ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«Технології протидії витокам даних в організаціях на основі DLP Safetica ONE»

Виконав студент 6 курсу, групи БСЗМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Кукшин Д.В.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2022 року

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

Кукшин Дарії Вікторівни
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія протидії витокам даних на основі DLP Safetica ONE»

керівник магістерської роботи Марченко Віталій Вікторович,старший викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «12» жовтня 2022 року №122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

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

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Актуальність проблеми захисту кінцевих точок корпоративних інформаційних систем.
2. Склад та умови функціонування корпоративної інформаційної системи.
3. Методи та засоби управління захистом кінцевих точок.
4. Варіант топології системи управління захистом кінцевих точок корпоративної інформаційної системи.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

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

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

4. Результати аналізу методів та засобів протидії витокам даних.

5. Призначення та можливості рішення DLP Safetica ONE.

6. Варіант топології системи протидії витокам даних в організаціях на основі DLP Safetica ONE.

7. Рекомендації щодо застосування технології протидії витокам даних DLP Safetica ONE.

8. Висновки за результатами роботи.

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми протидії витокам даних в корпоративних інформаційних системах.	26.09.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	….. 2022 р.	
3.	Аналіз методів та засобів протидії витокам даних.	….. 2022 р.	
4.	Розроблення варіанту топології системи протидії витокам даних в організаціях на основі DLP Safetica ONE.	…..2022 р.	
5.	Розроблення рекомендацій щодо застосування технології протидії витокам даних DLP Safetica ONE.	…..2022 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	……2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент _____ Кукшин Д.В.
(підпис) прізвище та ініціали

Керівник магістерської роботи _____ Марченко В.В.
(підпис) прізвище та ініціали

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ

ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Кукшин Д.В. до захисту магістерської роботи
(прізвище та ініціали)

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

на тему: «Технології протидії витокам даних в організаціях на основі DLP Safetica ONE ».

Магістерська робота і рецензія додаються.

Директор інституту _____ _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Кукшин Д.В. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2021 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту _____ Бреславська Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студентка ***Кукшин Д.В.*** обрала тему роботи, метою якої було дослідити зміст технології протидії витокам даних в організаціях на основі DLP Safetica ONE та розробити варіант топології системи протидії витокам даних на підприємстві. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Кукшин Д.В. показала відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконувала сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану магістерську роботу студентки Кукшин Дарії Вікторівни на оцінку **«відмінно»** та присвоїти їй кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“____” _____ 2022 року

Висновок кафедри про магістерську роботу

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

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

РЕФЕРАТ

Текстова частина магістерської роботи: сторінки, рисунків, таблиці, джерел.

Об'єкт дослідження – процес протидії витокам даних в організаціях.

Предмет дослідження – технологія протидії витокам даних в організаціях.

Мета роботи – розробити варіант топології системи протидії витокам даних на основі DLP Safetica ONE та надати рекомендації щодо застосування даної технології в організаціях.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу протидії витокам даних.

В роботі проведено аналіз проблеми протидії витокам даних та визначено мету та завдання протидії витокам даних в організаціях. Проаналізовано існуючі технології протидії витокам даних.

Досліджено методи та засоби протидії витокам даних на прикладі рішення DLP Safetica ONE. Визначено призначення, основні функції та склад програмного комплексу DLP Safetica ONE. Надані рекомендації щодо впровадження та налаштування DLP Safetica ONE.

На основі досліджень проведених в роботі розроблено варіант топології системи протидії витокам даних та рекомендації щодо застосування технології протидії витокам даних на основі DLP Safetica ONE в організаціях.

Галузь використання – корпоративні інформаційні системи організацій.

ВИТОКИ ДАНИХ, КІБЕРБЕЗПЕКА, DLP - РІШЕННЯ, ВПРОВАДЖЕННЯ, ТЕХНОЛОГІЯ ПРОТИДІЇ ВИТОКАМ ДАНИХ

ABSTRACT

Master’s thesis: pages, figures, tables, sources.

Object of research –
Subject of research –
The aim of research –

Research methods –

Field of use –.

ВІДГУК РЕЦЕНЗЕНТА

на магістерську роботу

студентки Кукшин Дарії Вікторівни
на тему: «Технології протидії витокам даних в організаціях на основі DLP Safetica ONE»

Актуальність:
Протидіяти витокам даних стає все більш складним у зв'язку зі цифровізацією документообігу в організаціях. Витік даних є великою проблемою сучасних підприємств і вимагає використовувати сучасні засоби для запобіганням втратам інформації. Використання сучасних DLP-рішень може значно скоротити ризики витоку даних. Тому тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми витоку даних, визначено мета та завдання протидії витокам даних.
2. Досліджено методи та засоби протидії витокам даних на базі рішення DLP Safetica ONE.
3. Запропоновано варіант технології застосування протидії витокам даних на базі рішення DLP Safetica ONE та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У магістерській роботі бажано було б провести саме порівняльний аналіз DLP – рішень різних виробників.
2. Запропонований варіант протидії витокам даних на базі рішення DLP Safetica ONE доцільно було б показати на прикладі конкретного підприємства.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку «**відмінно»**, а студентка **Кукшин Дарія Вікторівна** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека..

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

Підпис рецензента (_____)

_____

ЗМІСТ

ВСТУП

Актуальність дослідження. Сучасний світ стає все більше цифро візованим, тому більшість інформації зберігається в електронному вигляді. Організації стараються повністю перейти на електронний документообіг. Хоча це і зручно для підприємств, але існує багато загроз і є ризики, що інформація може потрапити до зловмисників, які зможуть її використати проти самих власників інформації.

Протидія витокам даних є серйозною функцією системи безпеки організації. Витоки даних можуть завдати значних збитків. Тому сучасна компанія має використовувати спеціальні програмні засоби і правильно вміти їх інтегрувати в існуючі системи захисту. DLP –рішення допомагають налаштувати політики передачі інформації, щоб протидія витокам даних та унеможливити передачу даних сторонніми каналами.

Вищенаведені аргументи актуалізують тему даної магістерської роботи, зміст якої становлять дослідження щодо технології протидії витокам даних на прикладі DLP Safetica ONE.

Об'єкт дослідження – процес протидії витокам даних в організаціях.

Предмет дослідження – технологія протидії витокам даних в організаціях.

Мета роботи – розробити варіант топології системи протидії витокам даних на основі DLP Safetica ONE та надати рекомендації щодо застосування даної технології в організаціях.

Наукові завдання:

1. дослідити сутність проблеми протидії витокам даних;
2. встановити сутність завдань протидії витокам даних;
3. проаналізувати існуючі технології протидії витокам даних;
4. проаналізувати методи та засоби протидії витокам даних;
5. проаналізувати основні функції та принципи протидії витокам даних.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу протидії витокам даних.

Практичне значення одержаних результатів полягає в розробці варіанта топології системи протидії витокам даних на базі DLP Safetica ONE, а також у розробці рекомендацій щодо застосування технології протидії витокам даних на підприємстві.

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ВИТОКУ ІНФОРМАЦІЇ ТА ЗАСОБІВ ЗАХИСТУ

1.1 Витоки інформації

Досить швидко розвиваються інформаційні (цифрові) технології. Як і все цивілізоване суспільство, зокрема, компанії й люди «на повну» споживають блага такого розвитку. Усе частіше суспільство використовує у своїй життєдіяльності інформаційні технології. В Україні також почало швидко розвиватись електронний документообіг, а автоматизація окремих функцій і процесів управління персоналом сприяла економії ресурсів і часу. Однак широкомасштабне застосування інформаційних технологій пов’язане з додатковими ризиками й загрозами щодо захисту даних. Як наслідок, приватність стала «відкритою», а увагу періодично привертають інформаційні скандали, що й зумовлює зацікавленість у проблематиці захисту корпоративних даних.

Важливо розрізняти витік даних і злам даних. Ці терміни часто використовуються як синоніми, але вони мають одну помітну відмінність. Витік даних відбувається, коли внутрішнє джерело розкриває інформацію. Злам даних відбувається, коли зовнішнє джерело отримує доступ до системи під час кібератаки. Злочинці можуть використовувати різноманітні методи, щоб спробувати зламати мережу. Іншими словами, витік даних зазвичай є випадковим, тоді як злам є навмисним.

Іноді межа між витоком і зламом стирається, оскільки зловмисники використовують інформацію в результаті витоку даних, щоб розпочати масштабний атаку на організацію. Візьмемо, наприклад, витік пароля електронної пошти. Якщо один обліковий запис електронної пошти зламано, злочинець може використовувати цей обліковий запис для здійснення шахрайських дій[1].

Ключова річ, яку шукають кіберзлочинці, — це персональна інформація. Особиста інформація включає номери соціального страхування, номери кредитних карток та будь-яку іншу особисту інформацію. Зауважте, що не вся інформація, яка дозволяє ідентифікувати особу, є конфіденційною.

Іншою поширеною метою є медична або захищена інформація про здоров’я, як визначено в стандарті США HIPAA, «інформація, яка створюється постачальником медичних послуг і стосується минулого, теперішнього чи майбутнього фізичного чи психічного здоров’я або стану будь-якої людини».

Наступне, на що націлені кіберзлочинці, це інформація про клієнтів. Ці дані в різних компаніях можуть відрізнятися, але зазвичай є деякі загальні фактори:

•Інформація про особу: ім'я, адреса, номер телефону, адреса електронної пошти, ім'я користувача, пароль.

•Інформація про діяльність: історія замовлень і платежів, звички перегляду, деталі використання.

•Інформація про кредитні картки: номери карток, коди CVV, терміни дії, поштові індекси виставлення рахунків.

•Інформація, яка є специфічною для компанії, також може бути розкрита. Це можуть бути фінансові дані для банків та інвестиційних груп, медичні записи для лікарень і страхових компаній або конфіденційні документи та форми для державних установ.

Також, захисту потребує інформація про компанію:

•Внутрішня комунікація: записки, електронні листи та документи, що детально описують діяльність компанії.

•Метрики: статистика ефективності, прогнози та інші зібрані дані про компанію.

•Стратегія: деталі повідомлень, дорожні карти, rolodex та інша важлива бізнес-інформація.

Оприлюднення такого типу інформації може перешкодити проектам компанії, дати конкурентам зрозуміти бізнес-операції та розкрити внутрішню культуру та особистості. Чим більша компанія, тим більше інтересу до такого типу даних.

Комерційна таємниця - це найнебезпечніша річ, яку можна викрити під час витоку даних. Інформація, яка має вирішальне значення для вашого бізнесу та його здатності конкурувати. Комерційна таємниця включає:

•Плани, формули, проекти: інформація про існуючі або майбутні продукти та послуги.

•Код і програмне забезпечення: власна технологія, яку компанія продає або створює для внутрішнього використання.

•Комерційні методи: Ринкові стратегії та контакти.

Оголошення такого типу даних може знецінити продукти та послуги, які надає ваш бізнес, і звести нанівець роки досліджень[2].

Більшість витоків даних стаються через внутрішні проблеми організацій. Це обнадійлива новина, оскільки можливо налаштувати свою систему так, щоб дані не могли покидати межі корпоративних мереж. Щоб зрозуміти, чому відбувається витік даних, нам потрібно відійти назад і зрозуміти, як інформація генерується, маніпулюється та використовується. Сьогодні відомо, що існують величезні набори конфіденційних даних і компанії їх використовують. Коли ми розглядаємо інформаційну безпеку, стає зрозуміло, що організувати стійкий процес важко. Операційні прогалини, помилки процесу та низька обізнаність про кібербезпеку можуть призвести до виникнення вразливостей, що призводить до витоку даних.

Переваги та ризики цифрових даних однакові. Цифрові дані можна відтворити без погіршення якості. Організації мають багато копій виробничих даних, які включають: дані клієнтів, комерційну таємницю та іншу конфіденційну інформацію. Справа в тому, що існує багато копій даних, і чим більше існує копій даних, тим вище ймовірність того, що щось або хтось може їх випадково розкрити.

Наведемо деякі з найпоширеніших причин витоку даних[2].

Фішинг та соціальна інженерія

Фішингові та атаки за допомогою соціальної інженерії стали двома найбільш популярними способами проникнення хакерів у мережу та розповсюдження шкідливих програм та програм-вимагачів. Хоча технічно це зовнішні загрози, вони покладаються на співробітників, яких легко обдурити. Кіберзлочинці обманом змушують інсайдерів розкривати свої облікові дані або переходити за зараженими посиланнями чи вкладеннями. Це стає можливим завдяки тому, що

зловмисники видають себе за друзів чи інші надійні джерела. Опинившись усередині, вони можуть легко поставити під загрозу безпеку мережі.

Антивірусне програмне забезпечення може допомогти запобігти фішинговим атакам, виявляючи підозрілі електронні листи. А із соціальною інженерією найкраще справлятися за допомогою навчання з питань безпеки. Співробітники повинні бути поінформовані про те, як зовнішні зловмисники можуть наблизитись до них і як їм слід реагувати на отримання підозрілих запитів. Розуміння соціальної інженерії необхідне для запобігання такого роду атак. Знання та навички також слід перевірити, щоб виявити будь-які потенційні недоліки серед співробітників.

Обмін даними за межами компанії

Надання співробітниками конфіденційних даних компанії, таких як інтелектуальна власність або конфіденційна інформація, захищена відповідно до законів про захист даних, за межами компанії, може призвести до катастрофи. Зазвичай це відбувається через неуважність: замість простої відповіді натискається кнопка «Відповісти всім», інформація надсилається не на ту адресу електронної пошти або щось випадково публікується у відкритому доступі. Часто працівники зловживають можливістю використовувати різні месенджери і надсилають конфіденційну інформацію, адже для них це простіше і швидше.

Навчання такого роду інцидентів рідко допомагає, оскільки вони є людськими помилками, до яких ми всі схильні. Спеціалізоване програмне забезпечення, таке як інструменти запобігання втрати даних (DLP), може допомогти організаціям відстежувати конфіденційні дані та гарантувати, що їх передача електронною поштою або іншими інтернет-сервісами обмежена або повністю заблокована. Деякі рішення DLP, такі як Endpoint Protector, пропонують можливість налаштування різних дозволів та політик безпеки залежно від відділу працівника та робочого часу.

Тіньове IT

IT-відділу часто важко відстежити використання неавторизованого стороннього програмного забезпечення, додатків або інтернет-сервісів на

робочому місці, звідси і термін «тіньове IT». Причини поширеності тіньового IT досить прості: співробітники використовують відомі програми для таких речей, як обмін файлами та обмін повідомленнями за звичкою, тому що вони підвищують їх ефективність та полегшують їхнє робоче навантаження або є більш зручними для користувача, ніж альтернативи, дозволені компанією.

Це проблематично, тому що компанії більшу частину часу не знають, що це відбувається, по суті, створюючи сліпу пляму у стратегіях кібербезпеки. Ще однією небезпекою є потенційна вразливість цих сторонніх сервісів, яка може призвести до витоку даних або порушень безпеки.

Тіньове IT зазвичай сигналізують про нездатність компанії надати співробітникам потрібні інструменти для виконання їхніх завдань. Організації повинні вести відкритий діалог зі своїми співробітниками, щоб зрозуміти їхні технологічні потреби та зробити все можливе для їхнього задоволення. Інструменти DLP також можуть допомогти компаніям запобігти завантаженню співробітниками конфіденційної інформації на ці неавторизовані служби.

Використання неавторизованих пристроїв

Багато політик захисту даних зосереджено на передачі даних за межі мережі компанії через Інтернет і не враховують інший часто використовуваний метод: портативні пристрої. Зокрема, USB-накопичувачі тривалий час були прокляттям для стратегій захисту даних. Легко втратити або вкрасти, але зручно використовувати, USB-накопичувачі призвели до деяких катастрофічних витоків даних, таких як сумнозвісний інцидент з безпекою в аеропорту Heathrow, коли необережний співробітник втратив USB-накопичувач з більш ніж 1000 конфіденційних файлів, включаючи особливо важливу інформацію безпеки та особисту інформацію.

Найпростіший спосіб запобігти таким порушенням – повністю заблокувати доступ співробітників до USB-портів і периферійних портів. Проте не можна заперечувати корисність USB на робочому місці. Для компаній, які все ще хочуть використовувати USB, є заходи безпеки, які можуть бути реалізовані для усунення цих загроз кібербезпеці. Головним із них є примусове шифрування всіх файлів, що

передаються на USB-накопичувачі, у поєднанні з політикою довірених пристроїв, що дозволяє лише довіреним пристроям підключатися до комп'ютера компанії.

Фізична крадіжка пристроїв компанії

У сьогоднішньому все більш мобільному робочому середовищі співробітники часто виносять свої робочі комп'ютери та портативні пристрої з офісу. Незалежно від того, чи працюєте ви віддалено, відвідуєте клієнтів або відвідуєте галузеві заходи, робочі пристрої часто виходять за межі безпеки корпоративних мереж і стають вразливішими як для фізичної крадіжки, так і для зовнішнього втручання.

Шифрування завжди є хорошим рішенням для захисту від фізичної крадіжки. Будь то ноутбуки, мобільні телефони або USB-накопичувачі, шифрування виключає можливість того, що будь-хто, хто їх вкраде, зможе отримати доступ до інформації на них. Увімкнення параметрів віддаленого очищення також може допомогти організаціям видалити всі дані з викрадених пристроїв на відстані[3].

За даними Cybint, 95% витоків даних спричинені помилками людини, тобто їм, ймовірно, можна було запобігти. Розглянемо такий сценарій:

Вашій маркетинговій команді потрібно перемістити ваш список електронних адрес від одного постачальника послуг електронної пошти до іншого, і вони збережуть дані у невикористаному сегменті S3, поки вони виберуть новий інструмент. Після того, як інструмент буде визначено, контакти завантажуються в новий інструмент, і все гаразд. За винятком того, що команда маркетингу забула очистити сегмент S3, і він налаштований на повний публічний доступ.

Це може здатися людським фактором, і це так. Проблема не в тому, що хтось зробив помилку, проблема в тому, що нічого не було, щоб запобігти помилці або принаймні виявити її, щоб її можна було негайно виправити.

Ви можете подумати, що це не велика проблема, це лише електронні листи, але що, якщо це був ваш список клієнтів або, що ще гірше, особиста інформація вашого клієнта? Навіть адреси електронної пошти є великою справою та можуть призвести до незаперечної шкоди репутації. Стійкість має бути вбудованою в процедурну роботу, яка виконується день у день.

Головне, що слід розуміти, це те, що витоки даних можна використати. Ось

чотири поширені способи використання витоку даних:

•Шахрайство з кредитними картками: кіберзлочинці можуть використовувати інформацію про кредитну картку для шахрайства.

•Продажі на чорному ринку: коли дані оприлюднені, їх можна буде продати на аукціоні в темній мережі. Багато кіберзлочинців спеціалізуються на пошуку незахищених хмарних інстанцій і вразливих баз даних, які містять номери кредитних карток, номери соціального страхування та іншу особисту інформацію, щоб продати їх для шахрайства. Це може бути так само просто, як використання пошукових запитів у Google.

•Вимагання: іноді інформація зберігається над головою компанії з метою отримання викупу або завдати шкоди репутації.

•Зменшення конкурентних переваг: конкуренти можуть скористатися витоком даних. Усе, від ваших списків клієнтів до комерційних секретів, надає вашим конкурентам доступ до ваших ресурсів і стратегії. Це може будь-яка інформація, як наприклад, над чим працює ваша маркетингова команда, або складні логістичні операції[2].

Звіт IBM показує, що дані з кожним роком набувають все більшої ваги, та відповідно їх витоки коштують компаніям все більше і більше. В середньому ціна витока даних по всьому світу дорівнює $4,24 млн (рис. 1.1).

•38% - частка втрат бізнесу у загальних витратах пов'язаних із витоком даних.

•$180 - ціна одного запису, що містить персонально ідентифіковану інформацію.

•287 днів в середньому потрібно для виявлення та локалізації витоку даних.

•На 80% скорочуються витрати від витоку даних після впровадження AI та автоматизації безпеки.

•Гібридні IT-інфраструктури скорочують втрати від витоку даних у середньому на $1,19 млн.

•Середні витрати на витік даних у 2022 році становлять 4,35 мільйона доларів, що на 2,6% більше, ніж у 2021 році (4,24 мільйона доларів)[4].

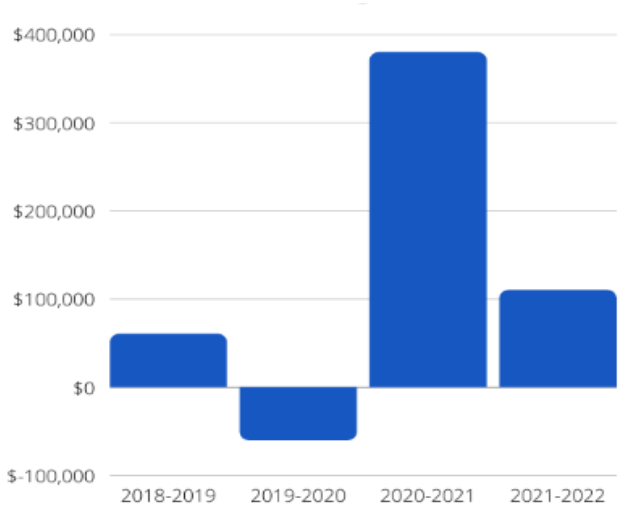

Рис.1.1. Схема порівняння витрат на витоки даних

Топ-5 найдорожчих векторів атак на витік даних у 2021 році (рис.1.2):

•Компрометація бізнес-електронної пошти – 4,89 млн доларів (порівняно з 5,01 млн доларів у 2021 році).

•Фішинг – $4,91 млн (порівняно з $4,65 млн у 2021 році).

•Зловмисні інсайдери – $4,18 млн (порівняно з $4,61 млн у 2021 році).

•Злочинні атаки соціальної інженерії – $4,10 млн (порівняно з $4,47 млн у 2021 році).

•Уразливості в сторонньому програмному забезпеченні – $4,55 млн (порівняно з $4,33 млн у 2021 році)[5].

