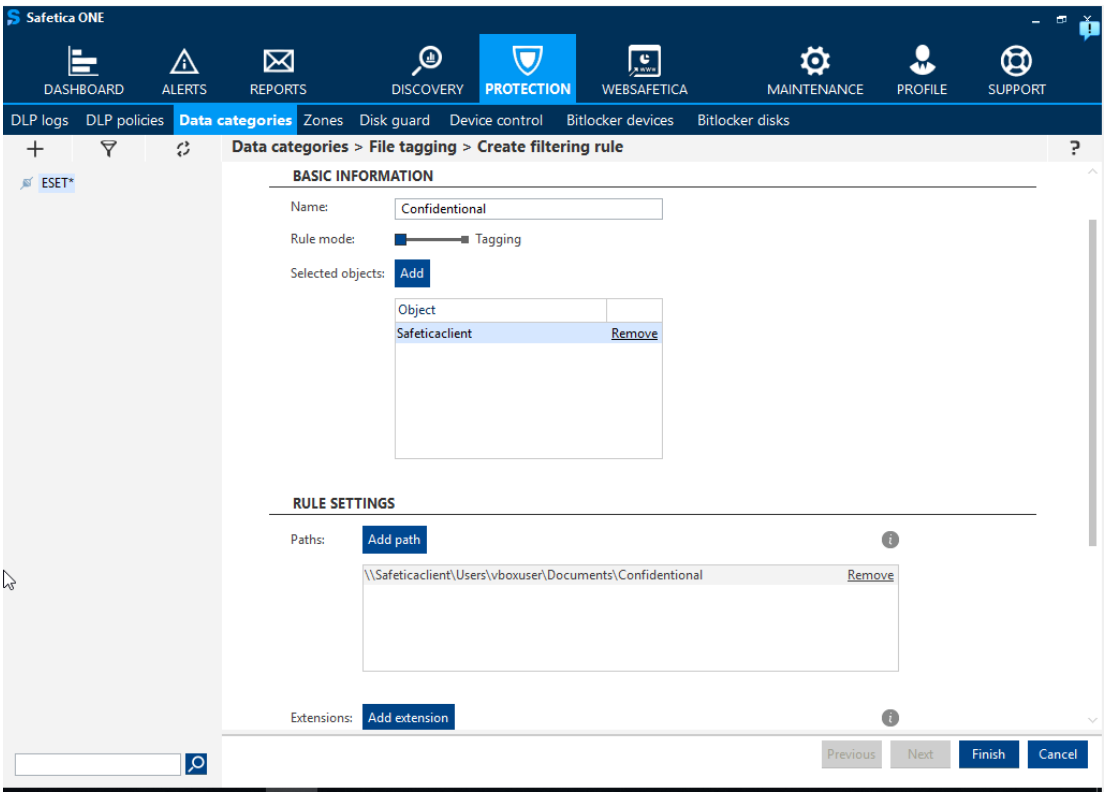

Рис. 3.32. Вікно створення правила тегування

Перевірка створеного правила тегування за шляхом до теки та натиснути «Finish», щоб категорія даних успішно збереглася (рис.3.33).

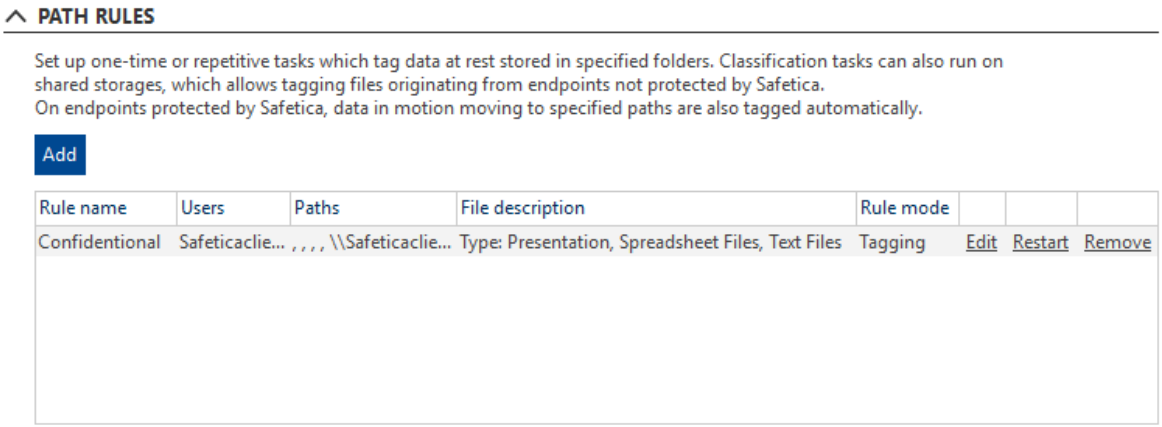

Рис. 3.33. Створене правило тегування

Після успішного створення категорії даних перейти до створення політики. В новому вікні вводимо назву політики та обираємо тип Data. Далі обирати із