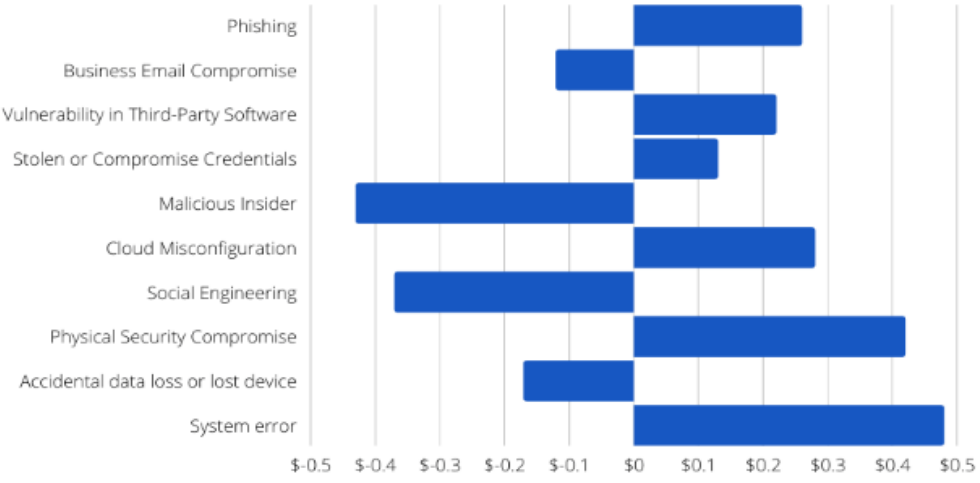

Рис.1.2. Вектори атак на витік даних у 2021 році

Три приклади витоку даних, які завдали величезної шкоди:

•Приблизно 6,2 мільйона адрес електронної пошти було виявлено Комітетом кампанії Демократичної партії в Сенаті в неправильно налаштованому ядрі зберігання Amazon S3. Список адрес, розділених комами, був завантажений в 2010 році співробітником DSCC. І в сегменті, і в назві файлу є посилання на «Клінтон», імовірно, пов'язане з однією з попередніх кандидатур Гілларі Клінтон на посаду сенатора від Нью-Йорка. Список містив адреси електронної пошти від основних провайдерів електронної пошти, а також університетів, державних установ і військових.

•Дослідник UpGuard виявив три загальнодоступні сегменти Amazon S3, пов'язані з Attunity. З них один містив велику колекцію внутрішніх ділових документів. Загальний розмір невідомий, але дослідник завантажив зразок розміром близько терабайта, включаючи 750 гігабайт стиснених резервних копій електронної пошти. Також були присутні резервні копії облікових записів співробітників OneDrive, які охоплювали широкий спектр інформації, необхідної співробітникам для виконання роботи: листування електронною поштою, системні паролі, контактну інформацію відділу продажів і маркетингу, специфікації проекту тощо.

•Хмарне сховище, що містить інформацію, що належить LocalBlox, службі пошуку особистих і бізнес-даних, було залишено загальнодоступним, розкриваючи 48 мільйонів записів із детальною особистою інформацією про десятки мільйонів людей, зібраних і зібраних із багатьох джерел[5].

Більшість витоків даних викликані операційними проблемами, включаючи технічні та людські помилки. Запобігання витокам даних починається з багаторівневого підходу до кібербезпеки та поваги до конфіденційності даних. Хоча служба безпеки в організації повинна забезпечити надійну систему захисту, вони також повинні запровадити план реагування на інциденти, щоб швидко відновитися.

Найкращі методи запобігання втраті даних

1. Навчайте своїх співробітників

Один із найефективніших передових методів запобігання втраті даних починається з навчання ваших співробітників усьому, що їм слід і чого не слід робити під час роботи з цінними даними вашої організації. Навчання співробітників має включати безпечні методи передачі, перегляду та зберігання даних. Для досягнення максимального ефекту тренінги повинні спонсоруватися на рівні виконавчої влади та повторюватися через регулярні проміжки часу, щоб закріпити та оновити найкращу практику поведінки.

2. Встановіть політику обробки даних

Ключовий компонент найкращих практик DLP, політики обробки даних включають:

- Де можна зберігати дані.
- Як передавати дані.
- Хто може переглядати певні типи даних.
- Які типи даних вам дозволено зберігати і тд.

Оскільки ці політики керують всіма правилами поведінки та оцінкою обробки даних, їх слід встановити якнайшвидше. Їх також слід регулярно оновлювати, щоб відобразити зміни в організації та нормативних актах. Після того, як політика обробки даних буде введена, ви можете перейти до інших технічних заходів, щоб ваші дані залишалися там, де вони повинні бути.

3. Створіть систему класифікації даних

Ключ до створення політики запобігання втраті даних – почати з системи класифікації даних. Загальні класифікації включають особисту інформацію, фінансову інформацію, загальнодоступні дані, інтелектуальну власність і тд. Для кожної класифікації можна встановити унікальний набір протоколів захисту.

4. Відстежуйте конфіденційні дані

Успішний захист даних вимагає можливості відстежувати конфіденційні дані. Програмне забезпечення для запобігання втраті даних зазвичай містить можливості для моніторингу всіх аспектів використання та зберігання даних, зокрема:

- доступ користувача;

- доступ до пристрою;
- доступ до програми;
- типи загроз;
- географічне положення;
- час доступу;
- контекст даних.

У рамках процесу моніторингу програмне забезпечення DLP надсилає сповіщення групі реагування, коли дані використовуються, переміщуються, видаляються чи змінюються несанкціонованим чином.

5. Налаштуйте різні рівні авторизації та доступу

Ця практика поруч з класифікацією даних, оскільки поєднання цих двох налаштувань дає змогу надавати доступ до даних лише тим, хто має дозвіл на цю інформацію. Ваше програмне забезпечення DLP також має включати певні політики захисту даних із нульовою довірою, які за своєю суттю не надають довіри жодному користувачу, водночас постійно перевіряючи особистість і дозвіл.

6. Використовуйте супутні інструменти DLP

DLP не живе у вакуумі. Вся концепція DLP спирається на екосистему інструментів, які працюють разом, щоб надати статистику, плани дій і активний захист ваших даних. Ці інструменти включають захищені веб-шлюзи, доступ до хмари, захист електронної пошти та інфраструктури[6].

1.2 Що таке DLP?

DLP-система – це система запобігання витоку даних або запобігання втрат, яка попереджує втрату або просочування конфіденційних даних. Система DLP розроблена в основному для захисту від самих співробітників компанії, законних користувачів, які вже мають доступ до більшості внутрішніх систем і даних. Користувачам дозволяють минати більшу частину захисту системи, для того, щоб вони могли ефективно виконувати свою роботу. Персонал можливо не хоче

навмисно шкодити компанії, але й бувають випадки, коли робітники витягують інформацію в корисливих цілях. Впровадження DLP системи на підприємстві - результативна відповідь на виклики сучасної кіберзлочинності. Система з'ясовує, які фрагменти інформації важливіші за інші, створюючи список пріоритетів і пропонуючи комплексний набір методології і технології, які можуть забезпечити перегляд більшого обсягу інформації за різними напрямками, на відміну від локальних індивідуальних запитів.

Фундаментальні основи системи захисту даних у світлі функціонування сучасного підприємства вимагають знань про те, що це таке системи DLP. У загальному вигляді вони представляють набір інструментів і процесів, що забезпечують цілісність конфіденційної інформації, щоб дані використовувалися виключно за призначенням і не були доступними неавторизованим користувачам (рис.1.3).

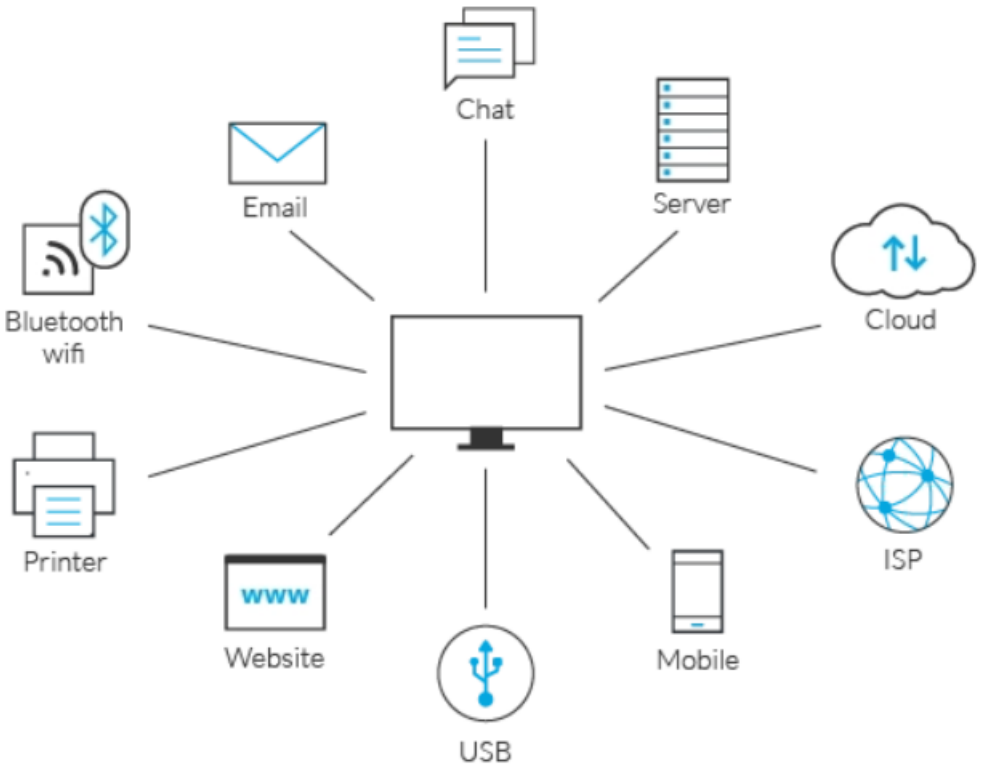

Рис.1.3. Запобігання втраті даних з різних джерел[10]

Програмне забезпечення DLP класифікує регульовані, конфіденційні та важливі для бізнесу дані і виявляє порушення політик, визначених компанією в

рамках встановленого пакету захисту, відповідно до нормативних вимог до DLP систем: HIPAA, PCI-DSS або GDPR. Після виявлення цих порушень, DLP виконує виправлення за допомогою попереджень, шифрування та інших захисних дій, щоб запобігти випадковому або зловмисному обміну даними.

Програмне забезпечення та інструменти для запобігання втрати інформації відстежують і контролюють дії кінцевих точок, фільтрують потоки в корпоративних мережах і у хмарі для захисту даних. DLP також надає звіти для відповідності нормативним вимогам і аудиту, виявляючи слабкі місця і аномалії для криміналістики, з метою реагування на інциденти. Для того щоб виконати впровадження DLP систем потрібно складати і ретельно виконувати плани розгортання системи[7].

Існує кілька методів безпеки DLP, які реалізуються за допомогою передових практик і програмних засобів. Найкращі стратегії запобігання втраті даних включають різноманітні підходи для охоплення всіх потенційних векторів порушення.

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.

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[8].

Існує три види DLP:

Мережеві DLP: відстежують та захищають всі дані, які використовуються, перебувають у стані спокою або знаходяться в мережі компанії, включаючи хмару

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

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

Мережеві DLP

Відстежують та аналізують мережеву активність і трафік організації в мережі та хмарі. Включаючи моніторинг електронної пошти, обміну повідомленнями та передачі файлів, щоб виявити, коли критично важливі для бізнесу дані надсилаються з порушенням політики інформаційної безпеки організації Створюють базу даних, яка записує, чутливі та конфіденційні дані, хто має до них доступ і, якщо це можливо, куди дані переміщуються в мережі Забезпечують команді інформаційної безпеки повну видимість усіх даних у мережі

Endpoint DLP

Відстежують 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. Допомагають в класифікації нормативних, конфіденційних, приватних або важливих для бізнесу даних, щоб упорядкувати звітність і відповідність вимогам. Відстежують дані, що зберігаються на кінцевих

точках як у мережі, так і поза нею.

Cloud DLP

Сканують та перевіряють дані в хмарі, щоб автоматично виявляти та шифрувати конфіденційну інформацію перед тим, як вона буде прийнята та збережена в хмарі. Зберігають список авторизованих хмарних програм і користувачів, які мають доступ до конфіденційних даних. Попереджають команду інформаційної безпеки про порушення правил або аномальну активність. Ведуть журнали доступу до конфіденційних хмарних даних та ідентифікацію користувача.

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[9].

Система DLP – це набір правил, які також називаються політиками і є принципом або протоколом для керівництва рішеннями і досягнення раціональних результатів. Ці політики встановлюються адміністратором і містять правила для мережі та кінцевих точок, повідомляють що дозволено, а що ні. Ці правила можуть бути встановлені на певній програмі або веб-сторінці. Також можуть бути встановлені різні правила в залежності від рівня доступу користувача. Чим

конкретніше ці політики встановлюються, тим менше помилково позитивні та помилково негативні сигнали будуть видаватися системою DLP, що зробить систему більш точною. Існує декілька дій, які може виконувати система DLP, тобто те, що система DLP повинна робити з певним типом файлу або вмістом. Це може бути блокування, відправлення в карантин або пропускання, це залежить від політики, встановленої адміністратором. Система може також реєструвати події з інформацією про те, хто це зробив, коли це сталося і які дії були вжиті.

Враховуючи складність ландшафту загроз і розгалужену природу більшості корпоративних мереж, першим кроком у впровадженні політики DLP часто є визначення надійного та здатного партнера з кібербезпеки. Спеціальна команда досвідчених спеціалістів у сфері безпеки матиме вирішальне значення для надання допомоги бізнесу на кожному етапі програми, від стратегії та проектування до реалізації та експлуатації.

Нижче наведено найкращі методи, які допоможуть компаніям максимізувати свої інвестиції в DLP і забезпечити відповідність рішення існуючій стратегії та заходам безпеки компанії.

1. Визначте основну мету DLP

Для багатьох організацій застосовується рішення DLP, щоб компанія могла відповідати складним стандартам відповідності, що розвиваються, таким як HIPAA або GDPR. Незважаючи на те, що це одна з важливих функцій DLP, комплексне рішення забезпечує багато інших застосувань для організації, включаючи захист даних, запобігання інцидентам, покращену видимість і можливості швидкого реагування на інциденти.

2. Переконайтеся, що DLP узгоджується з архітектурою та стратегією безпеки організації

При впровадженні рішення DLP важливо, щоб організація врахувала існуючі заходи безпеки, такі як брандмауери або системи моніторингу, які можна використовувати як частину цієї нової можливості. Організація також повинна переконатися, що рішення DLP повністю інтегровано в архітектуру кібербезпеки компанії.

3. Класифікуйте дані

Щоб компанії краще захищали свою конфіденційну інформацію, вони повинні точно знати, що вони мають. Як найкраща практика, компанії повинні проводити аудит даних та інвентаризацію, щоб легше класифікувати та визначати пріоритети цих даних. Завдяки цьому вони краще розуміють, які дані завдадуть більшої шкоди, якщо їх зламано.

4. Розробіть плани впровадження будь-яких нових інструментів у рамках рішення DLP

У цих планах повинні бути задіяні як групи IT, так і групи інформаційної безпеки, щоб переконатися, що зацікавлені сторони обізнані про призначення інструменту та його використання. Цей процес планування також має визначити операційний вплив інструменту на бізнес.

5. Запровадьте регулярну перевірку безпеки для рішення DLP

Нові можливості, можливості та функції часто додаються до рішень регулярно. Ваші команди повинні оцінювати, тестувати та впроваджувати плани розгортання, коли нові можливості виходять на ринок. «Встановити та забути» — це рецепт невдачі, оскільки загрози, тактика та методи змінюються швидше, ніж більшість інструментів можуть адаптуватися.

6. Встановіть керівні принципи управління змінами

Узгоджену конфігурацію інструменту слід документувати, а потім перевіряти кілька разів на рік. Команди інформаційної безпеки повинні часто обговорювати конфігурації та нові функції з постачальниками та групами підтримки, щоб максимізувати цінність інструменту та підтвердити його використання в середовищі організації.

7. Перевіряйте себе

Регулярні аудити та вправи з емуляції супротивника повинні гарантувати, що рішення DLP працює належним чином[9].

Кожна система DLP сьогодні відрізняється тим, як вони підходять до проблеми витоку даних, але багато важливих частин залишаються схожими. Більшість систем DLP мають заздалегідь визначені словники вмісту, які містять

такі слова, як "Конфіденційно", "Секретний", "Номер кредитної картки / Інформація" тощо. Вони також йдуть зі словниками з шаблонами номерів кредитних карток для різних виробників, таких як Visa, Master Card, American express. Система DLP сканує файли, які потрібно передати, і якщо є номери, що відповідають будь-якому з цих шаблонів, це буде позначено як номер кредитної картки. Як згадувалося, залежно від політики, встановленої для такого типу події, система DLP виконуватиме визначену дію.

Системи DLP не забезпечують повної безпеки для даних в інфраструктурі. Жодна з систем не дає захисту від витоків інформації на 100%. Наявність DLP не обов'язково має вплив на зменшення потенційної загрози, але може обмежити вплив атаки. Велике значення в роботі систем DLP відіграє людський фактор. Часто відбуваються витоки даних через неправильне використання системи або через відсутність розуміння класифікації – що конфіденційне, а що - ні.

1.3 Safetica ONE

В даній роботі я буду використовувати DLP-рішення Safetica ONE. На прикладі даного програмного забезпечення я покажу, як інтегрувати DLP в структуру організації та які модулі можна використовувати для захисту від витоків даних.

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[11].

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.1.4).

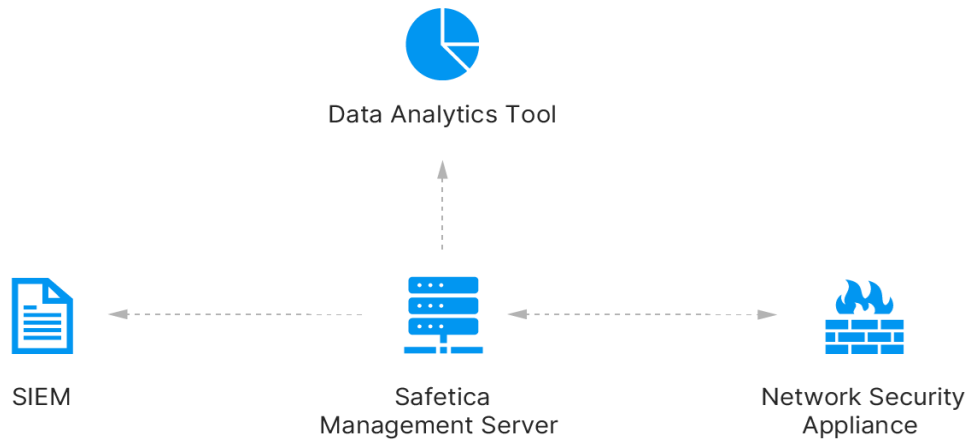

Рис.1.4. Схема надсилання звітів Safetica

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.1.5).

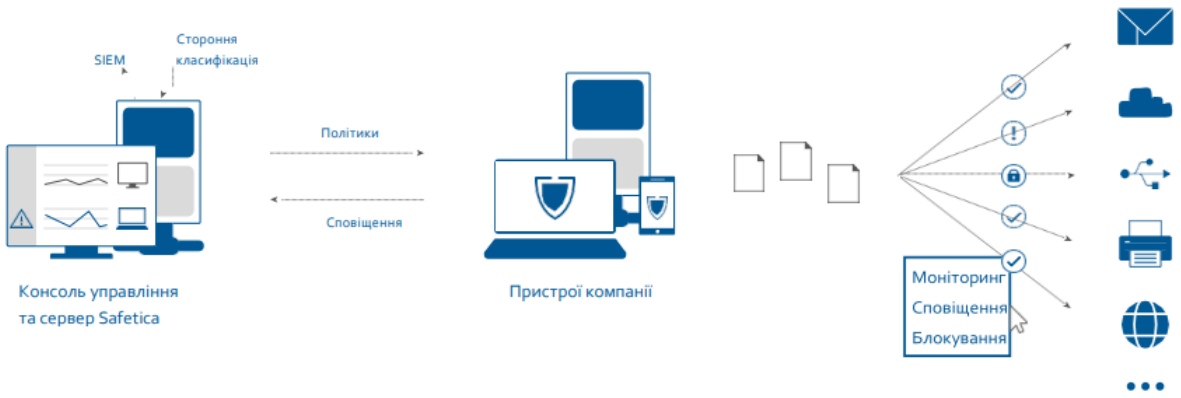

Рис.1.5. Схема роботи Safetica

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.1.6).