випадаючого списку попередньо створену категорію даних Context rule. Після цього перейти до налаштування політки натиснувши «Next». Використати дію Log and block, щоб мінімізувати можливий витік конфіденційний тегованих файлів. Налаштовати правила політики та натиснути «Next». Далі обирати ПК та\або користувачів, до яких буде застосовуватися політика і натиснути «Finish» (рис.3.34).

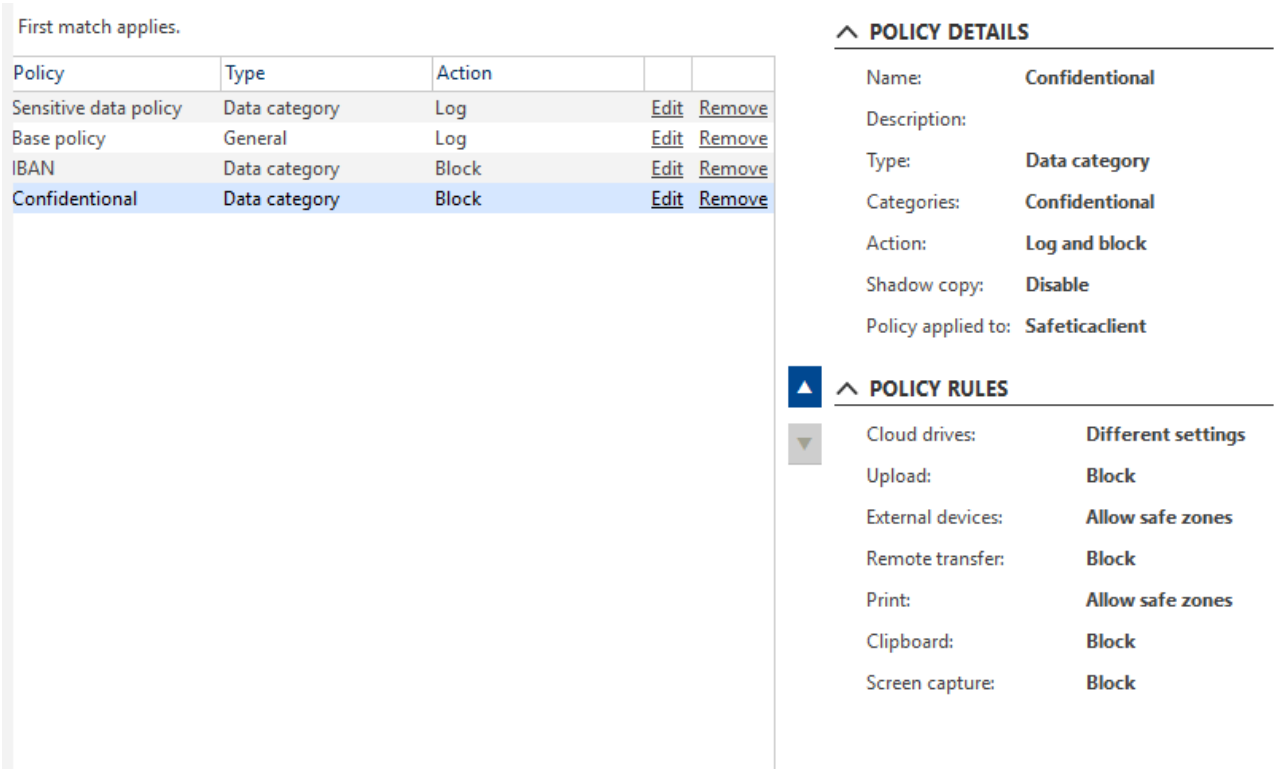

Рис. 3.34. Перегляд налаштувань політики

Перевірити правильність налаштувань та зберегти політику.