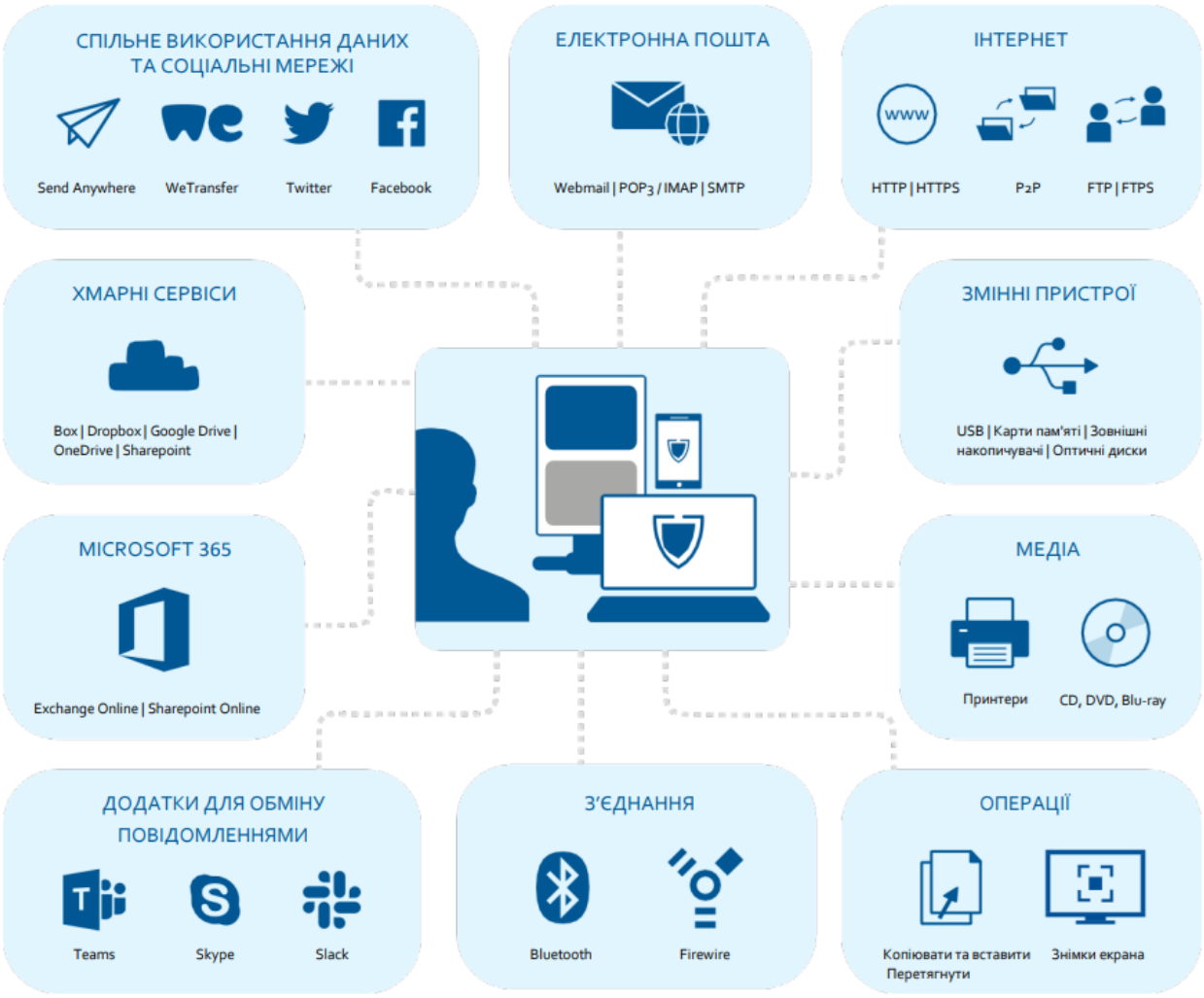

Рис.1.6. Канали переміщення інформації, з якими працює Safetica

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[12].

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.

Висновок

Отже, проблема з витоком даних стоїть дуже жорстко в корпоративному середовищі, адже може призвести до непоправних наслідків. Цифровізація організацій змогла спростити методи управління. Проте з’явилися нові виклики, з якими потрібно бути постійно насторожі. В свою чергу DLP-рішення зможуть закрити прогалину, якою можуть скористатися зловмисники, для витоку конфіденційних даних з організації. Грамотно побудована система з використанням DLP Safetica зможе допомогти різним компаніям зберегти свої дані та репутацію.

2 ВИМОГИ ДО ПРОГРАМНОГО ТА АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ ТА ГНУЧКЕ НАЛАШТУВАННЯ

2.1 Вимоги до програмного та апаратного забезпечення

DLP- рішення Safetica досить просто та зручно можна інтегрувати у власну систему безпеки на підприємстві. Для цього не потрібно наймати команду професіоналів чи проходити спеціальні курси. Проте для інтеграції потрібно підготувати інфраструктуру, щоб встановлення продукту пройшло легко і без помилок. Тому потрібно розглянути з яких компонентів складається DLP Safetica та рекомендації для апаратного та програмного забезпечення.

Продукти Safetica, засновані на архітектурі клієнт-сервер. На робочих станціях клієнт Safetica працює з сервером. Разом з клієнтом завантажений агент працює на робочих станціях, призначених для встановлення, оновлення та управління іншими клієнтськими компонентами. Для управління, налаштування та відображення отриманих даних використовується консоль управління Safetica або WebSafetica. Дані, отримані з окремих робочих станцій, зберігаються на сервері баз даних. База даних також зберігає налаштування для всіх компонентів Safetica.

Safetica Сервер Safetica працює як сервіс на виділеному сервері, забезпечує зв'язок між базою даних та іншими компонентами Safetica, а також забезпечує віддалене управління ними. Рекомендовані вимоги до програмного та апаратного забезпечення (табл.2.1):

- Чотирьохядерний процесор 2,4 ГГц.
- 8 ГБ та більше оперативної пам'яті.
- 100 ГБ вільного дискового простору.
- Спільний або виділений сервер, підтримка віртуальних машин і хмарного хостингу.
- Необхідне підключення до сервера з MS SQL 2012 та вище або Azure SQL.

Таблиця 2.1.

Рекомендовані вимоги до програмного та апаратного забезпечення серверу

Кількість ПК	Up to 200	Up to 500	Up to 2000
Процесор	Quad-core	8-core	8-core
RAM	8GB	16GB	32GB
Жорсткий диск	100GB free disk space	250GB free disk space	500GB free disk space
Операційна система	Windows Server 2012 or newer with IIS 7.5 and .NET 4.5.2 or newer		
База даних	MS SQL Server 2012 or newer (including MS SQL Express editions); MS SQL Server 2016 recommended / AzureSQL S1 or S2	MS SQL Server 2012 or newer; MS SQL Server 2016 recommended / AzureSQL S2 or S3	MS SQL Server 2012 or newer; MS SQL Server 2016 recommended / AzureSQL S4, S6 or P1

Safetica Management Console

Консоль використовується для налаштування та управління сервісом (сервером) Safetica, базою даних, клієнтами Safetica та агентами на робочих станціях. Вона також використовується для налаштування всіх функцій Safetica на робочих станціях. Консоль відображає отримані дані, статистику та графіки. Може запускатися будь-де, якщо передбачено підключення до керованого сервера.

WebSafetica — це вебконсоль для управління рішенням Safetica та відображення записів, отриманих з робочих станцій. Вона частково дублює і доповнює консоль адміністратора та будучи сайтом доступна у вашій локальній мережі організації і націлена більше на керівництво та менеджерів та як відображає інформацію аналізу поведінки користувачів.

База даних містить дані про активність робочих станцій та журнали безпеки.

Перед інсталяцією потрібно виконати наступні дії:

1. Перевірити, чи задовольняються вимоги до програмного та апаратного

забезпечення всіх компонентів Safetica.

2. Проаналізувати корпоративну мережу:

o Вирішити, на яких ПК ви потрібно встановити сервер. Рекомендуємо звернути увагу на те, що:

- ПК з сервером Safetica повинен мати можливість підключення до сервера SQL, на якому будуть зберігатися основні бази даних.
- Залежно від кількості підключених SEC та типу сервера баз даних, оберіть, скільки серверів ви бажаєте встановити. Кількість SEC, які можуть підключатися до одного сервера, обмежена базою даних SQL, яку сервер використовує для зберігання даних.

o Вирішити, на яких ПК потрібно встановити консоль у вашій мережі. ПК з консолью повинен мати можливість підключення до всіх серверів, якими можна управляти, використовуючи консоль адміністрування.

o Вирішити, на яких ПК потрібно встановити агент. ПК з агентом повинен мати можливість підключення до сервера.

o Вирішити, на яких ПК потрібно встановити клієнт Safetica. Рекомендуємо звернути увагу на те, що:

- Для кожного клієнта Safetica потрібно визначити, до якого сервера його буде підключено. Не всі комп'ютери будуть підключені до всіх ПК з сервером.
- ПК з клієнтом повинен мати можливість підключення до певного сервера.

o Виділити і позначити SQL-сервери, на яких будуть зберігатися центральні бази даних окремого сервера. Кожен сервер потребує трьох призначених баз даних на сервері SQL: одну для налаштувань, одну для записів та одну для бази даних категорій.

3. Перед інсталяцією різних компонентів Safetica (сервер, консоль, клієнт), переконатися, що вони не будуть блокуватися брандмауером або антивірусним програмним забезпеченням.

o Додати винятки для вхідних підключень до процесу STAService. exe та

наступні порти на ПК, на яких буде встановлено сервер:

- 4438 (клієнт зв'язку -> сервер, база даних).
- 4441, 4442 (консоль зв'язку -> сервер).

o Додати виключення для процесу STAConsole.exe на ПК, на яких буде встановлюватися консоль.

o Встановити винятки для наступних процесів на ПК, на яких буде встановлено клієнт: STCService.exe, STUserApp.exe, Safetica.exe, вихідні та вхідні з'єднання.

- Встановити винятки для порту 1433 (порт за замовчуванням для підключення до бази даних) на ПК, куди будуть встановлені бази даних
- WebSafetica використовує вебсервер Microsoft IIS та доступний на портах 80 та 443. Переконатися, що на комп'ютері не запущено програми, які б блокували порти 80 та 443, або налаштували різні порти IIS після встановлення.

4.Завантажити універсальний інсталятор з останньою версією Safetica[13].

2.2 Автоматична інсталяція

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

• Автоматичну інсталяцію (інсталяцію Safetica) – 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[13].

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. Переконайтеся, що комп'ютер має достатню обчислювальну потужність для роботи з базою даних, сервером, а також WebSafetica.

Після запуску універсального інсталятора Safetica виконайте наступні дії:

1. Оберіть мову інсталятора (рис.2.1).

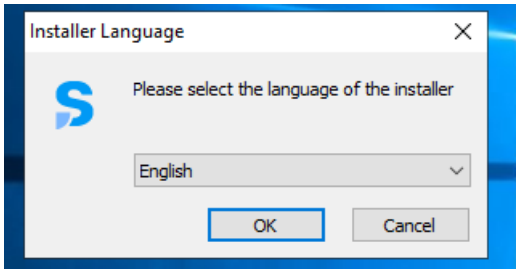

Рис. 2.1. Вікно вибору мови інсталятора

2. Натисніть кнопку «Автоматична інсталяція» (рис.2.2).

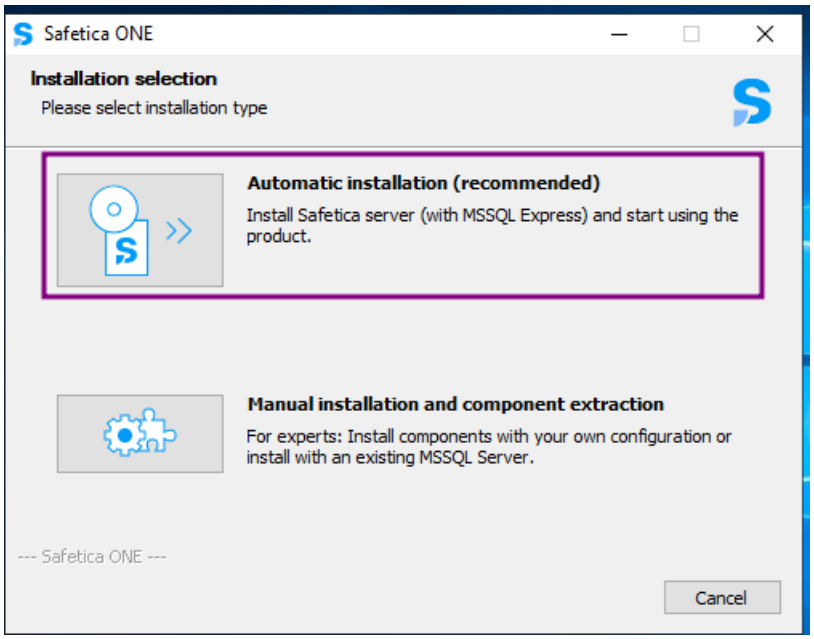

Рис. 2.2. Вікно вибору Автоматичної інсталяції

3. Натисніть «Далі», щоб підтвердити, що обране середовище відповідає вимогам до апаратного забезпечення (рис.2.3).

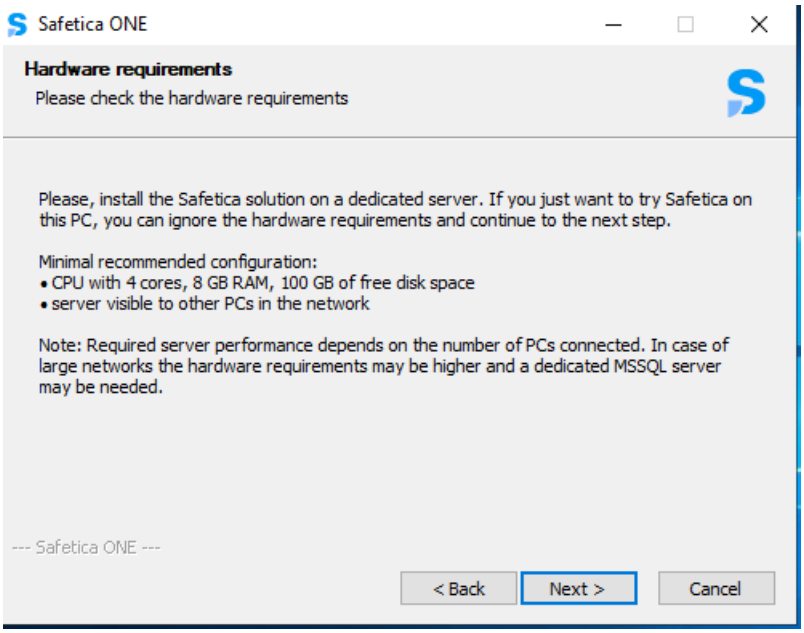

Рис. 2.3. Вимоги апаратного забезпечення

4. Введіть надійний пароль для облікового запису адміністратора. За замовчуванням пароль safetica. Підтвердіть умови ліцензійної угоди на сервері SQL і запустіть інсталяцію, натиснувши кнопку «Інсталювати» (Install) (рис.2.4 – 2.8).

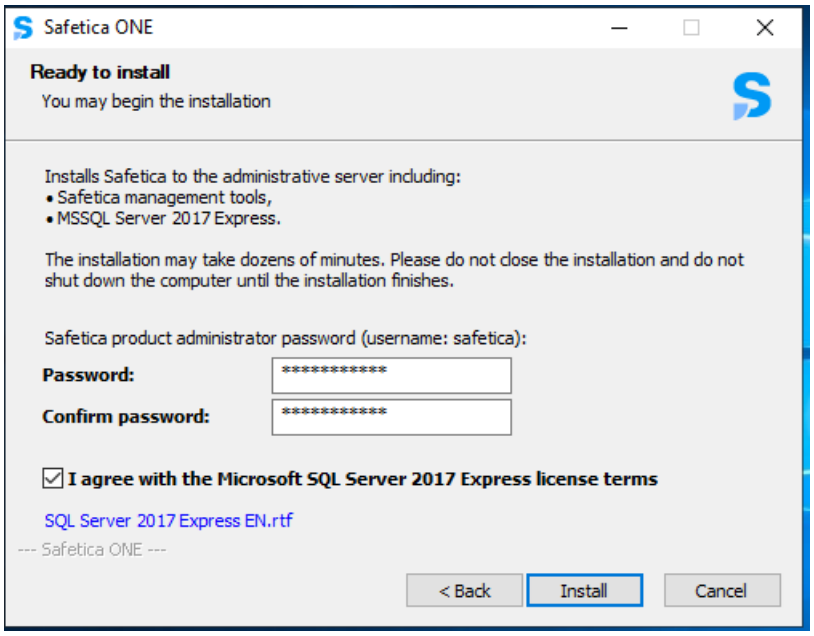

Рис. 2.4. Вікно створення паролю адміністратора

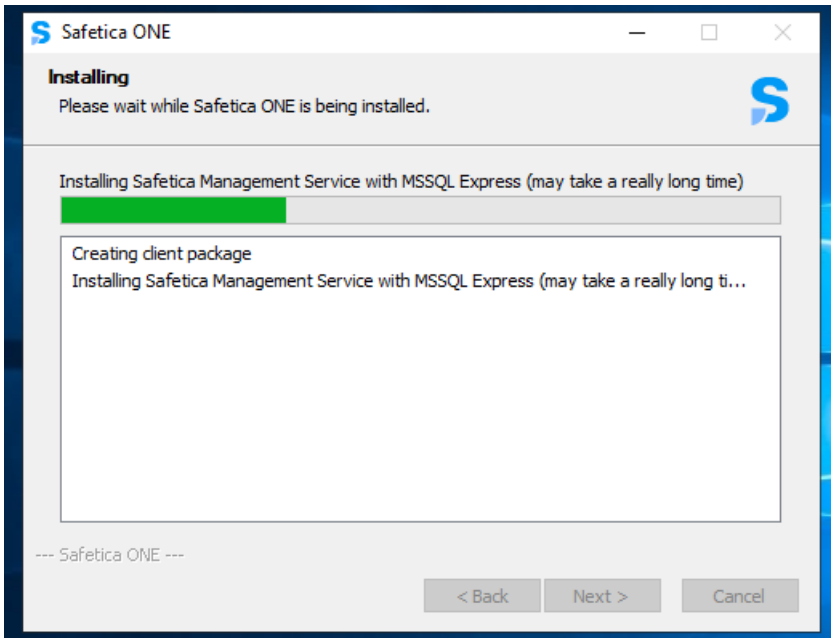

Рис. 2.5. Вікно встановлення Safetica Management Service

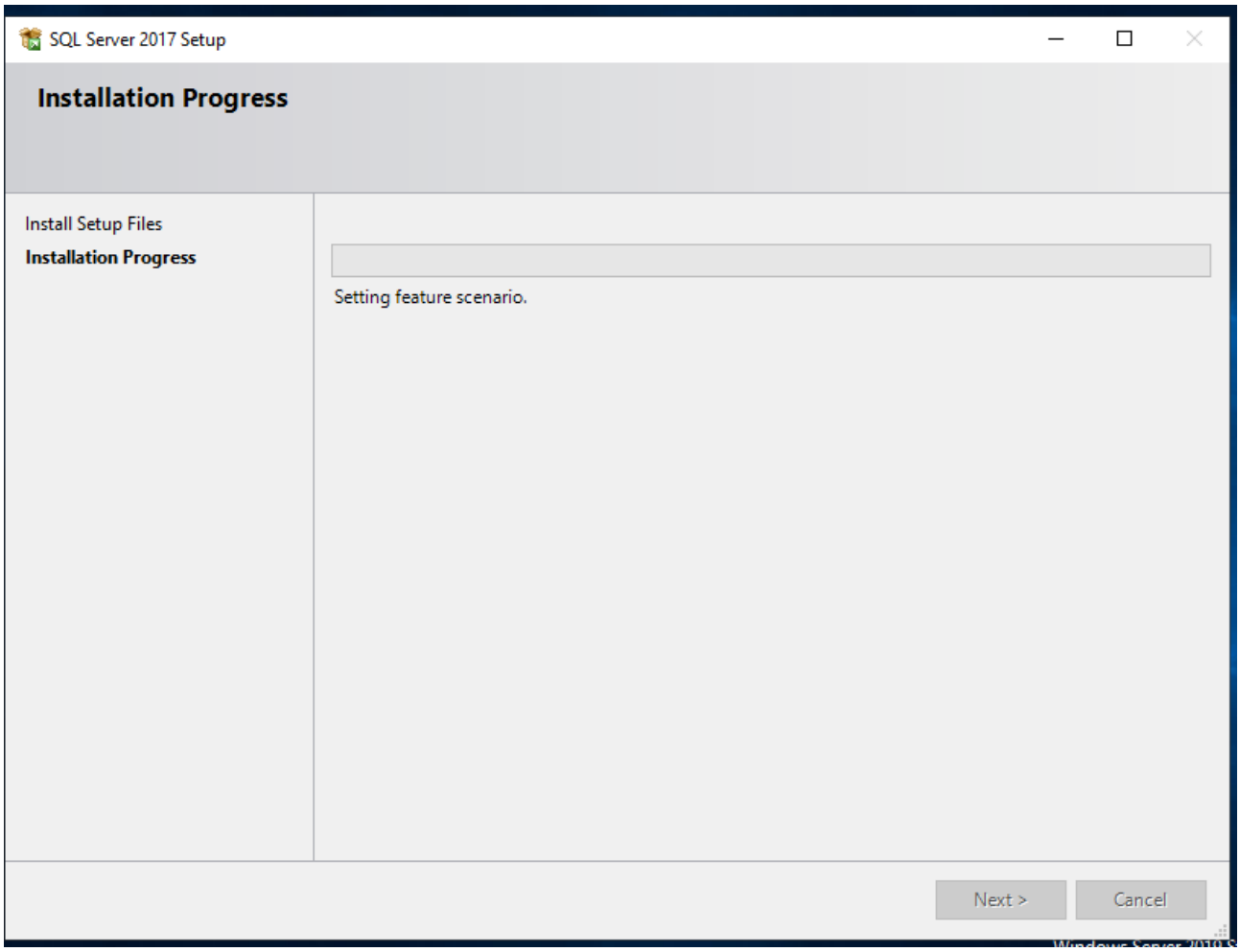

Рис. 2.6. Вікно встановлення SQL Server 2017

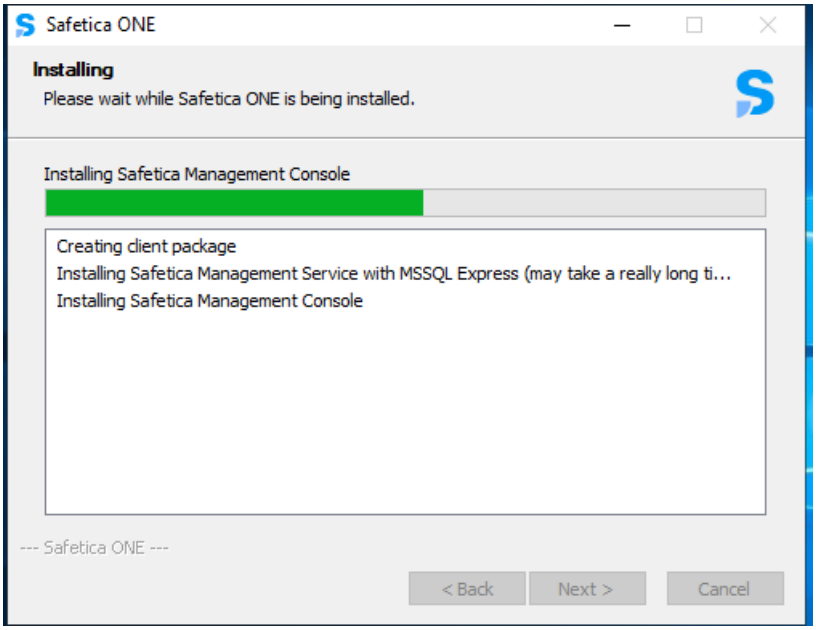

Рис. 2.7. Вікно встановлення Safetica Management Console

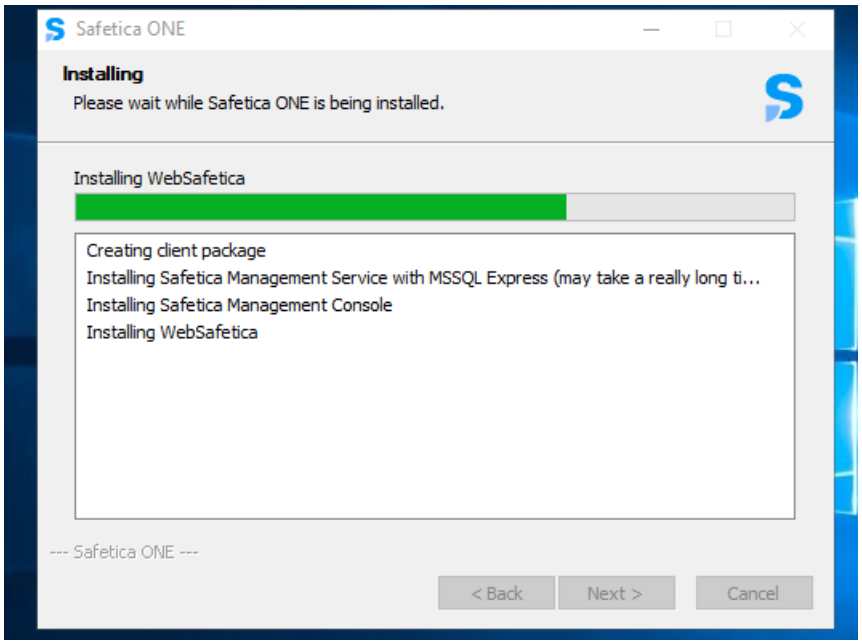

Рис. 2.8. Вікно встановлення WebSafetica

5. Щоб підтвердити успішну інсталяцію серверної частини потрібно натиснути «ОК» (рис.2.9).

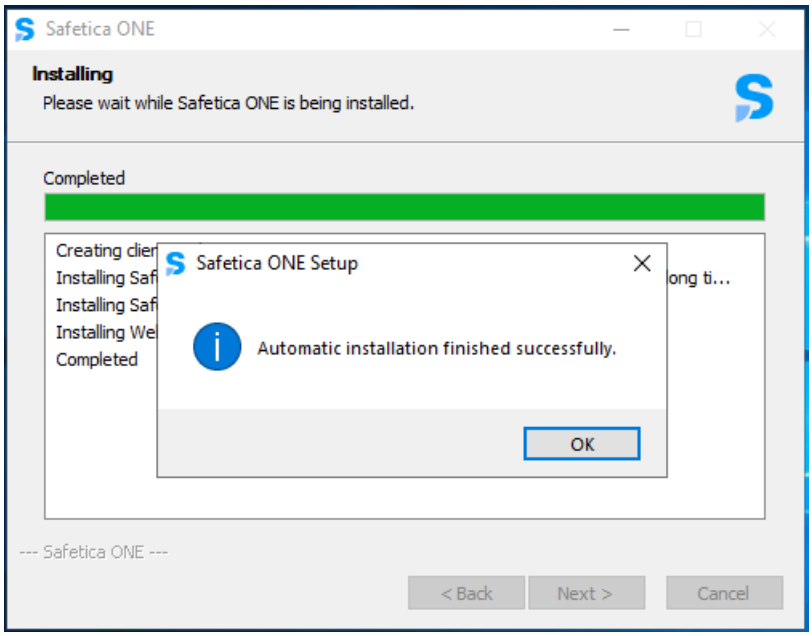

Рис. 2.9. Вікно підтвердження інсталяції

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.2.10).

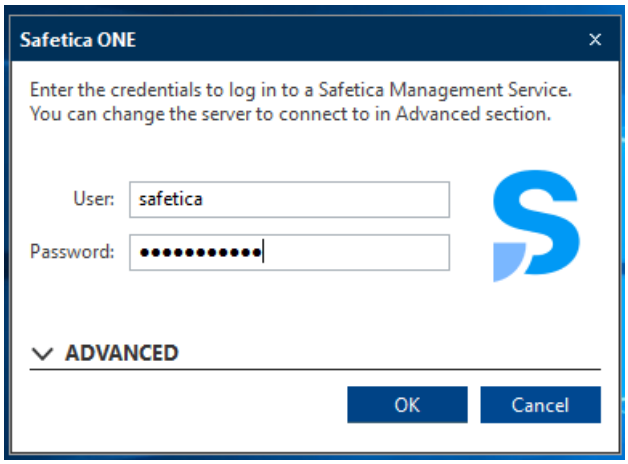

Рис. 2.10. Вікно входу в консоль управління

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.2.11).

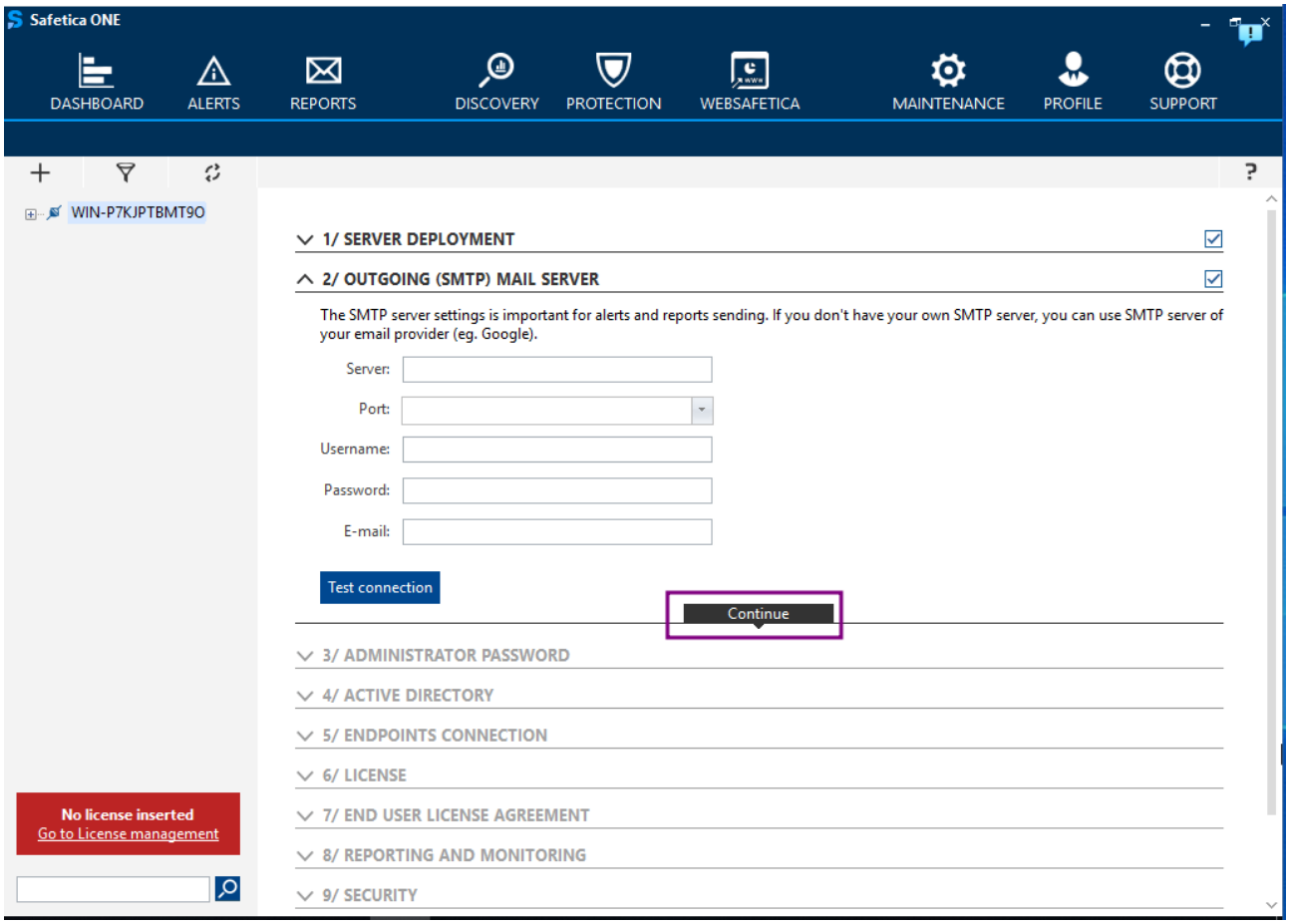

Рис. 2.11. Вікно налаштування підключення до поштового серверу

8. Під час наступного етапу можна імпортувати структуру Active Directory в компанії. Це можливо, якщо комп'ютер з сервером Safetica в домені (рис.2.12).

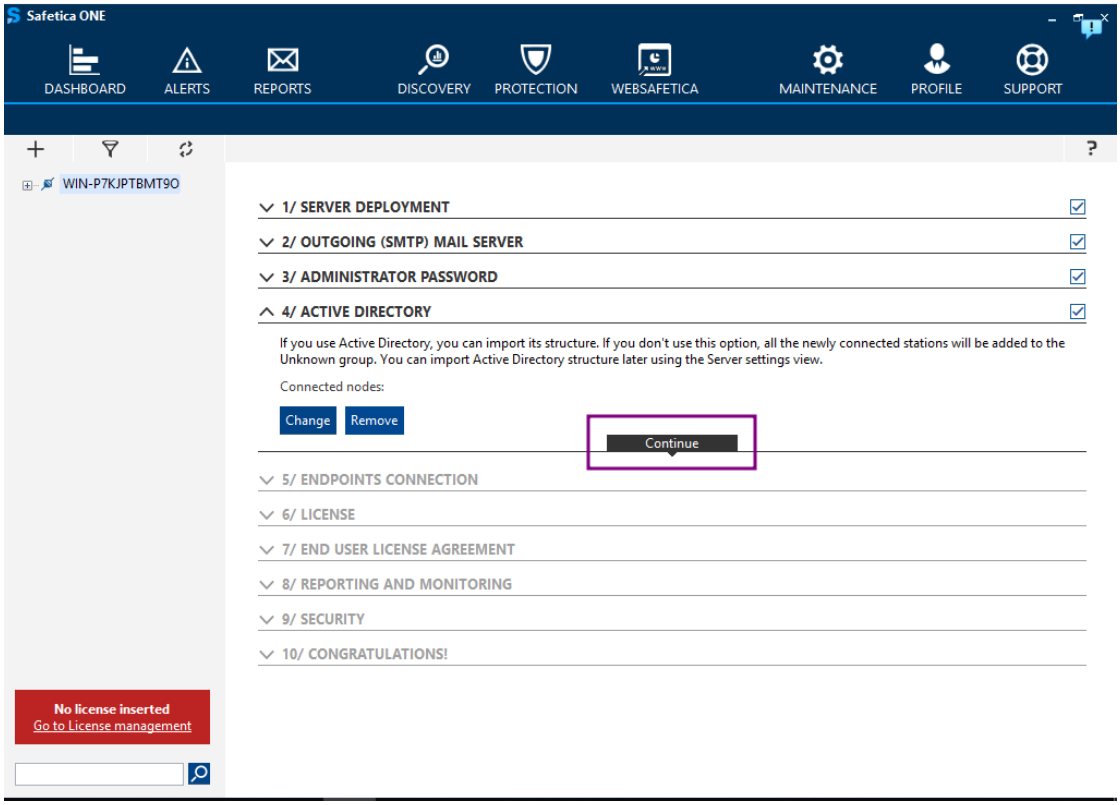

Рис. 2.12. Вікно налаштування підключення до Active Directory

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.2.13).

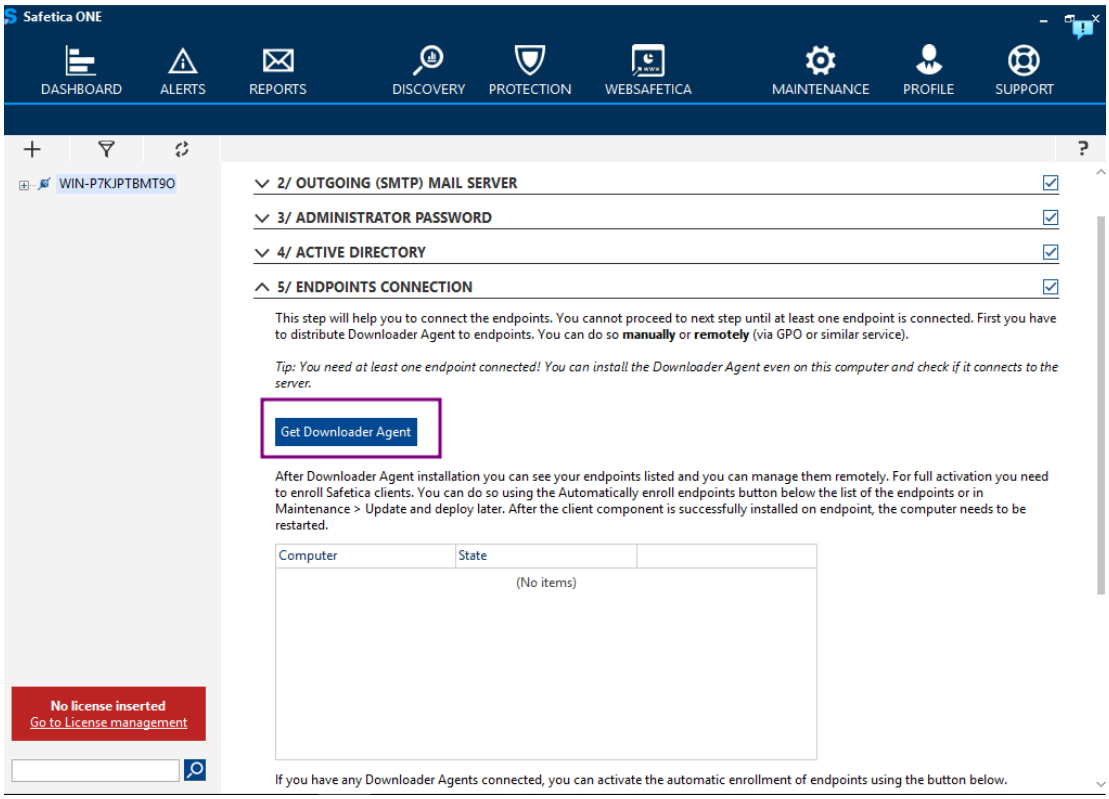

Рис. 2.13. Вікно для завантаження агента

10. Обираємо, куди завантажити інсталятор агента та натискаємо «Save» (рис.2.14 та рис.2.15).

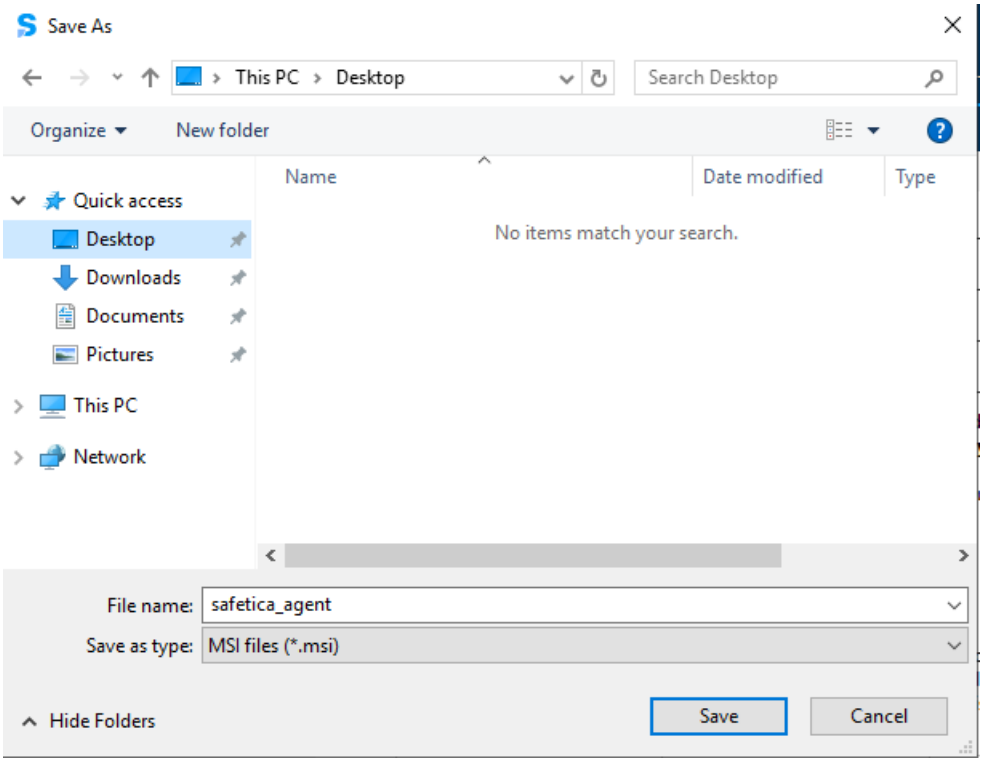

Рис. 2.14. Вікно вибору шляху завантаження

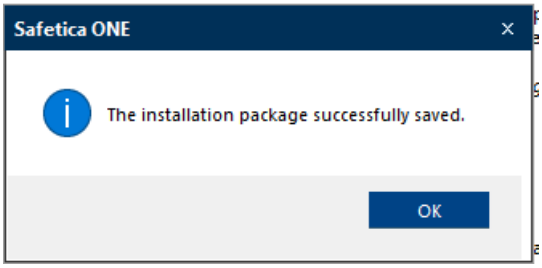

Рис. 2.15. Вікно успішного завантаження інсталятора агентам

11. Далі потрібно ввести ліцензійний ключ (рис.2.16).

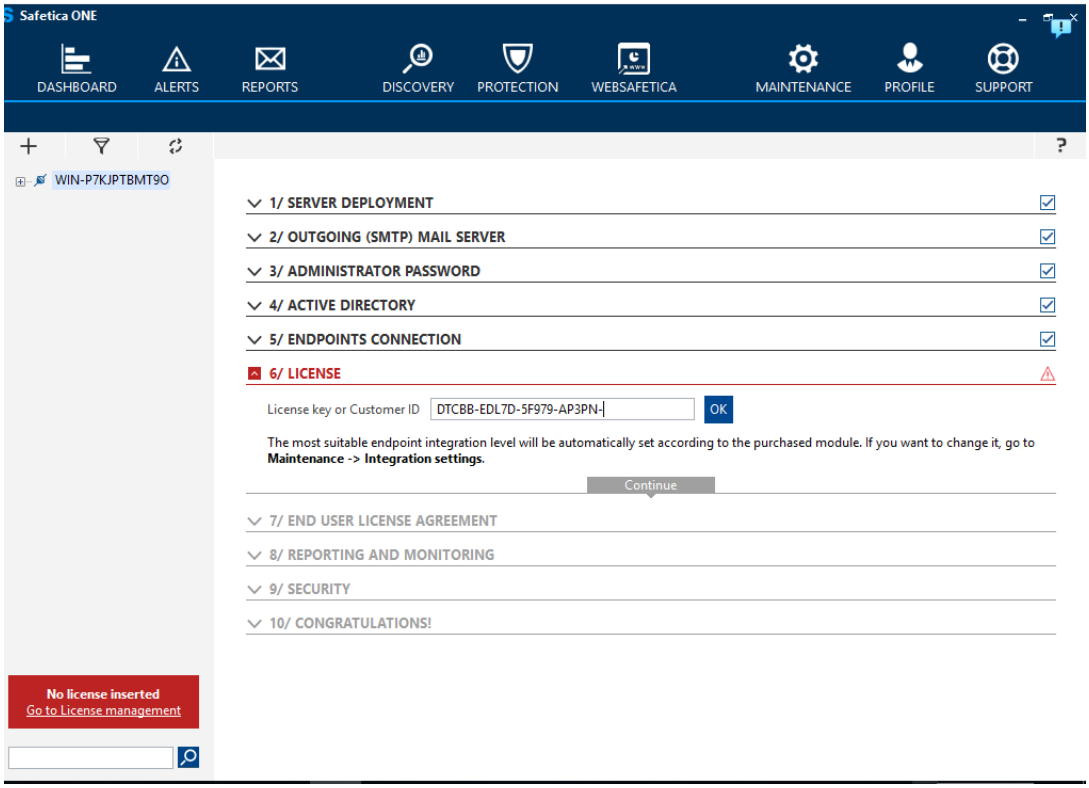

Рис. 2.16. Вікно вводу ліцензійного ключа

12. Вводимо дані адміністратора системи та погоджуємося з Safetica EULA (рис.2.17).

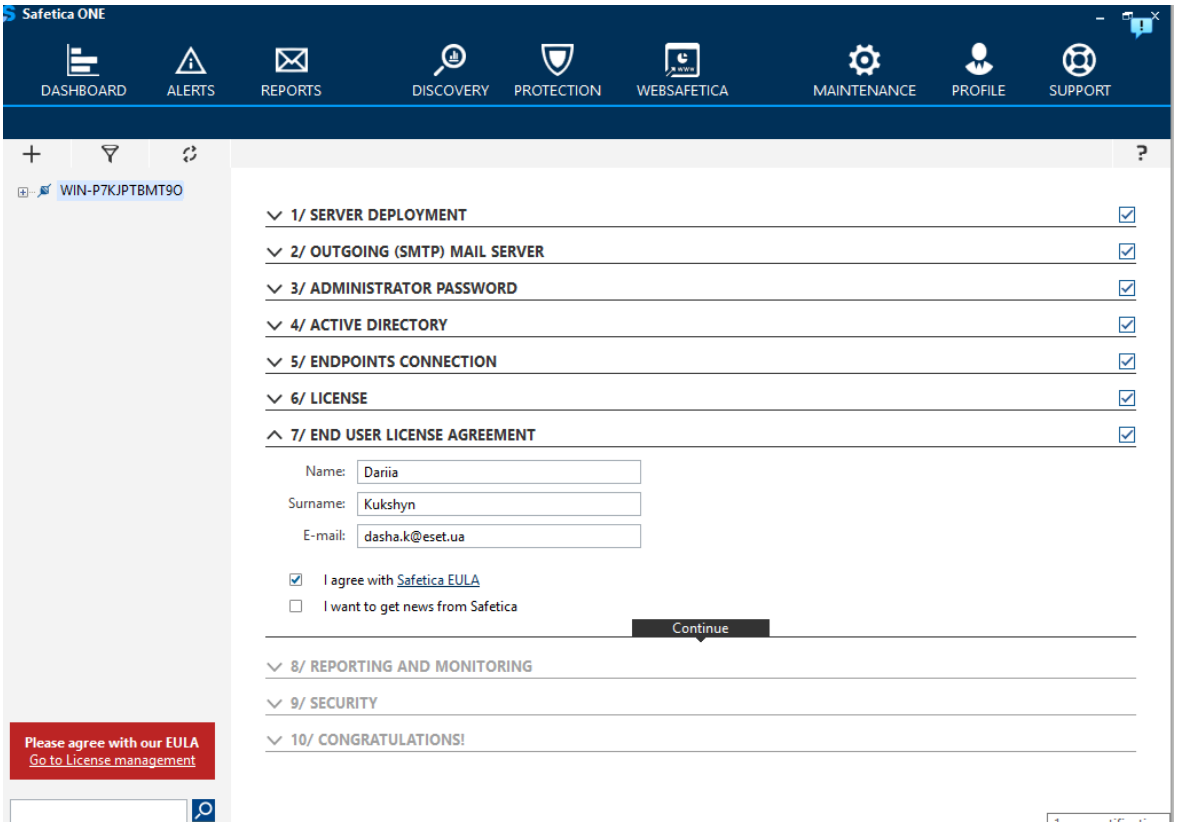

Рис. 2.17. Вікно вводу даних адміністратора

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.2.18).