Наступним кроком є перевірка, чи застосувалися правила тегування до відповідних файлів. Переходимо на клієнтський ПК та відкриваємо командний рядок. Вводимо команду dir C:\Users\vboxuser\Documents\Confidentional /r. Команда видає детальну інформацію про всі файли в теці. Бачимо, що у властивостях файлу є прописаний тег SafTag5. Це означає, що правило тегування працює коректно (рис.3.35).

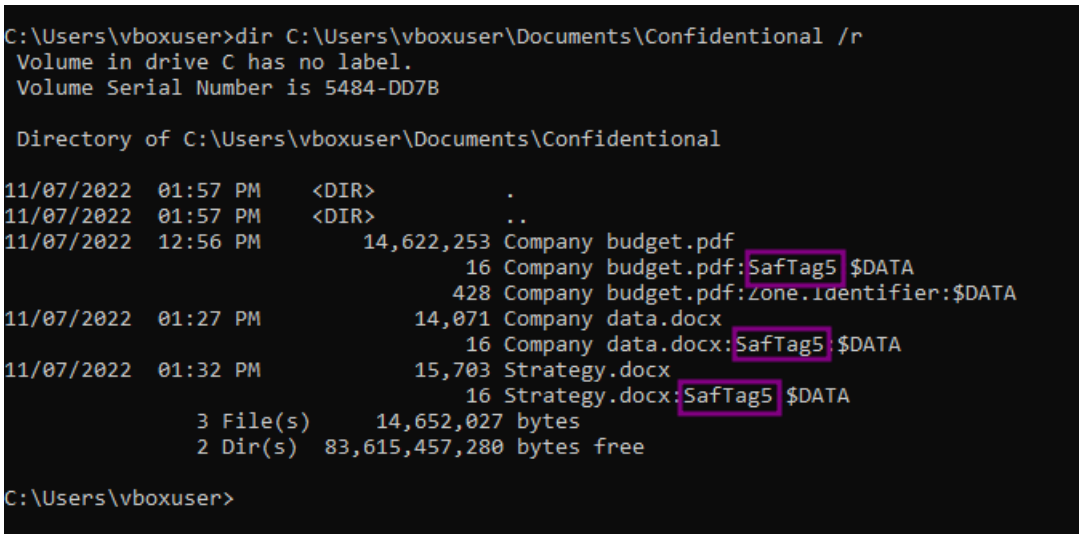

Рис. 3.35. Вивід команди з детальною інформацією про файли

Створення політики з використанням WebSafetica

DLP-рішення Safetica має в своєму арсеналі веб консоль WebSafetica. Вона частково дублює і доповнює консоль управління. Вона є сайтом, тому доступна у вашій локальний мережі організації і націлена більше на керівництво та менеджерів, так як відображає інформацію з аналізу поведінки працівників та їх активність.

За допомогою WebSafetica створюються політики блокування доступу до додатків та веб сайтів на ПК. Так обмежується доступ працівників, щоб вони не могли використовувати неавторизовані у вашій системі додатки для передачі інформації. Для простих працівників зручніше відправити документ у месенджері, чим використовувати дозволені шляхи передачі конфіденційної інформації. Щоб запобігти виникненням таких ситуації на робочому місці, необхідно превентивно заблокувати доступ до месенджерів (додатків і веб версій) на робочих комп’ютерах [12-14].

Виконати відповідне налаштування необхідно відкривши WebSafetica та авторизуватися. В розділі Policies в якому є два види налаштування політик доступу: додатки та веб сайти. Обирати спершу Websites та натиснути «Add policy» (рис.3.36).