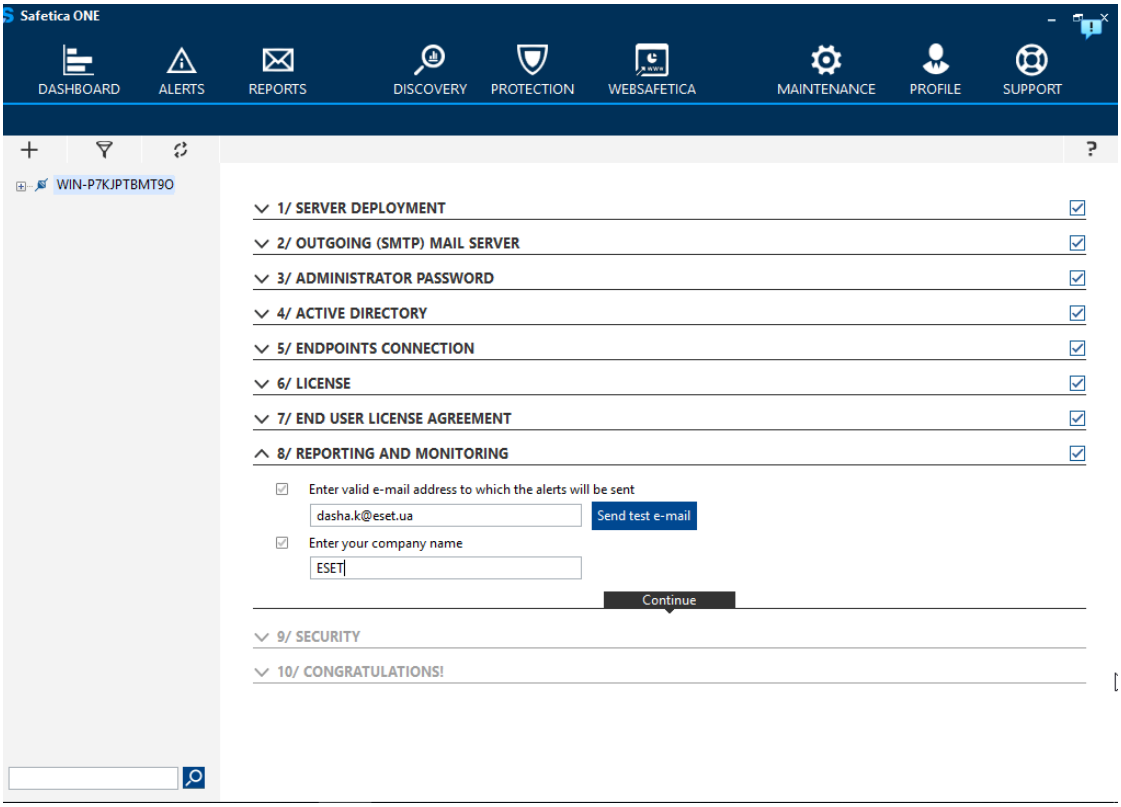

Рис. 2.18. Вікно для вводу назви компанії

14. Всі налаштування введені коректно і можна починати захист даних (рис.2.19).

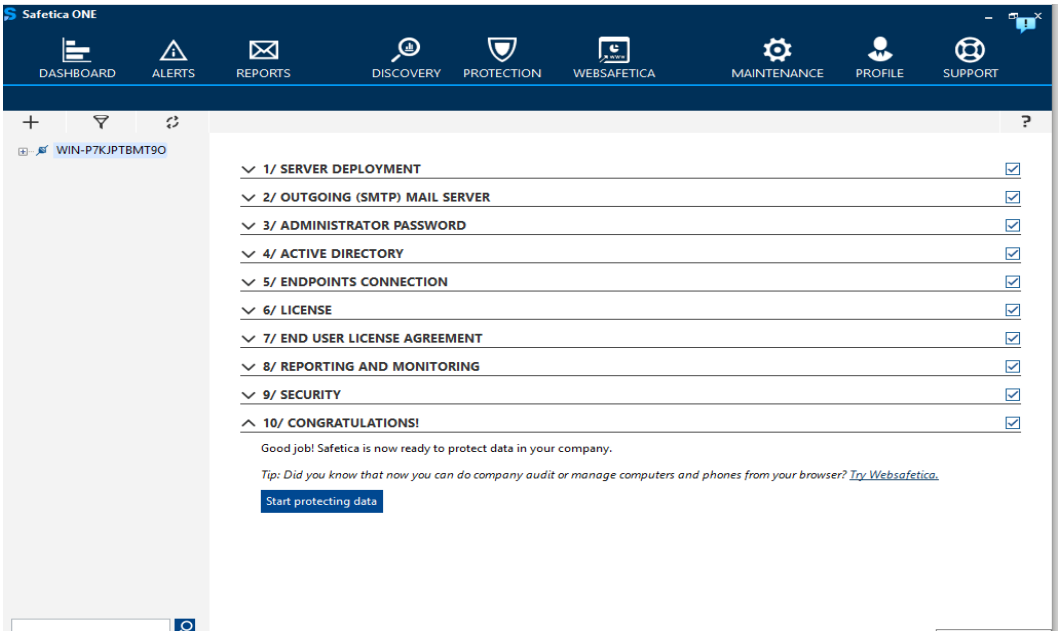

Рис. 2.19. Вікно підтвердження успішного налаштування системи

2.3 Встановлення та налаштування Safetica агент та Safetica клієнт

Переходимо до налаштування клієнтської частини DLP Safetica. Вона складається з агента та клієнта.

Агент - це компонент Safetica, який використовується для управління клієнтом Safetica на робочих станціях. Він дозволяє здійснювати віддалену інсталяцію, встановлювати оновлення та інші завдання управління.

Safetica клієнт забезпечує всі функції захисту та моніторингу Safetica на робочих станціях. Сервіс клієнта завжди запускається під час запуску системи та забезпечує моніторинг, дотримання DLP-політик, а також полегшує зв'язок з базою даних та сервером. Під час встановлення клієнта Safetica компонент агента буде інстальовано автоматично, якщо його не було інстальовано раніше.

Safetica клієнт продовжує працювати, навіть якщо сервер недоступний (наприклад, сервер не працює або клієнт знаходиться в іншій мережі). Він використовує локальну зашифровану та захищену базу даних, де зберігає всі налаштування та журнали, поки не буде знову підключений до сервера[13].

Рекомендовані вимоги до програмного та апаратного забезпечення

Safetica клієнт для Windows:

- Чотирьохядерний процесор 2,4 ГГц.
- 2 ГБ та більше оперативної пам'яті.
- 10 ГБ вільного дискового простору.
- MS Windows 7, 8.1, 10 (32-біт [x86] або 64-біт [x64]).
- Інсталяційний пакет MSI.
- .NET 4.7.2 та вище.

Safetica клієнт для macOS:

- Чотирьохядерний процесор 2,4 ГГц.
- 2 ГБ та більше оперативної пам'яті.
- 10 ГБ вільного дискового простору.
- macOS 10.10 та вище.

Для коректної інсталяції спочатку потрібно встановити агент на клієнтській

машині. Завантажений пакет інсталяції переносило на ПК і запускаємо. Процес інсталяції агента досить швидкий і не потребує зусиль і часу (рис.2.20).

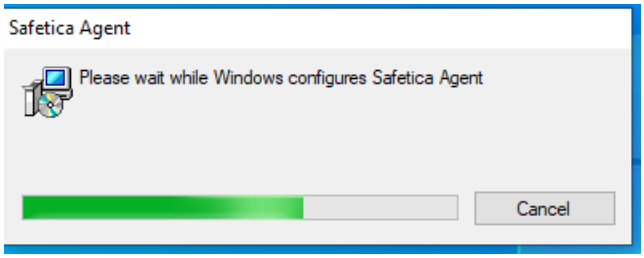

Рис. 2.20. Вікно інсталяції агента

Safetica клієнт є останнім та суттєвим компонентом продукту Safetica, який потрібно інсталювати. На комп'ютерах клієнтів він забезпечує виконання DLP-політик та гарантує, що всі функції, налаштовані в консолі, виконуються належним чином. Для користувачів він також може надавати набір інструментів безпеки для використання.

Інсталювати клієнт можна віддалено за допомогою консолі управління. Для цього потрібно створити відповідне завдання. Заходимо в консоль і обираємо розділ Maintenance – Update and deploy. Далі обираємо «Встановити клієнта на кінцевих точках» (рис.2.21).

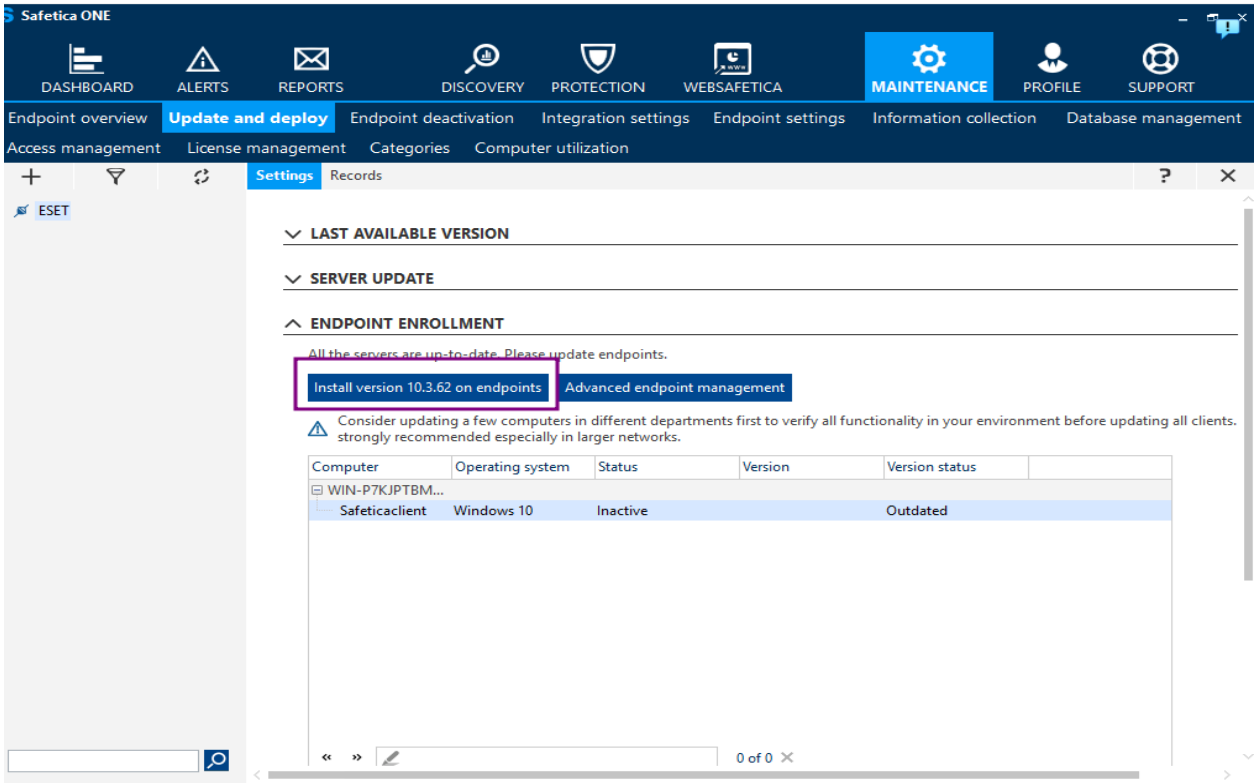

Рис. 2.21. Вікно створення задачі інсталяції клієнта

Ви можете перевірити успішність встановлення з консолі, де ви знайдете синій значок у дереві користувачів з назвою робочої станції (рис.2.22).

Рис. 2.22. Значок коректної роботи клієнта Safetica

2.4 Розгляд функцій Safetica Managent Console

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.2.23):

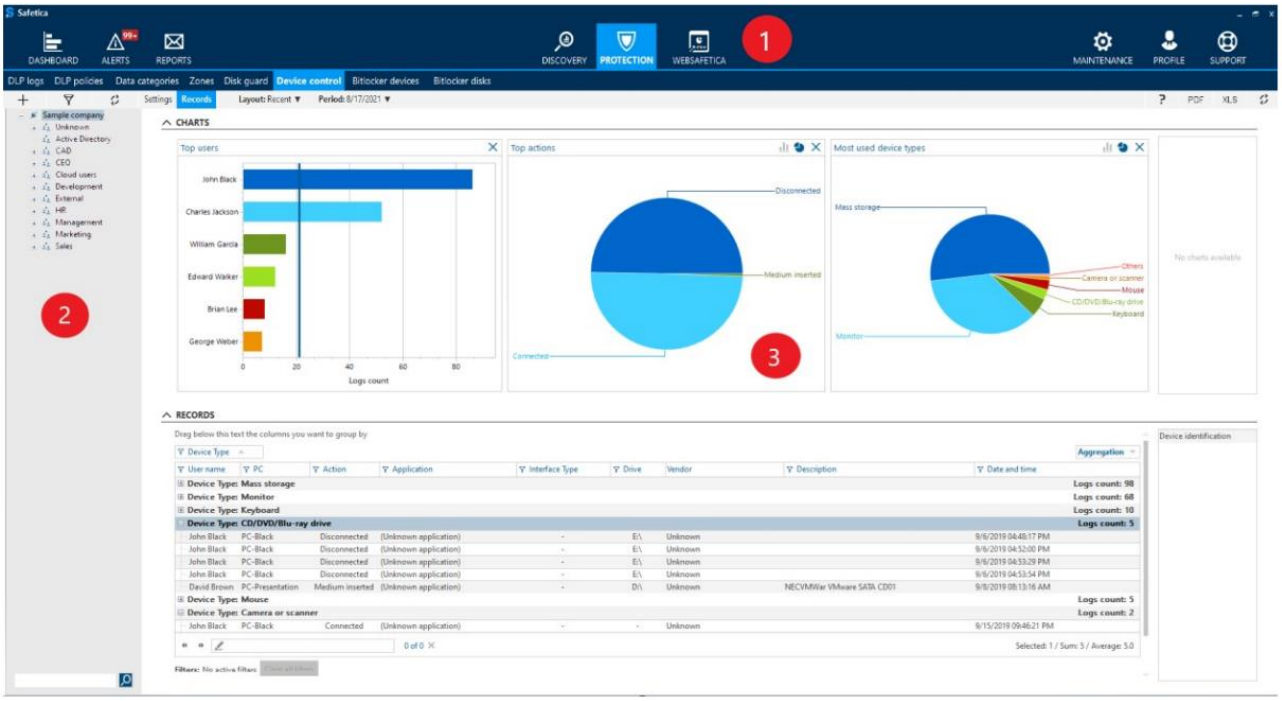

Рис. 2.23. Інтерфейс консолі управління

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[13].

Висновок

Отже, DLP-рішення Safetica захищає данні від витоку. Для налаштування роботи для початку необхідно розібратися, як її інтегрувати в існуючу систему. Тому починати потрібно з вивчення рекомендацій щодо апаратного та системного забезпечення. Правильна інтеграція допоможе коректно налаштувати всі компоненти системи так, щоб було зручно працювати з ними. Розгортання DLP Safetica не займає багато часу та зусиль, що є її перевагою. Але незважаючи на це, її компоненти можуть працювати злагоджено для подальшого контролю витоків інформації, що надасть ще один рівень безпеки для організацій.

3 РОЗРОБКА ТЕХНОЛОГІЇ ПРОТИДІЇ ВИТОКАМ ДАНИХ В ОРГАНІЗАЦІЯХ НА ОСНОВІ DLP SAFETICA ONE

3.1 Налаштування політик DLP

Успішна інтеграція будь-якого продукту в систему є тільки першим кроком до використання його функцій. Після нього настає більш широкий процес налаштування роботи продукту. DLP-рішення Safetica має достатньо зрозумілий інтерфейс для адміністраторів безпеки. Вона зможе допомогти класифікувати дані і створити необхідіні політики запобігання витоку інформації. DLP-рішення Safetica має два основні модулі Discovery та Protection.

Розділ Discovery забезпечує огляд потенційних проблем безпеки та дає змогу краще зрозуміти процеси безпеки. За його допомогою можна перевіряти конфіденційні файли, витік яких може становити загрозу безпеці. Також, всю інформацію можна використовувати для впровадження DLP-політик. Крім цього, завдяки аудиту апаратного забезпечення можна побачити, на які пристрої передаються файли, як використовуються принтери та які файли завантажуються через корпоративну мережу.

Даний модуль допоможе проаналізувати вашу 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 вашу 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 можна використовувати зони. В зонах можна створити набори довірених та заборонених

зовнішніх пристроїв, принтерів, IP-адрес, мережевих шляхів та електронних адрес.

Існує кілька послідовність, як налаштування захисту 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)[13].

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 можна створити різні DLP-політики і таким чином захистити класифіковані дані.

Safetica використовує політики DLP для захисту даних на робочих станціях та для контролю поведінки програм. Політиками ми можемо заблокувати 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. Вона допоможуть попередити можливі витоки даних та зменшують збитки від можливого людського фактору від працівників.

3.2 Створення політики з розпізнавання IBAN та номерів карток

Створення категорії даних потрібно починати з розуміння того, що ми маємо захистити від витоку. Як було сказано в 1 розділі роботи найчастіше зловмисники полюють на особисті дані, такі як номери кредитних картках чи IBAN, щоб потім використати їх в зловмисних цілях або продати. Отже, перше, що ми будемо захищати — 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.

Відкриваємо Safetica Management Console та заходимо в розділ Protection. Обираємо підрозділ Data categories та натискаємо «New data category» (рис.3.1).

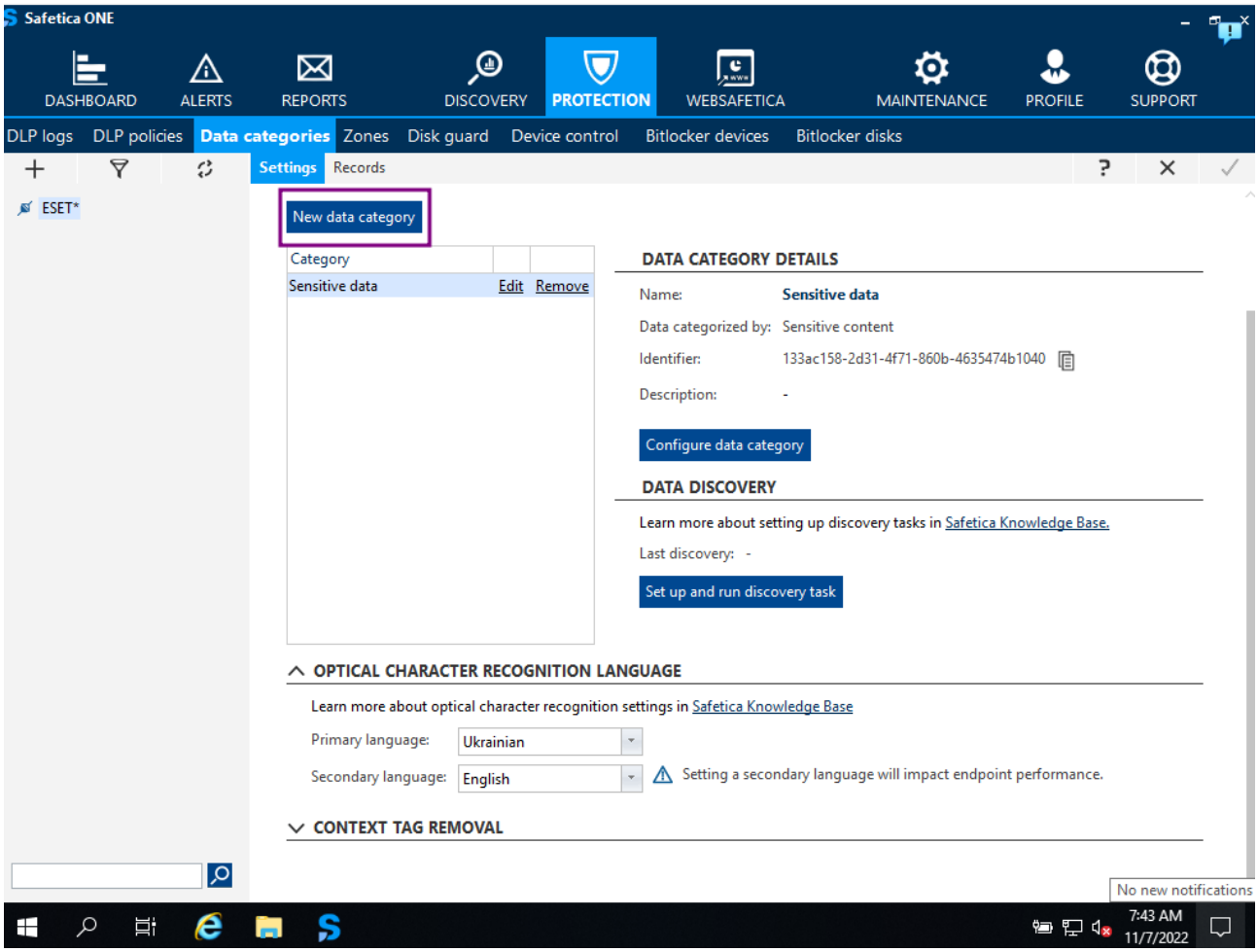

Рис. 3.1. Вікно підрозділу Data categories

Далі обираємо тип категорії даних Sensitive content та вводимо її назву. Після цього натискаємо «ОК» (рис.3.2).