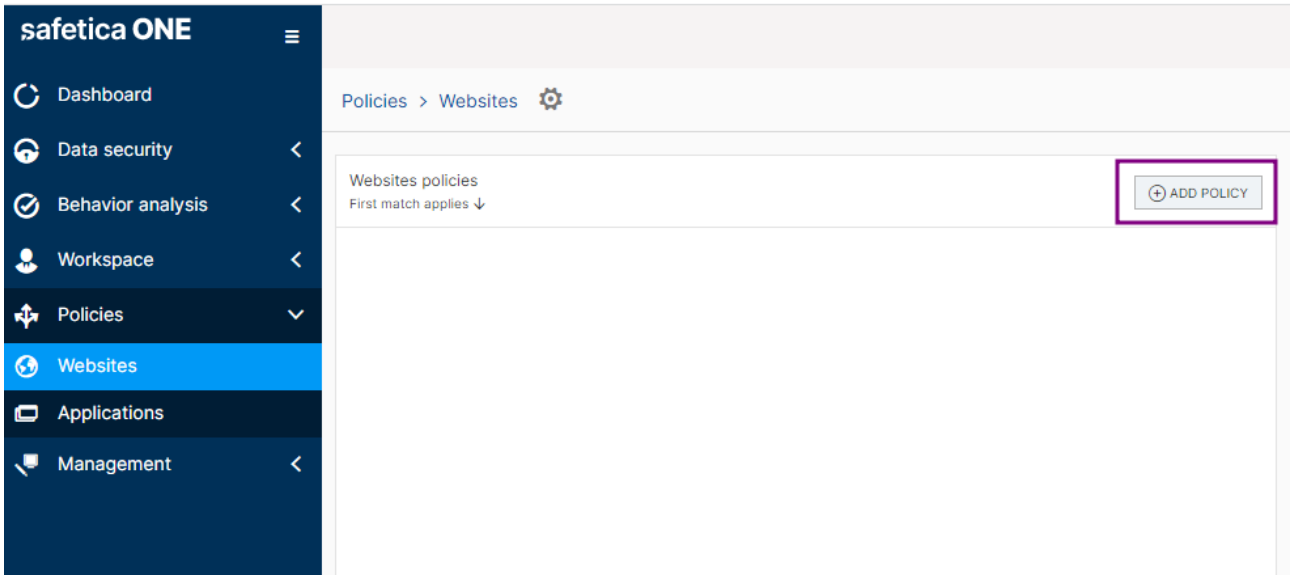

Рис. 3.36. Вікно додавання нової політики

Після цього налаштувати політику доступу. Ввести назву, обираємо до яких ПК буде застосовуватися політика. Наступним кроком додати правило блокування «Add rules». В новому вікні обрати готову категорію веб сайтів або ввести відповідний сайт вручну через URL (рис.3.37).

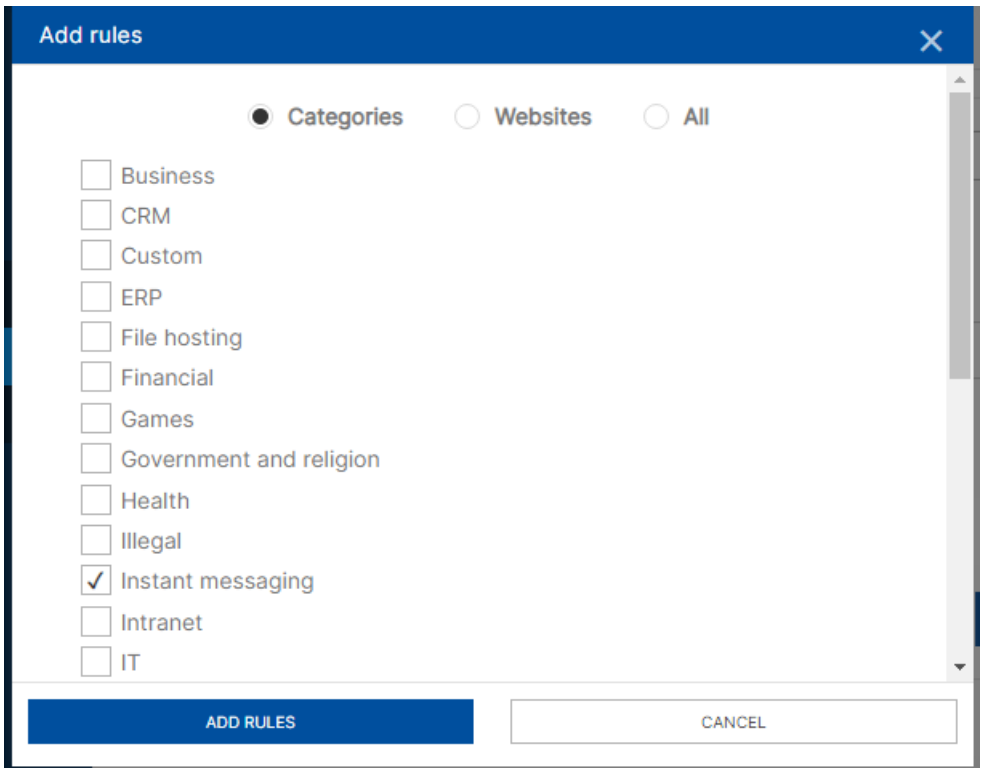

Рис. 3.37. Вікно налаштування правила блокування

Після вибору, які саме веб сайти блокувати, натисути «Add rules».

Далі перевіряємо введені дані та натискаємо «Add policy» (рис.3.38).

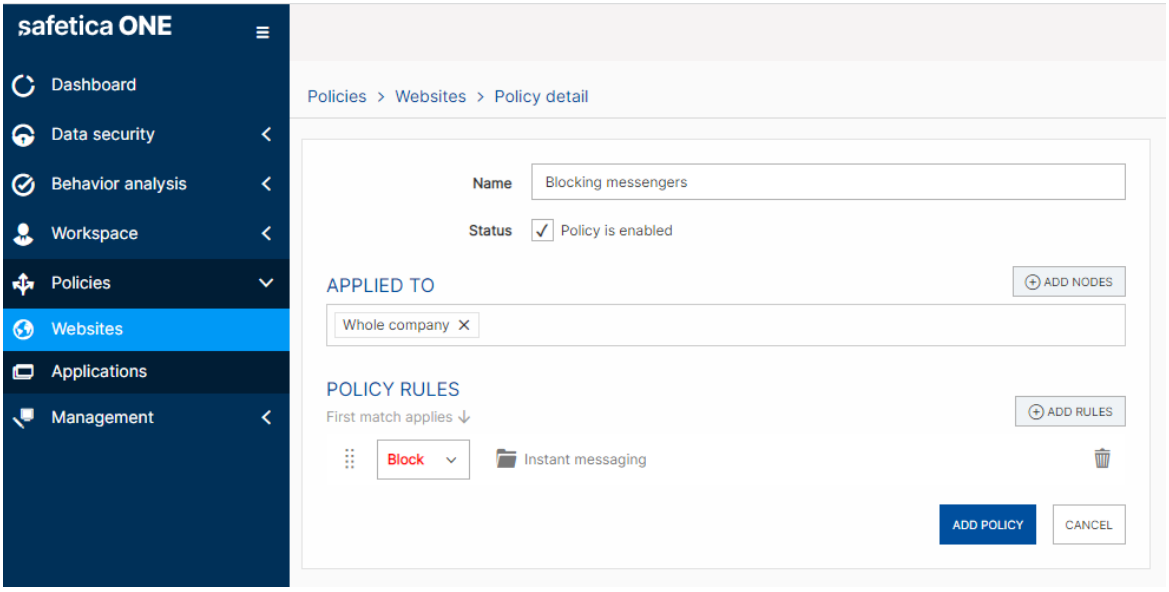

Рис. 3.38. Вікно перегляду налаштувань політики

Далі додати правило блокування доступу до додатків. «Add rules» аналогічно до політики блокування доступу до веб сайтів, можна блокувати доступ до додатків за категоріями додатків або обрати відповідний додаток із списку встановлених (рис.3.39).

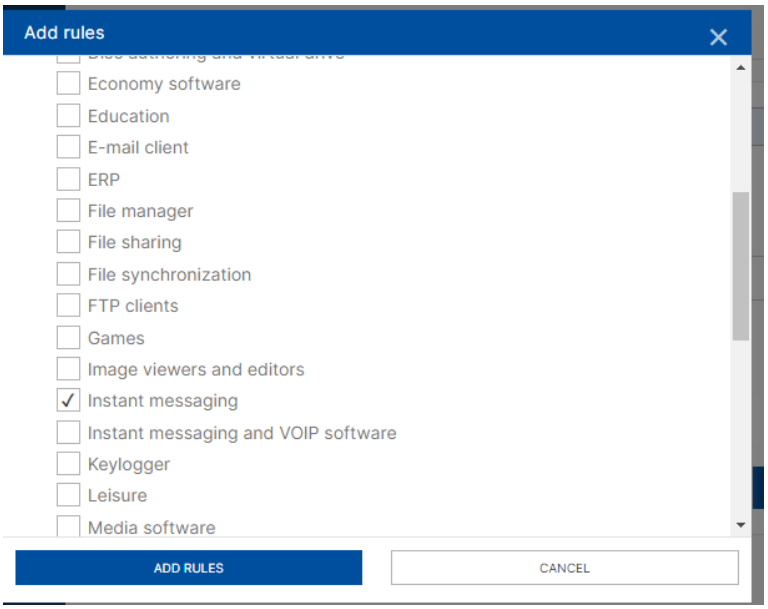

Рис. 3.39. Вікно вибору політики блокування

Після вибору правила блокування, натиснути «Add rules». Перевірити правильність введених даних, для коректної роботи політики та натиснути «Add policy» (рис.3.40).