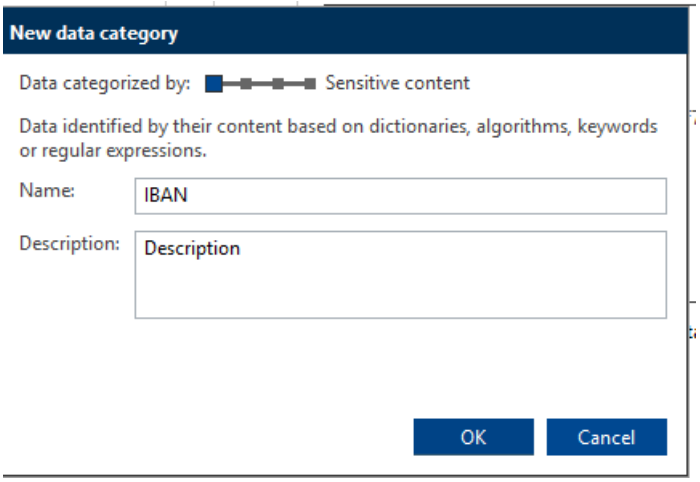

Рис. 3.2. Вікно вибору типу категорії даних

Повернувшись до попереднього вікна, обираємо створену категорію даних та натискаємо «Configure data category» (рис.3.3).

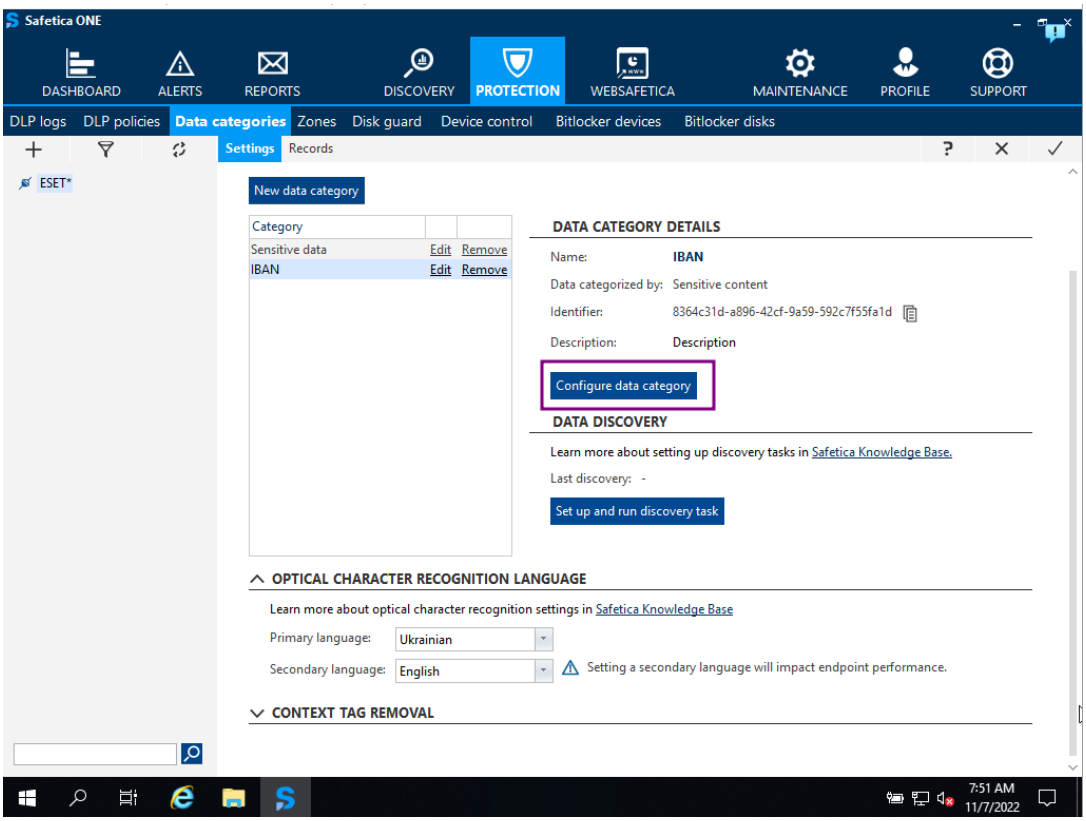

Рис. 3.3. Вікно вибору налаштування категорії даних

У наступному вікні потрібно обрати правило розпізнавання для категорії даних. Натискаємо «New detection rule» (рис.3.4).

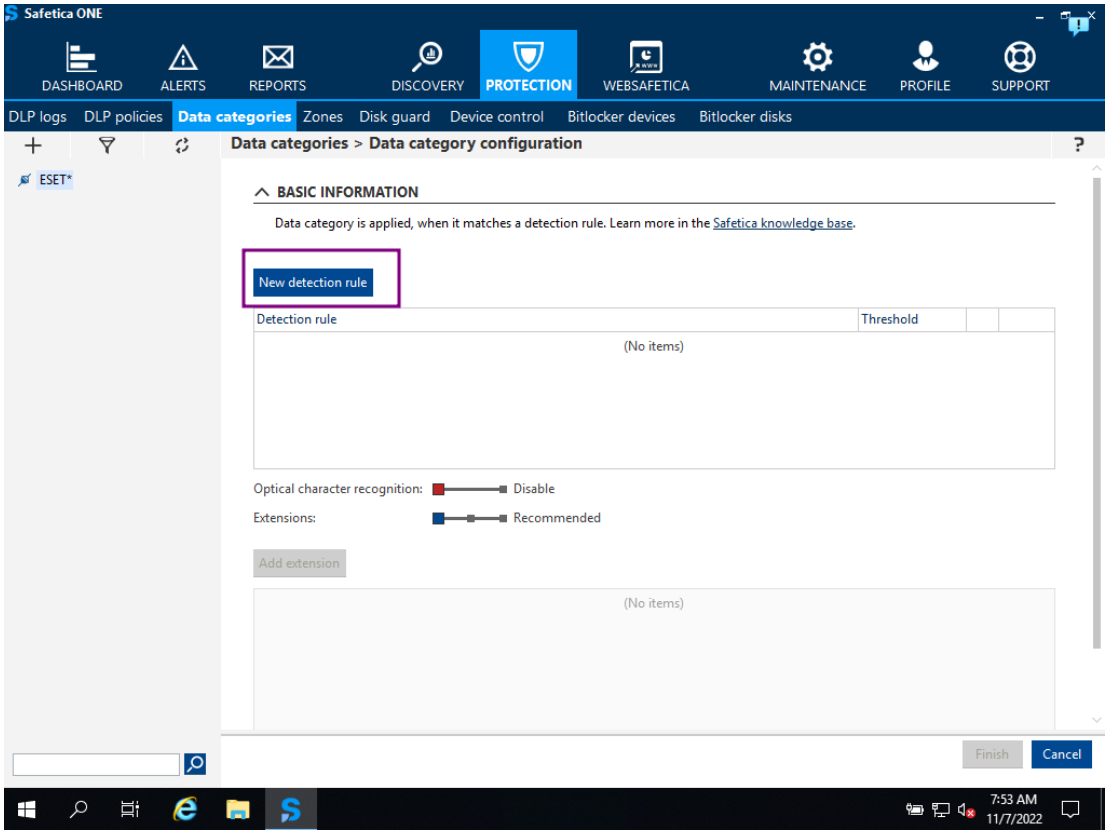

Рис. 3.4. Вікно налаштувань категорії даних

В новому вікні потрібно налаштувати правило розпізнавання. В першому

розділі можемо обрати кількість повторів обраної інформації в одному документі. Ми оберемо 2 повтори. В наступному розділі потрібно обрати інформацію, яку потрібно шукати в документах. Ми оберемо номери IBAN та натиснемо «ОК» (рис.3.5).

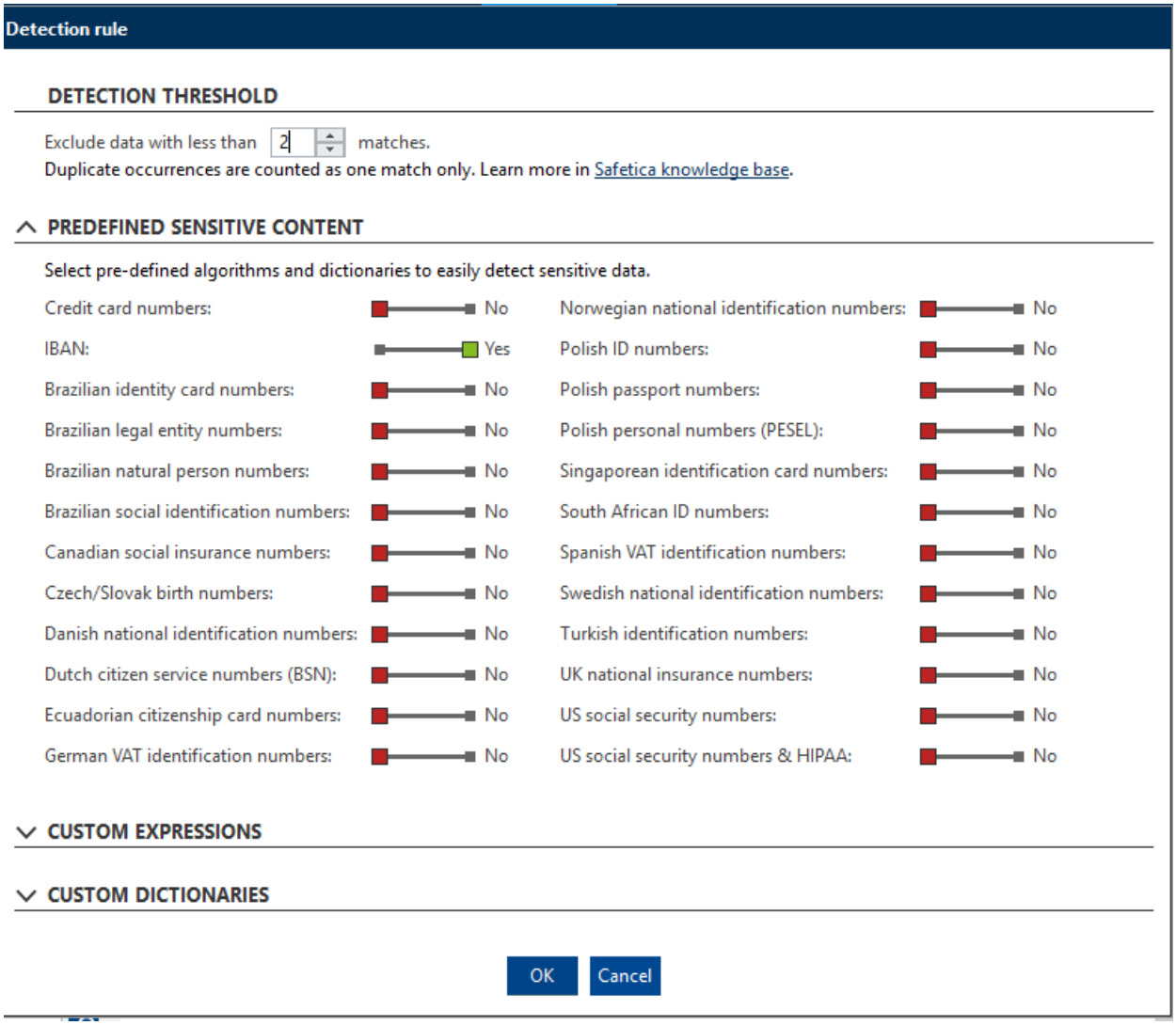

Рис. 3.5. Вікно створення правила розпізнавання IBAN

Далі так само створюємо правило розпізнавання номерів кредитних карток. Після цього опускаємося нижче, де є можливість обрати розширення файлів. Якщо ви знаєте, які розширення найчастіше використовуються, то можете їх ввести вручну або обрати відповідну категорію розширень файлів. Ми оберемо всі розширення файлів. Після цього натискаємо «Finish» (рис.3.6).

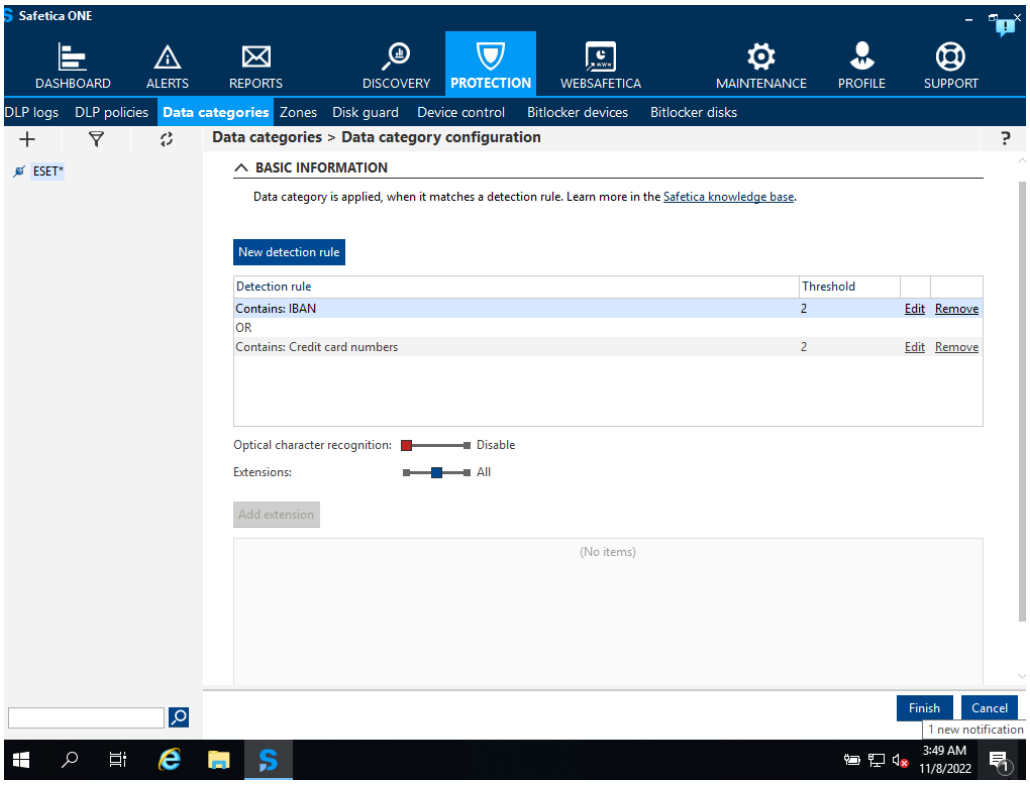

Рис. 3.6. Вікно створеного правила розпізнавання

Зберігаємо налаштування в підрозділі Data categories, натиснувши галочку вгорі справа 

Наступний крок - це створення політики. Для цього переходимо в підрозділ DLP policies. Обираємо «New policy», щоб створити нову політику (рис.3.7).

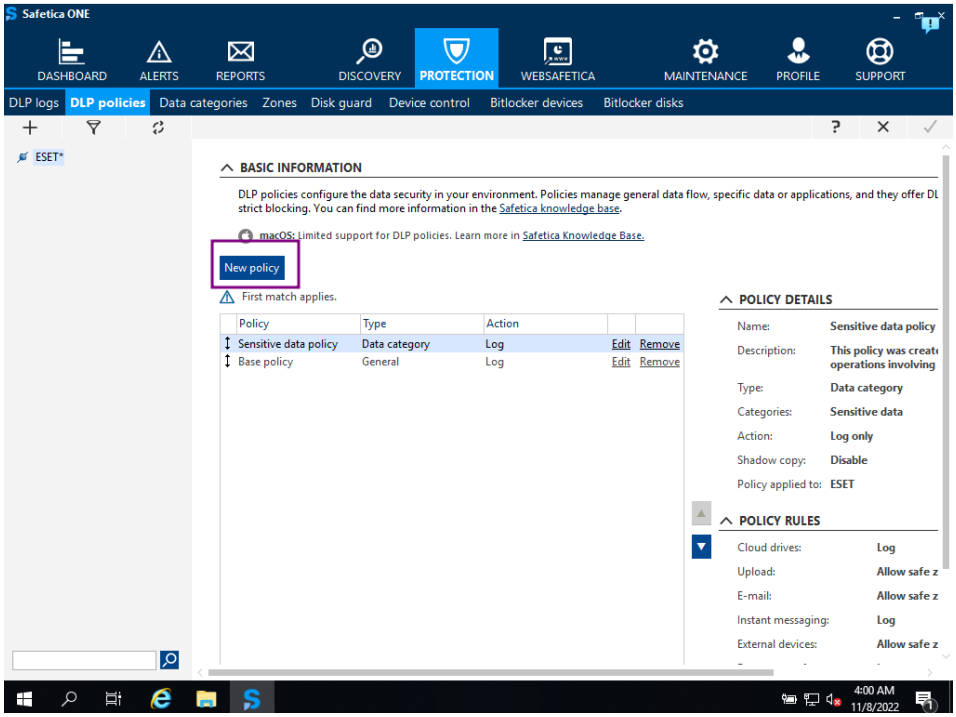

Рис. 3.7. Вікно підрозділу DLP policies

У новій вкладці потрібно обрати тип політики, яку ми будемо створювати. Потрібно обрати тип Data та обрати категорію даних, яку ми попередньо створили. Після цього натискаємо «Next», щоб перейти до налаштування політики (рис.3.8).

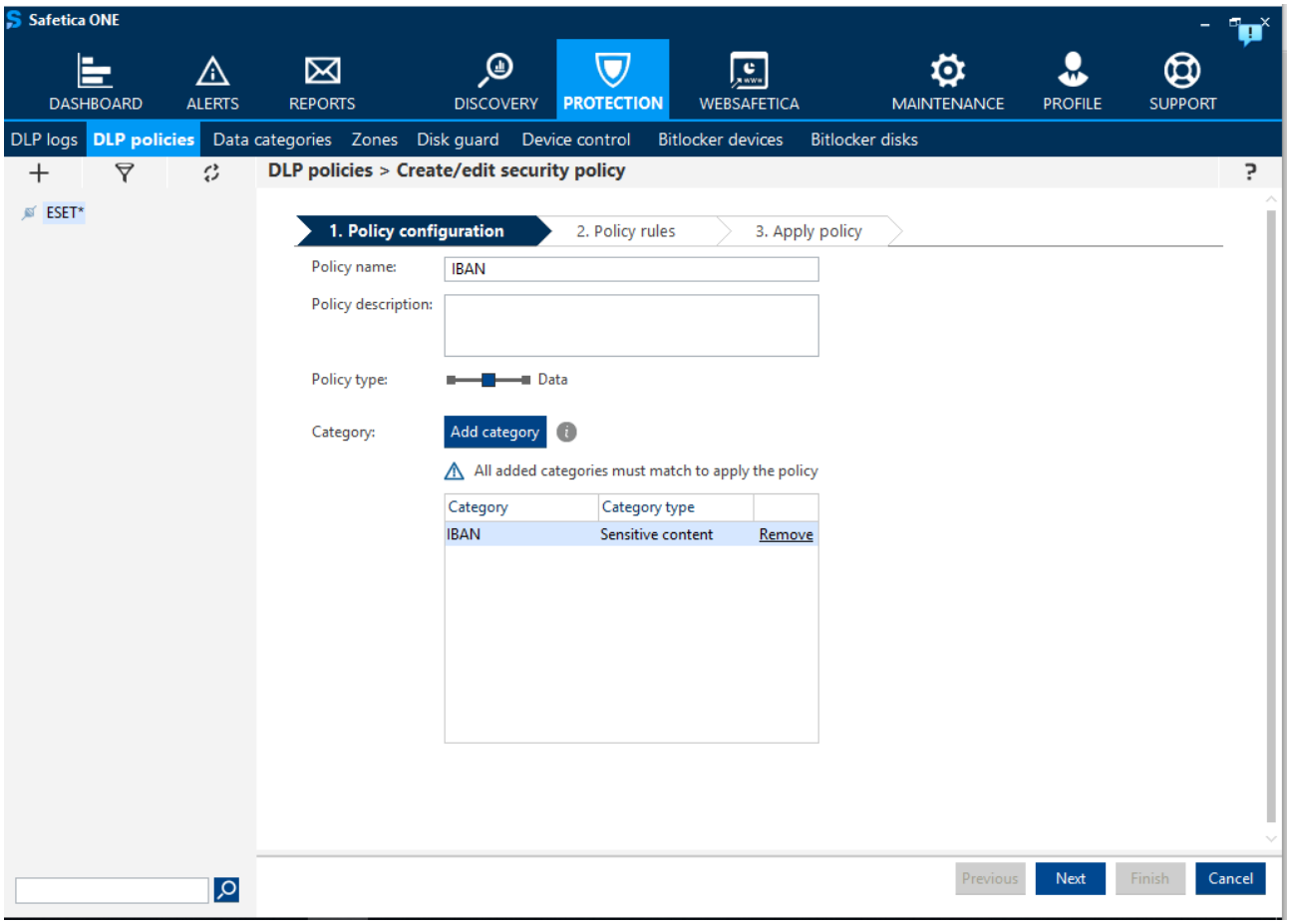

Рис. 3.8. Вікно вибору типу політики

Далі потрібно обрати дію, яку буде виконувати політика(логування або блокування). Ми обираємо дію Log and block. Щоб переглянути доступні правила політики DLP, натисніть «Customize». Доступні правила будуть розміщені у списку, тому ви можете обирати їх. Для створення нових DLP-політик також можна використовувати шаблони політик - заздалегідь визначені групи правил. Після вибору налаштувань натискаємо «Next» (рис.3.9).