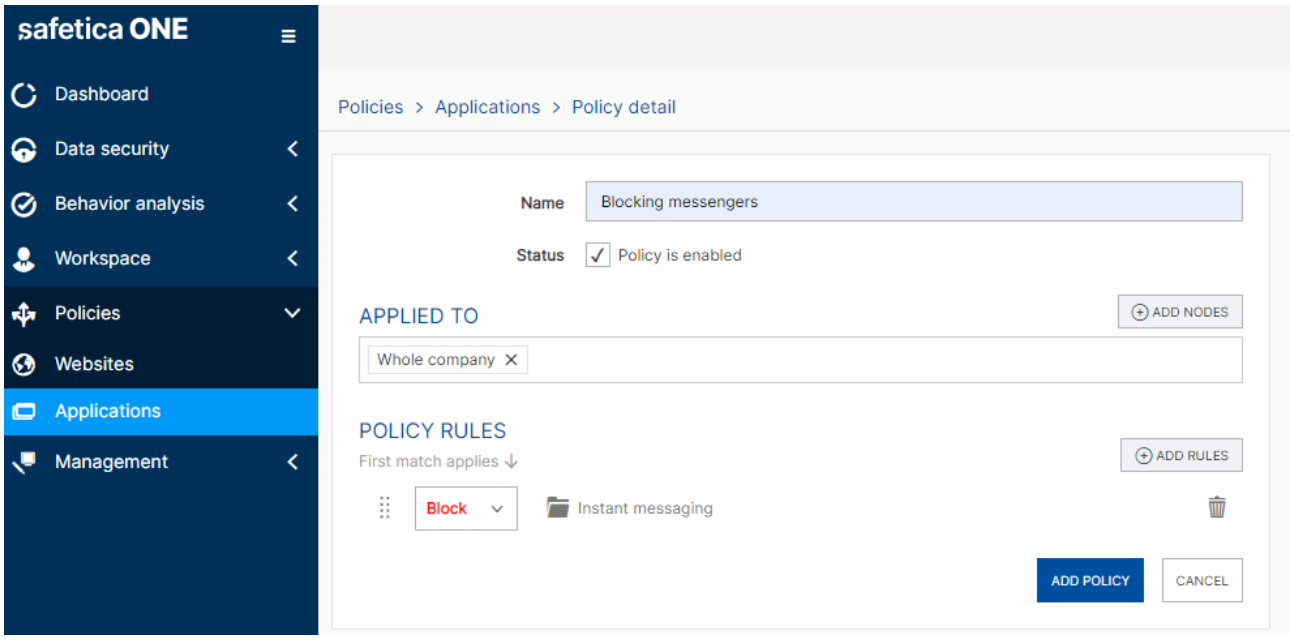

Рис. 3.40. Вікно перегляду налаштувань

Обидві політики успішно створені та застосовані до відповідних ПК.

Щоб переглянути, що в них входить в консолі управління, зайшовши в розділ Maintenance та обравши меню Categories. Тут зберігається інформація про категорії додатків, веб сайтів та категорії розширення файлів. Їх можна редагувати та створювати нові. Для цього потрібно натиснути біля відповідної категорії «Browse database» (рис.3.41).

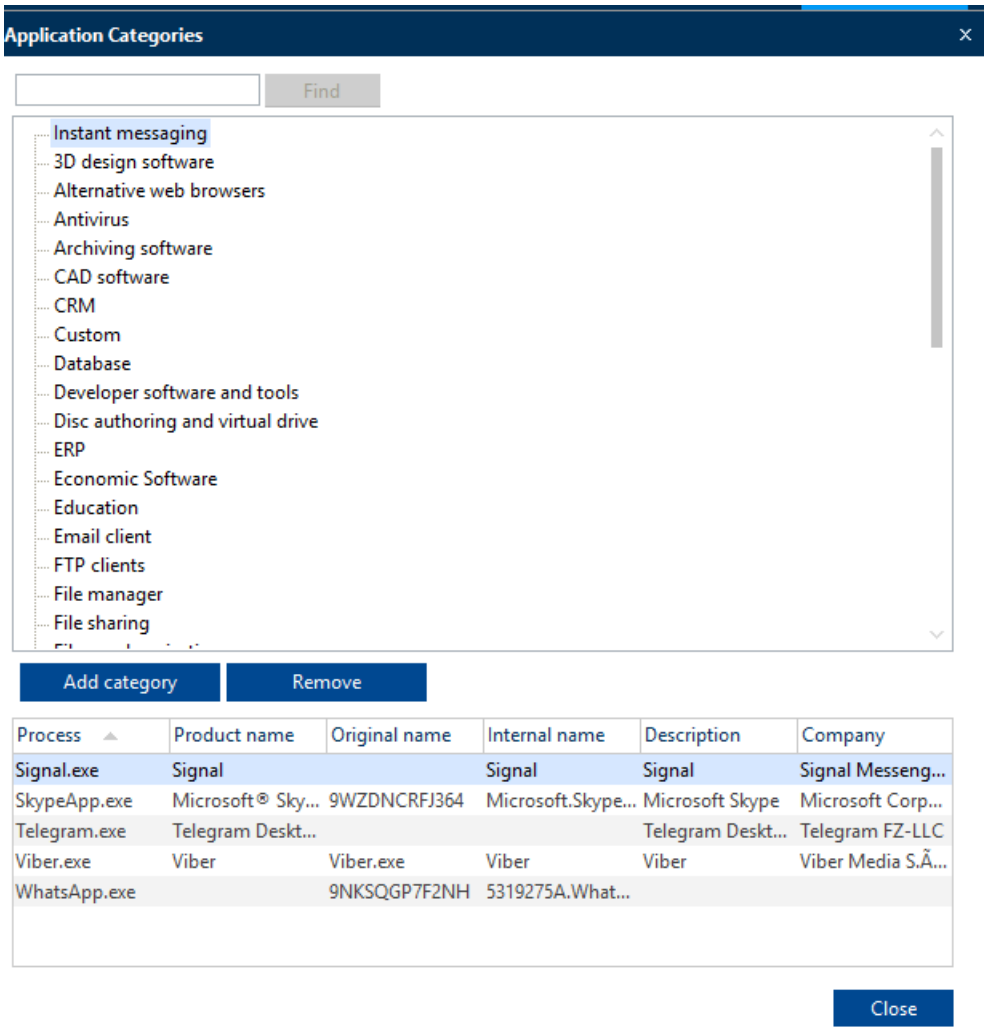

Рис. 3.41. Вікно перегляду категорій додатків

3.3. Розроблення рекомендацій щодо застосування технології протидії витокам даних в організації на основі DLP

Проаналізувавши попередні розділи та можливості технологій протидії витокам даних, приведемо рекомендації щодо застосування розробленої технології протидії витокам даних в організації на основі DLP Safetica One, що містить наступне:

1. Необхідно проаналізувати діяльність організації та сценарії витоку даних.
2. Розмежувати типи даних до відповідної категорії.
3. Оцінити наслідки та втрати витоку даних.

4. Вірно налаштувати DLP систему для протидії вторгнень.

5. Оптимізувати ефективність системи за допомогою тонких налаштувань політик безпеки та різних сервісів.

6. Поетапне впровадження DLP, починаючи з обмежених ділянок організації.

7. Навчання персоналу щодо правил та політик організації. Важливо зрозуміти, як працівники повинні поводитися з конфіденційною інформацією та як реагувати на повідомлення від системи.

8. Налаштування DLP для автоматичної реакції на порушення політики та введення механізмів попереджень для персоналу.

9. Постійний моніторинг роботи технології DLP та регулярне оновлення її правил та бази даних.

10. Інтеграція DLP з іншими засобами безпеки, такими як антивірусні програми, брандмауери, IDS/IPS та SIEM для створення комплексної системи безпеки.

11. Регулярне проведення аудиту ефективності технології DLP.

Висновки до розділу 3

Отже, в даному розділі було встановлено та налаштовано систему протидії витокам даних DLP Safetica One. Проведена детальна оптимізація для підвищення ефективності системи протидії витокам даних. Розроблено рекомендації щодо застосування технології протидії витокам даних в організації на основі DLP Safetica One.