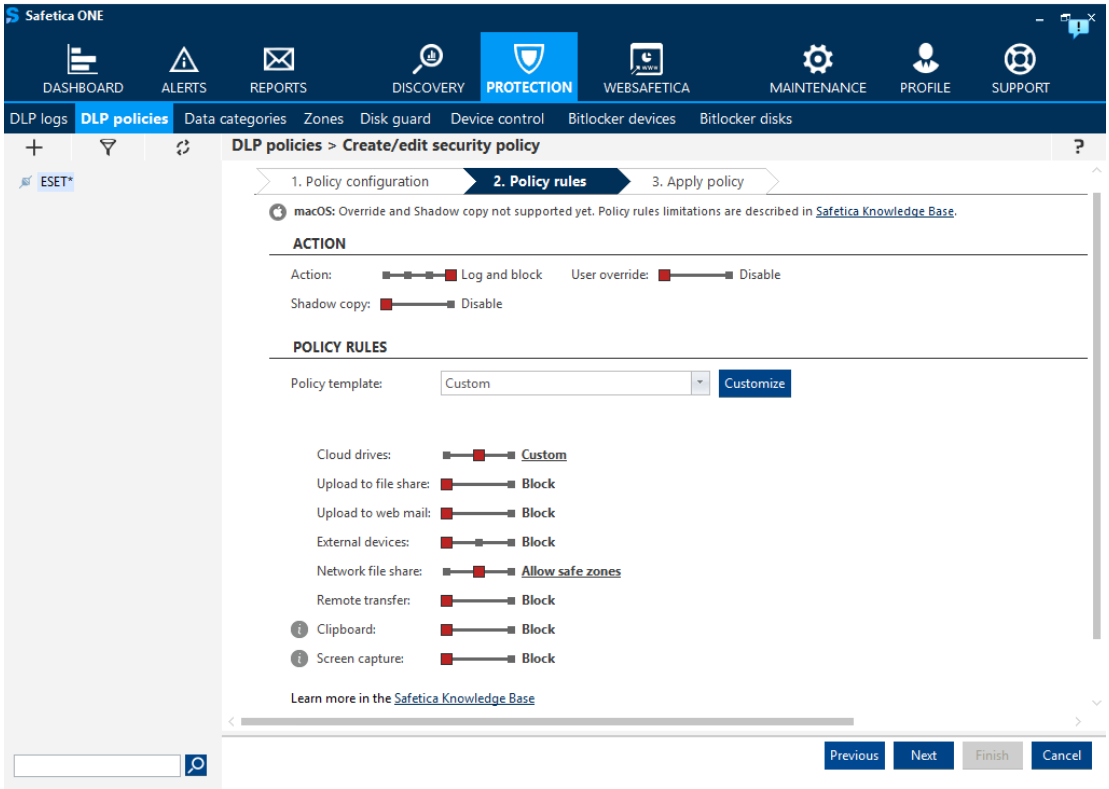

Рис. 3.9. Вікно вибору налаштувань політики

В наступному вікні обираємо ПК чи користувача до якого буде застосовано політику (можна обрати відразу всю організацію, тоді політика буде застосовуватися до всіх ПК та користувачів). Далі обираємо «Finish» (рис.3.10).

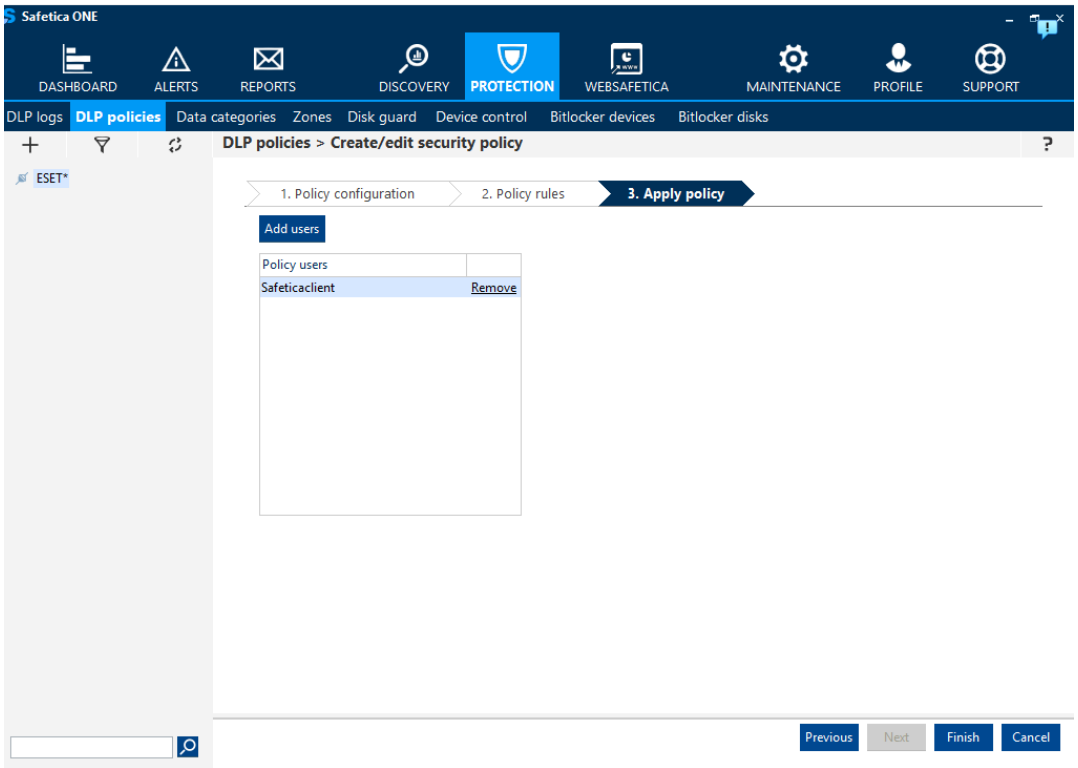

Рис. 3.10. Вікно вибору ПК чи користувачів

Зберігаємо налаштування в підрозділі DLP policies, натиснувши галочку вгорі справа 

3.3 Створення політики з використанням тегів

Наступну категорію даних можна використовувати, якщо у вас документи розміщенні по відповідним текам. Тобто після проведеного аудиту всі документи відсортовані за їх критичністю, а далі розміщені в теках з відповідними доступами. Щоб мінімізувати ризик витоку такої критичної інформації, можна скористатися категорією даних Context rules. При відповідних налаштуваннях вона присвоює кожному документу відповідний тег на основі файлової системи. Даний тег не можна видалити чи змінити кінцевому користувачеві, всі ці дії проводяться тільки у консолі управління адміністратором. Тег залишається на документі, якщо його перейменувати чи змінити розширення, навіть якщо заархівувати відповідний документ, тег залишиться на місті, адже він присвоєний на основі файлової системи. Переглянути, чи присвоєний тег відповідному документу можна за допомогою Командного рядка. Потрібно відкрити теку, де знаходяться протеговані документи і ввести команду виводу розширеної інформації dir /r і можна побачити в властивостях відповідний тег, який присвоєний DLP-рішенням Safetica.

Для того, щоб створити категорію даних Context rules відкриваємо Safetica Management console та переходимо в розділ Protection. Обираємо підрозділ Data categories та натискаємо «New data category», щоб створити відповідну категорію даних. У вікні вибору типу категорії даних обираємо Context rules та вводимо її назву. Після цього натискаємо «ОК» (рис.3.11).

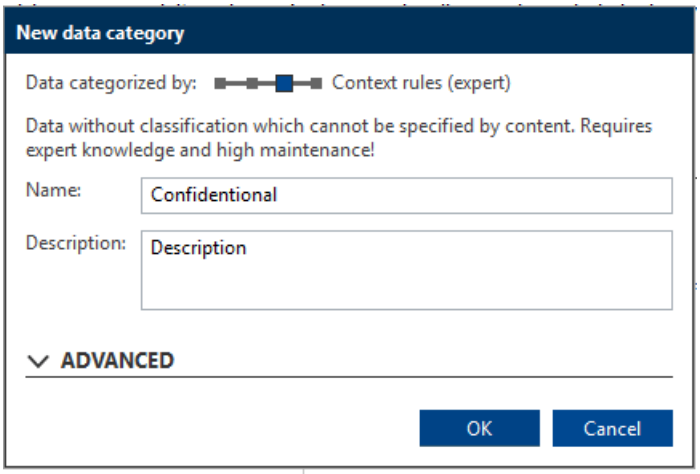

Рис. 3.11. Вікно вибору типу категорії даних

Повернувшись до попереднього меню, оберіть щойно створену категорію даних та натисніть «Configure data category», щоб налаштувати її. У новому вікні спускаємося нижче та знаходимо розділ Path rules. В даному розділі ми зможемо створити правило тегування файлів за шляхом до відповідної теки. Натискаємо «Add» (рис.3.12).

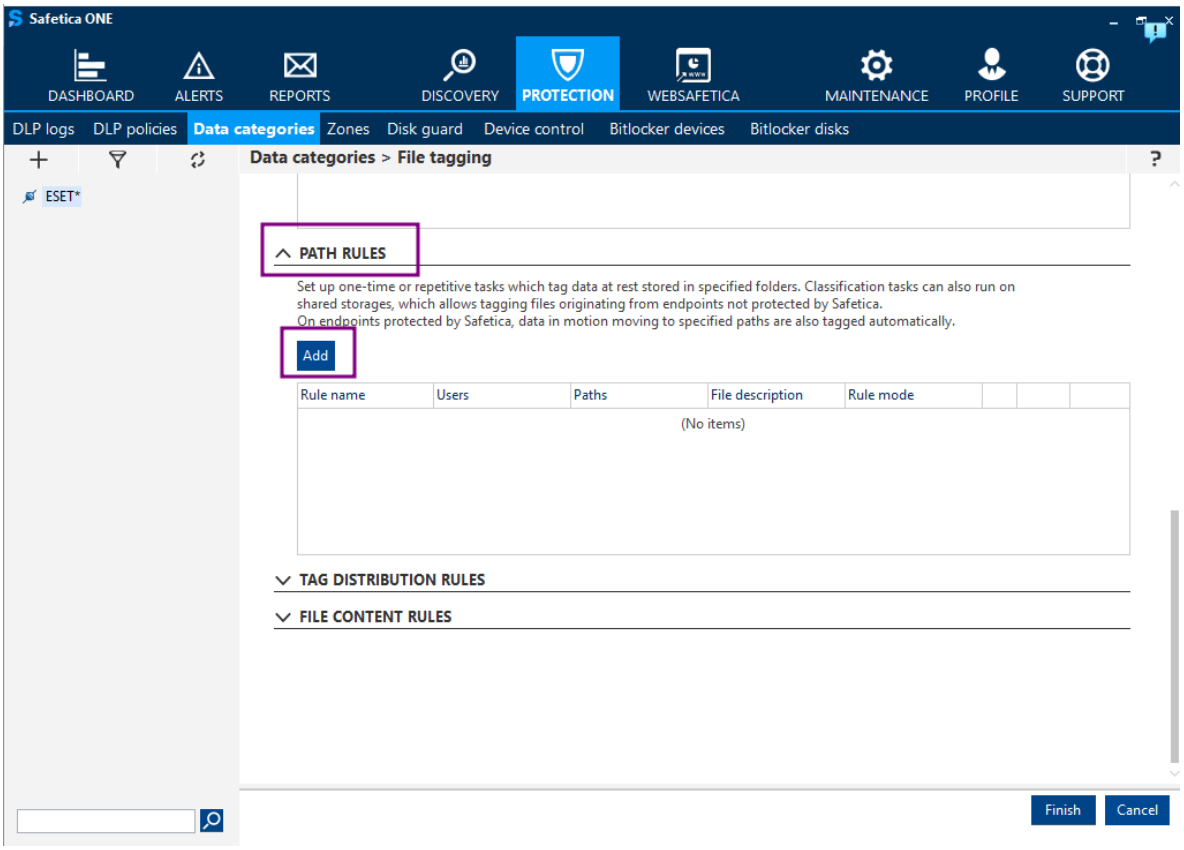

Рис. 3.12. Вікно створення правила тегування

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 файлів (ми використаємо створені за замовчуванням категорії розширення файлів Text files, Spreadsheet files, Presentation). Після введення всієї необхідної інформації натискаємо «Finish» (рис.3.13).

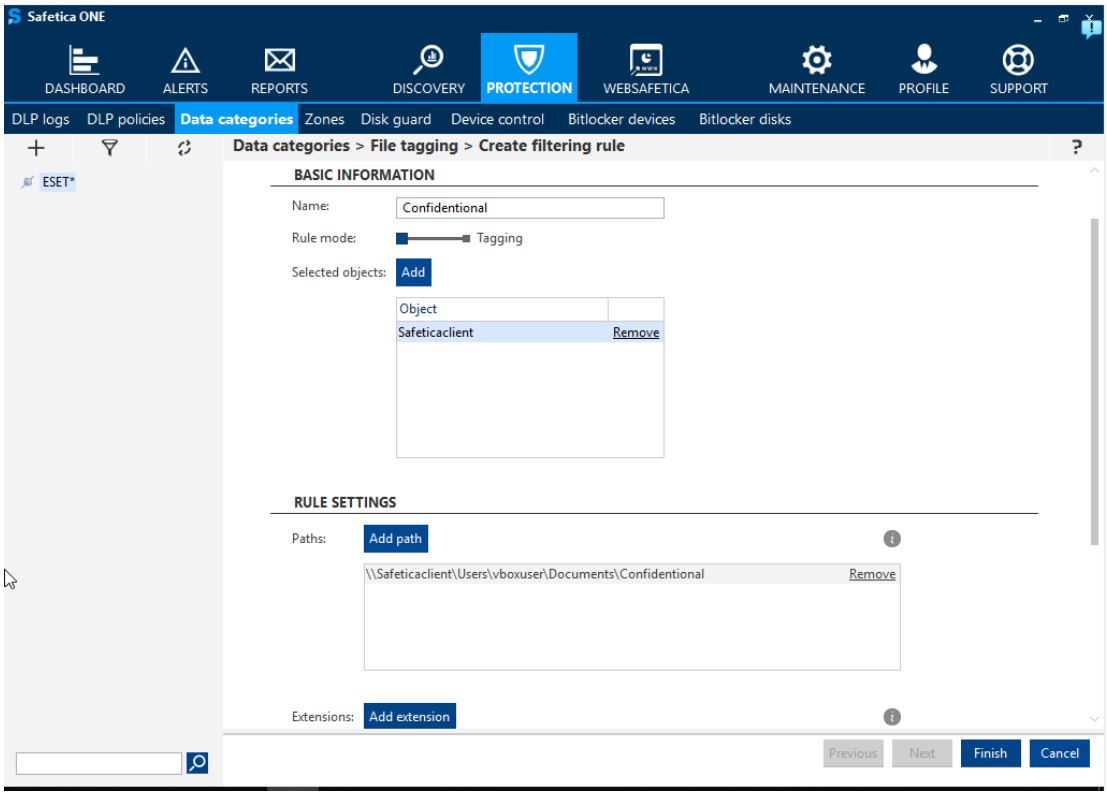

Рис. 3.13. Вікно створення правила тегування

Перевіряємо створене правило тегування за шляхом до теки та натискаємо «Finish», щоб категорія даних успішно збереглася (рис.3.14).

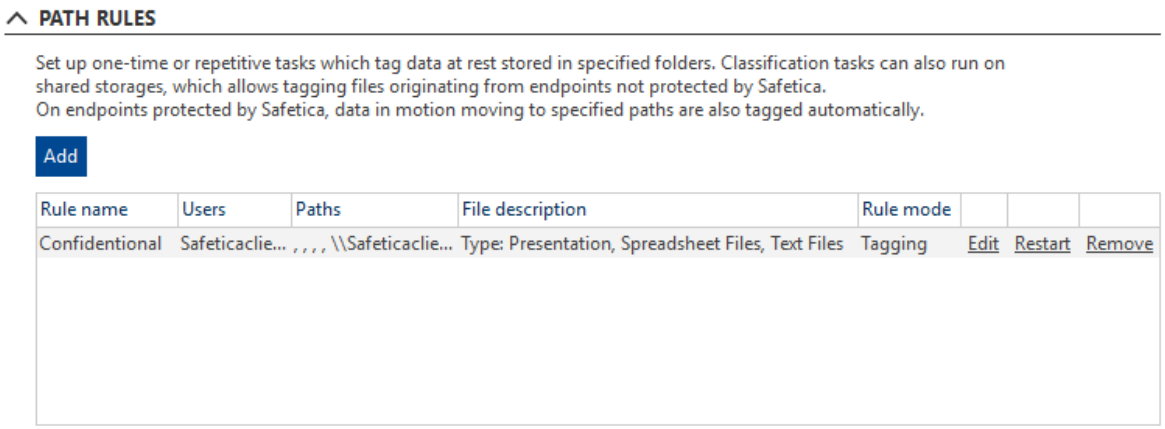

Рис. 3.14. Створене правило тегування

Після успішного створення категорії даних переходимо до створення політики. Переходимо у підрозділ DLP policy та натискаємо «New policy». В новому вікні вводимо назву політики та обираємо тип Data. Далі обираємо із випадаючого списку попередньо створену категорію даних Context rule. Після цього переходимо до налаштування політки натиснувши «Next». Ставимо дію Log and block, щоб мінімізувати можливий витік конфіденційний тегованих файлів. Налаштовуємо правила політики та натискаємо «Next». Далі обираємо ПК та\або користувачів, до яких буде застосовуватися політика і натискаємо «Finish» (рис.3.15).

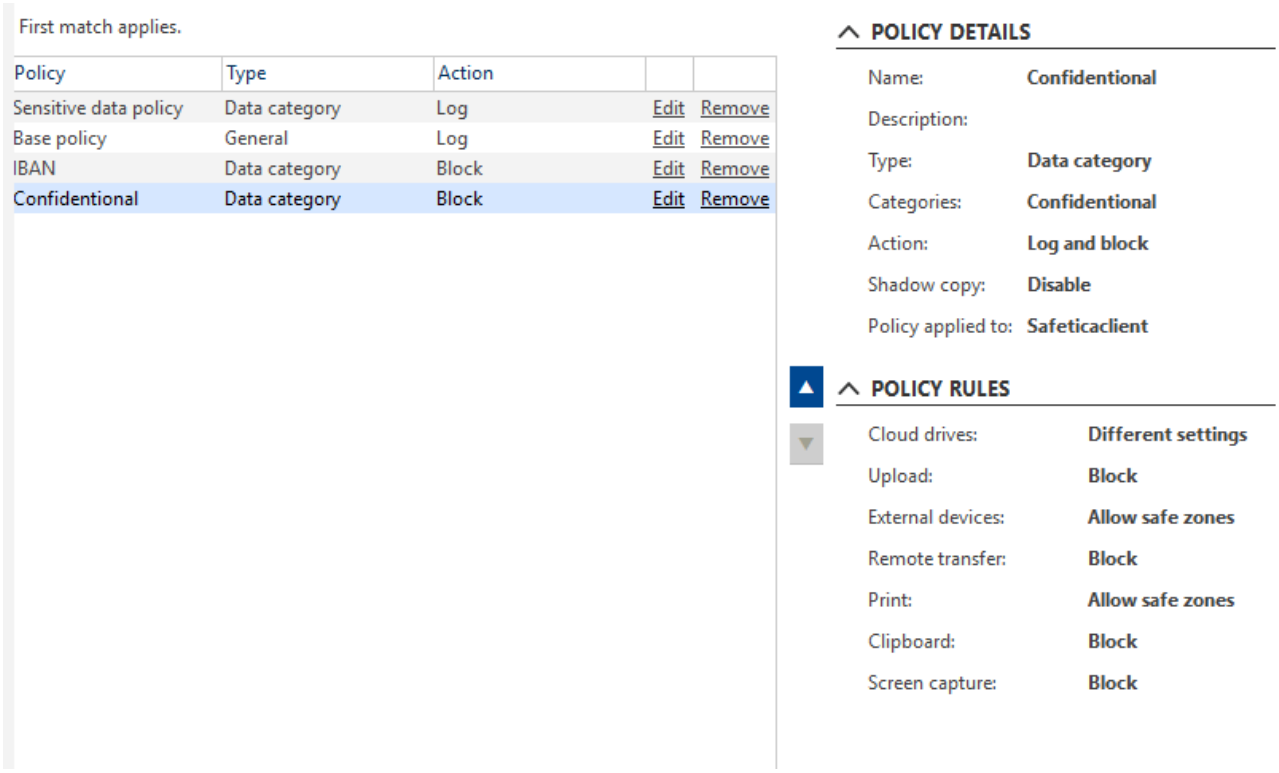

Рис. 3.15. Перегляд налаштувань політики

Перевіряємо правильність налаштувань та зберігаємо політику, натиснувши галочку вгорі справа 

Наступним кроком буде 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.3.16).

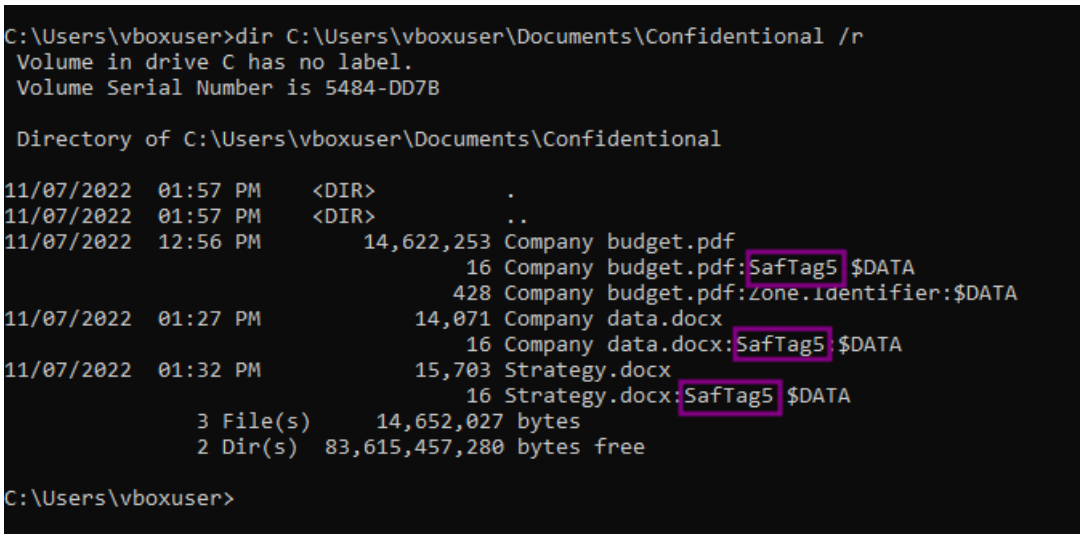

Рис. 3.16. Вивід команди з детальною інформацією про файли

3.4 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 можна створити політики блокування доступу до додатків та веб сайтів на ПК. Так можна обмежити доступ працівників, щоб вони не могли використовувати неавторизовані у вашій системі додатки для передачі інформації. Як було наголошено у першому розділі, часто використання саме месенджерів на робочу місці провокує багато витоків інформації. Для простих працівників зручніше відправити документ у месенджері, чим використовувати дозволені шляхи передачі конфіденційної інформації. Щоб запобігти виникненням таких ситуації на робочому місці, можна превентивно заблокувати доступ до месенджерів (додатків і веб версій) на робочих комп'ютерах.