Застосування цих рекомендацій сприяє оптимальному використанню технології DLP, забезпечуючи високий рівень безпеки даних та готовність організації до зустрічі з викликами кібербезпеки у сучасному бізнес-середовищі.

ВИСНОВКИ

У світі, де об'єм та цінність цифрової інформації стрімко зростає, захист від витоку даних стає ключовим для забезпечення стійкості, конфіденційності та цілісності даних організації. Використання технології протидії витокам даних на основі DLP (Data Loss Prevention) виявляється важливим стратегічним вибором для багатьох компаній, які прагнуть захистити свою конфіденційну інформацію та виконати вимоги сучасного кібербезпекового ландшафту.

В першому розділі було проаналізовано проблеми забезпечення безпеки організації від витоку даних. Визначено методи атак та проаналізовано типові сценарії витоку даних та їх наслідки. Розглянуто ключові моменти нормативних документів, що відповідають за регулювання, визначення та відповідальність порушень, щодо конфіденційних даних. Проведено оцінку наслідків витоку даних організації.

В другому розділі проаналізовано та приведені методи та засоби захисту від витоку даних. Було визначено основні принципи роботи DLP-систем та загальна архітектура. Описано архітектуру, основні компоненти та функціональні можливості DLP Safetica ONE, що дозволяє легко інтегруватися з різноманітними системами безпеки для кращого захисту даних від витоку чи несанкціонованого доступу до них.

В третьому розділі було встановлено та налаштовано систему протидії витокам даних DLP Safetica One. Проведена детальна оптимізація для підвищення ефективності системи протидії витокам даних. Розроблено рекомендації щодо застосування технології протидії витокам даних в організації на основі DLP Safetica One.

Застосування цих рекомендацій сприяє оптимальному використанню технології DLP, забезпечуючи високий рівень безпеки даних та готовність організації до зустрічі з викликами кібербезпеки у сучасному бізнес-середовищі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Багацький С. П. Технології протидії витокам даних в організаціях. Актуальні проблеми кібербезпеки : Всеукр. науково-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 17–19.

2. 5 Ways to Effectively Prevent Data Leakage. SecurityScorecard. URL: https://securityscorecard.com/blog/ways-to-prevent-a-data-leakage/ (date of access: 02.11.2023).

3. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 03.11.2023).

4. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI : станом на 8 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 03.11.2023).

5. Кондратенко М. Система запобігання витоку інформації на підприємстві : Дипломна робота "Бакалавра". Київ, 2021. 56 с.

6. Гончаренко Є. О. Вибір підходу до оцінки ризиків інформаційної безпеки для підприємств роздрібної торгівлі : Магістерська дисертація. Київ, 2018. 92 с.

7. Методи і способи захисту інформації. Pidru4niki. URL: https://pidru4niki.com/1801051351329/ekonomika/metodi_sposobi_zahistu_informatsiyi (дата звернення: 03.11.2023).

8. What Is DLP and How Does It Work? | Trellix. Trellix | Revolutionary Threat Detection and Response. URL: https://www.trellix.com/security-awareness/data-protection/how-data-loss-prevention-dlp-technology-works/ (date of access: 03.11.2023).

9. Boehm A. What is Data Loss Prevention (DLP)? [Guide] - CrowdStrike. crowdstrike.com. URL: https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/ (date of access: 04.11.2023).

10. What is DLP? Data Loss Prevention, Meaning & Definition. Netskope. URL: https://www.netskope.com/security-defined/what-is-data-loss-prevention-dlp (date of access: 04.11.2023).

11. DLP Systems: Models, Architecture and Algorithms. Share & Discover Presentations | SlideShare. URL: https://www.slideshare.net/liwei_ren/dlp-systems-models-architecture-and-algorithms (date of access: 05.11.2023).

12. Safetica ONE â Data loss prevention software | Safetica. Safetica | Data loss prevention (DLP). URL: https://www.safetica.com/products-safetica-one (date of access: 10.11.2023).

13. Data Loss Prevention Safetica ONE Product Overview. Malware Protection & Internet Security | ESET. URL: https://www.eset.com/fileadmin/ESET/INT/Products/Business/Safetica/Safetica_ONE_Product_Overview.pdf (date of access: 11.11.2023).

14. Safetica ONE Complete Documentation. HubSpot | Redirecting... URL: https://app.hubspot.com/documents/7097913/view/85697610?accessId=dc5c3b (date of access: 12.11.2023).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)