Виконати відповідне налаштування можна відкривши WebSafetica та авторизуватися. Знаходимо розділ Policies. Бачимо, що є два види налаштування політик доступу: додатки та веб сайти. Обираємо спершу Websites та натискаємо «Add policy» (рис.3.17).

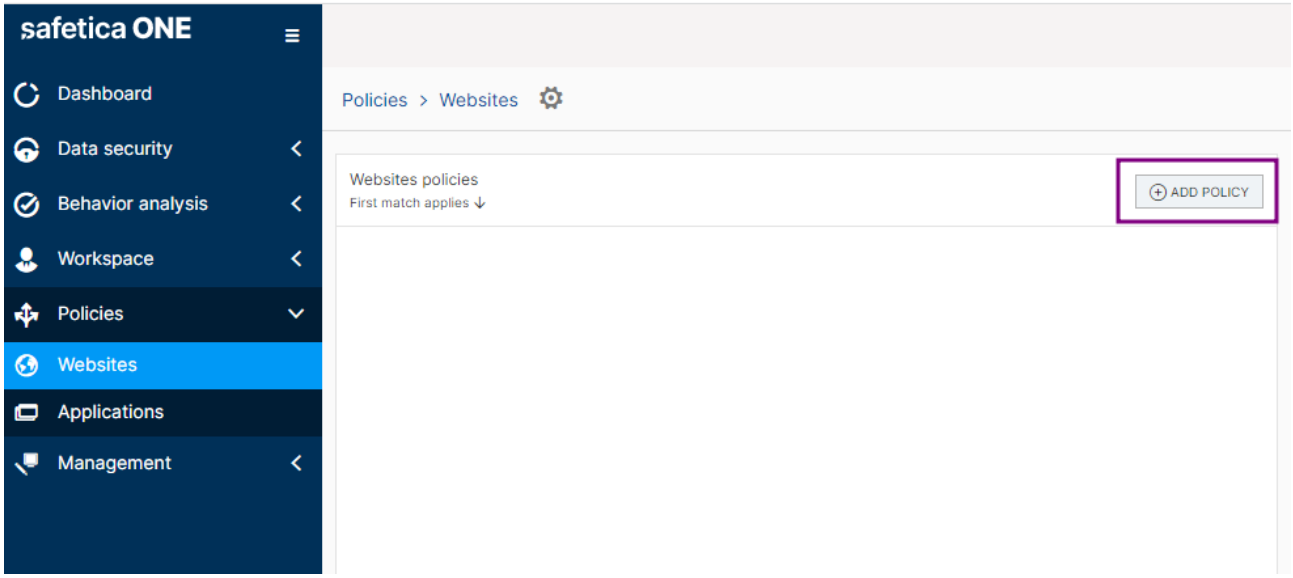

Рис. 3.17. Вікно додавання нової політики

Після цього налаштовуємо політику доступу. Вводимо назву, обираємо до яких ПК буде застосовуватися політика. Наступним кроком додаємо правило блокування, натискаємо «Add rules». В новому вікні можемо обрати готову категорію веб сайтів або ввести відповідний сайт вручну через URL (рис.3.18).

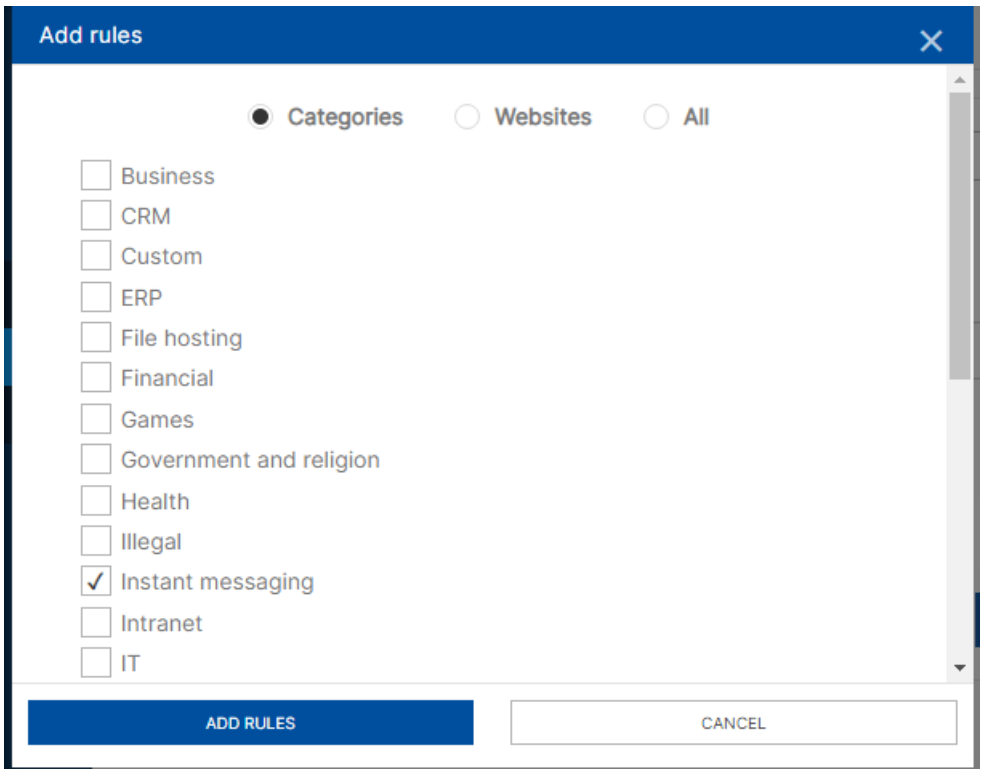

Рис. 3.18 Вікно налаштування правила блокування

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

Для зручності ми обрали категорію веб сайтів «Instant messaging», в ній зібрані веб версії відомих месенджерів. В одній політиці можна обрати декілька правил блокування. Далі перевіряємо введені дані та натискаємо «Add policy» (рис.3.19).

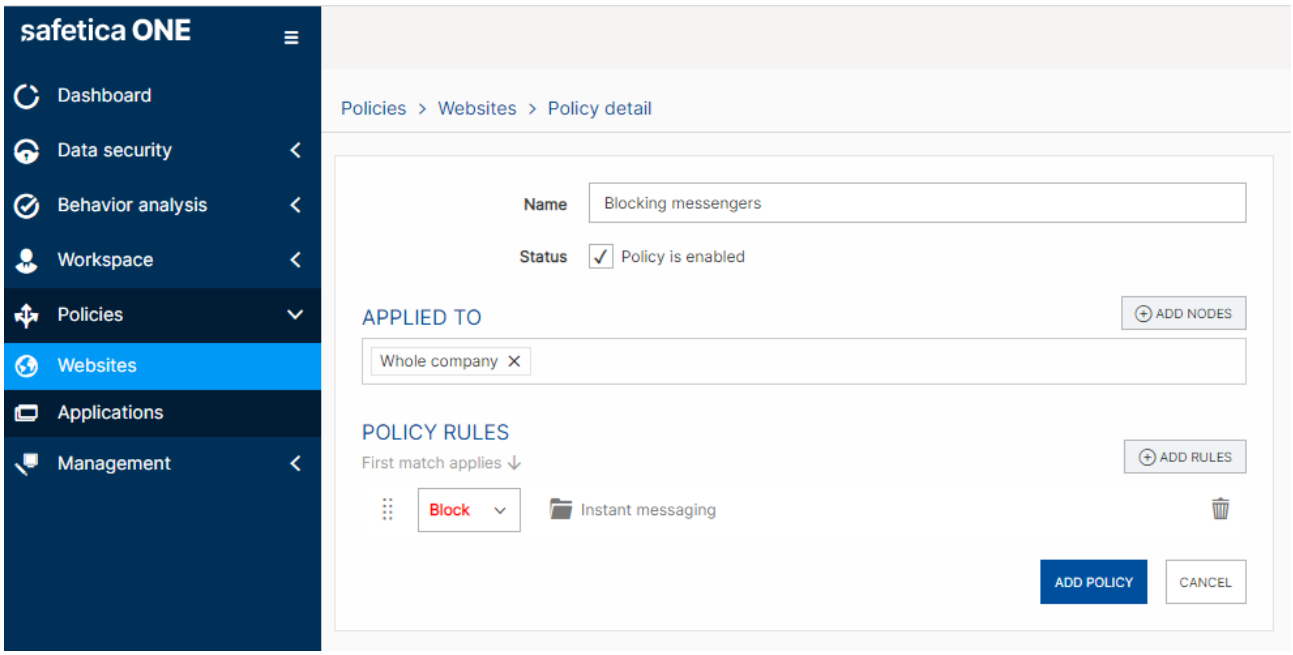

Рис. 3.19. Вікно перегляду налаштувань політики

Переходимо до меню Applications та натискаємо «Add policy». Вводимо назву нової політики та обираємо ПК, натиснувши «Add nodes». Далі додаємо правило блокування доступу до додатків. Натискаємо «Add rules». Бачимо, що аналогічно до політики блокування доступу до веб сайтів, можна блокувати доступ до додатків за категоріями додатків або обрати відповідний додаток із списку встановлених. Ми оберемо вже готову категорію даних «Instant messaging» (рис.3.20).

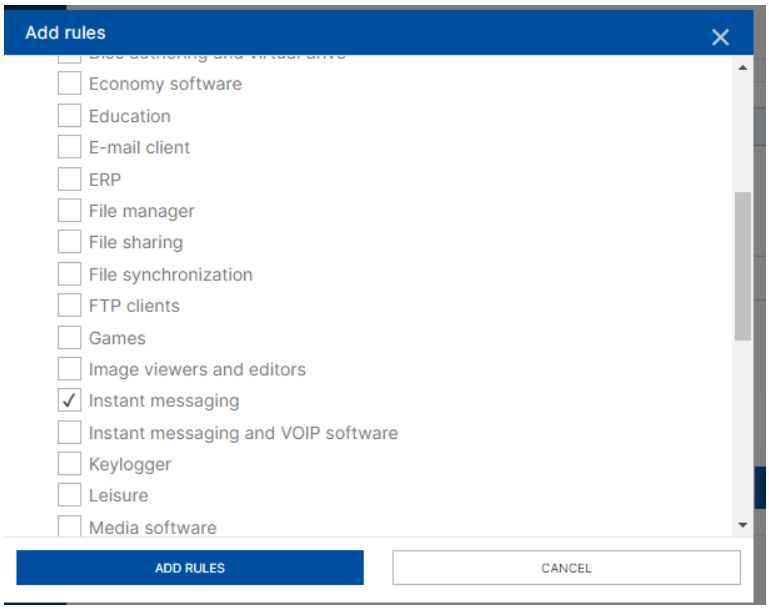

Рис. 3.20. Вікно вибору політики блокування

Після вибору правила блокування, натискаємо «Add rules». Перевіряємо правильність введених даних, для коректної роботи політики та натискаємо «Add policy» (рис.3.21).

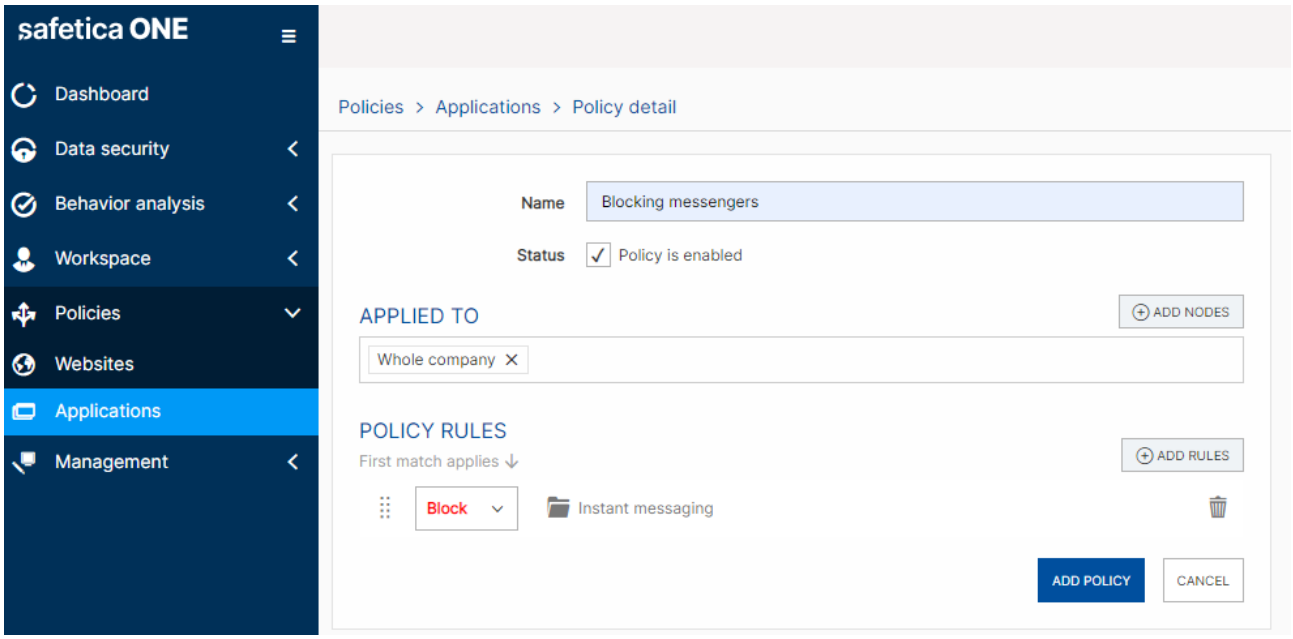

Рис. 3.21. Вікно перегляду налаштувань

Обидві політики успішно створені та будуть застосовані до відповідних ПК.

Під час налаштування політик блокування доступів до додатків та веб сайтів, ми використовували категорії додатків та веб сайтів. Ми можемо 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.3.22).

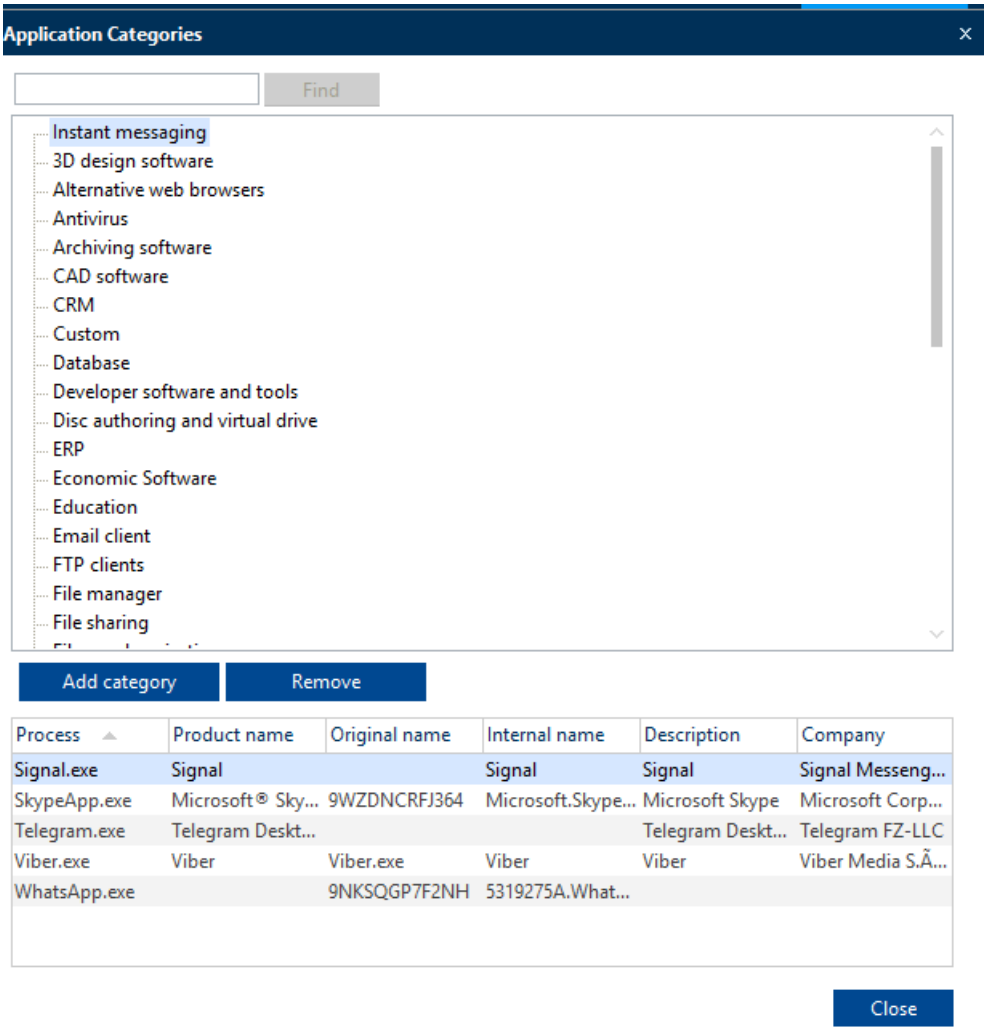

Рис. 3.22. Вікно перегляду категорій додатків

Висновок

В даному розділі було наведено налаштування найбільш потрібних політик захисту інформації від витоку даних. Ми за допомогою їх можемо мінімізувати ризики від витоку конфіденційної інформації з відповідних тек. Також, заблокували передачу несанкціонованими каналами передачі інформації з вказаними банківськими даними (IBAN, Credit cards). Заблокували доступ до месенджерів на робочих ПК, щоб працівники не зловживали ними та не надсилали конфіденційні документи. Дані налаштування DLP-рішення Safetica допоможуть захистити деякі конфіденційні дані в організації, проте це може бути тільки початком масштабного інтегрування даного рішення в систему безпек

ВИСНОВКИ

Отже, витік даних є дуже серйозним викликом для організацій, оскільки недотримання рекомендацій може призвести до непоправних наслідків. Цифровізація організацій змогла спростити методи управління. Проте з’явилися нові виклики, які потребують постійної пильності. У свою чергу, рішення DLP зможуть закрити вразливості, які зловмисники можуть використовувати для вилучення конфіденційних даних з організацій. Добре побудовані системи з DLP Safetica можуть допомогти компаніям будь-якого типу захистити свої дані та репутацію.

DLP-рішення Safetica протидіє витокам даних. Щоб налаштувати його на роботу, вам спочатку потрібно з’ясувати, як інтегрувати його у вашу існуючу систему безпеки. Тому потрібно почати з вивчення рекомендацій щодо апаратного та програмного забезпечення. Інтеграція рішення допоможе правильно налаштувати всі компоненти системи для зручності їх використання. Розгортання DLP Safetica не займає багато часу та зусиль, що є перевагою. Компоненти системи працюють разом для подальшого контролю над витоком інформації, що забезпечить ще один рівень безпеки для організацій.

Наведені найбільш затребуваних параметри політик захисту інформації від витоку даних. За їх допомогою можемо мінімізувати ризики від витоку конфіденційної інформації. Дані налаштування DLP-рішення Safetica допоможуть захистити деякі конфіденційні дані в організації, проте це може бути тільки початком масштабного інтегрування даного рішення в систему безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. What's the Difference Between a Data Leak and a Data Breach? [Електронний ресурс] – Режим доступу: https://abnormalsecurity.com/glossary/data-leak
2. What is a Data Leak? Stop Giving Cybercriminals Free Access [Електронний ресурс] – Режим доступу: https://www.upguard.com/blog/data-leak
3. Найпоширеніші внутрішні загрози безпеки даних та способи боротьби з ними [Електронний ресурс] – Режим доступу: https://corewin.ua/blog/internal-data-security-threats/
4. СКІЛЬКИ ВТРАЧАЄ БІЗНЕС ЧЕРЕЗ ВИТОК ДАНИХ? - ЗВІТ IBM 2021 [Електронний ресурс] – Режим доступу: https://denovo.ua/blog/vitok-danyh-v-2021-ibm
5. What is the Cost of a Data Breach in 2022? [Електронний ресурс] – Режим доступу: https://www.upguard.com/blog/cost-of-data-breach
6. The Cost of a Breach: 10 Terrifying Cybersecurity Stats Your MSP's Customers Need to Know [Електронний ресурс] – Режим доступу: https://connect.comptia.org/content/articles/the-cost-of-a-breach-10-terrifying-cybersecurity-stats-your-msp-s-customers-need-to-know
7. DLP-системи: що це таке. Впровадження, завдання та вимоги [Електронний ресурс] – Режим доступу: https://presa.com.ua/aktualne/dlp-sistemi-shcho-tse-take-vprovadzhennya-zavdannya-ta-vimogi.html
8. Data Loss Prevention (DLP) [Електронний ресурс] – Режим доступу: https://www.netskope.com/security-defined/what-is-data-loss-prevention-dlp
9. WHAT IS DATA LOSS PREVENTION (DLP)? [Електронний ресурс] – Режим доступу: https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/
10. Data Loss Prevention (DLP) [Електронний ресурс] – Режим доступу: https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/
11. Safetica ONE. Enterprise DLP and Insider Protection [Електронний ресурс] – Режим доступу: https://www.safetica.com/products-safetica-one
12. Safetica. Портфоліо рішень. Запобігання втратам даних[Електронний ресурс] – Режим доступу: https://eset.ua/download_files/products/Safetica_Datasheet.pdf
13. Safetica. Complete documentation [Електронний ресурс] – Режим доступу: https://cdn.safetica.com/help/Safetica_Complete_Documentation_EN.pdf