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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо захисту від несанкціонованого доступу до інформаційної системи з використанням DLP»

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

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

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

_____ Валентин СХЕЙБАЛ
(підпис)

Виконав: здобувач вищої освіти групи БСЗ-51
СХЕЙБАЛ Валентин
(прізвище, ім'я)

Керівник ст. викладач ЧУМАК Надія
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
"___" _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Схейбалу Валентину Руслановичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розробка рекомендацій щодо захисту від несанкціонованого доступу до інформаційної системи з використанням DLP»
керівник кваліфікаційної роботи Чумак Надія, ст. викладач
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «_27_» _лютого_ 2024 року № __36__.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи програмні засоби захисту від несанкціонованого доступу;
наукова та технічна література, експлуатаційна документація;
нормативні документи;
технологія захисту DLP Safetica ONE.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми забезпечення безпеки організації від несанкціонованого доступу.
2. Дослідження методів та засобів захисту від несанкціонованого доступу.
3. Розробка рекомендацій щодо захисту від несанкціонованого доступу до інформаційної системи з використанням DLP.

5. Перелік ілюстрованого матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту від несанкціонованого доступу до інформаційної системи.	27.02.2024 р.	викон.
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	05.03.2024 р.	викон.
3.	Аналіз проблеми забезпечення безпеки організації від несанкціонованого доступу.	15.04.2024 р	викон.
4.	Дослідження методів та засобів захисту від несанкціонованого доступу.	15.04.2024 р	викон.
5.	Розробка рекомендацій щодо захисту від несанкціонованого доступу до інформаційної системи з використанням DLP.	15.05.2024 р	викон.
6.	Оформлення результатів дослідження.	16.05.2024 р	викон.
7.	Підготовка доповіді до захисту.	31.05.2024 р.	викон.

Здобувач вищої освіти _____ Валентин СХЕЙБАЛ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Надія ЧУМАК
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача СХЕЙБАЛА Валентина

на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту від несанкціонованого доступу до інформаційної системи з використанням DLP»

Актуальність: В умовах зростаючих кіберзагроз та постійних спроб несанкціонованого доступу до конфіденційних даних, забезпечення інформаційної безпеки стає ключовим завданням для організацій. Технології Data Loss Prevention (DLP) пропонують ефективні інструменти для виявлення, моніторингу та запобігання витоку даних, що робить їх важливими для захисту інформаційних систем. Дослідження шляхів впровадження та розробка рекомендацій щодо використання DLP-систем допоможуть організаціям адаптуватися до нових загроз, підвищити рівень безпеки та зберегти конфіденційність критичної інформації. Це дослідження є надзвичайно актуальним для мінімізації ризиків та забезпечення стійкості сучасних інформаційних систем.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми забезпечення безпеки організації від несанкціонованого доступу.
2. Впровадження рекомендацій щодо використання DLP Safetica ONE значно знижує ризики витоку конфіденційної інформації та захищає організацію від несанкціонованого доступу.
3. 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 кваліфікаційній роботі доцільно було б більш детальніше описати методи та засоби захисту від несанкціонованого доступу інформаційної системи.
2. Запропонований варіант технології DLP Safetica ONE для захисту від несанкціонованого доступу доцільно було б порівняти з іншими існуючими DLP системами.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач **СХЕЙБАЛ Валентин** – присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач СХЕЙБАЛ Валентин до захисту кваліфікаційної роботи
(прізвище, ім'я)

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

на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту від несанкціонованого доступу до інформаційної системи з використанням DLP».

Кваліфікаційна робота і рецензія додаються.
Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***СХЕЙБАЛ Валентин*** обрав тему роботи, метою якої було дослідити методи та засоби захисту від несанкціонованого доступу до інформаційної системи з використанням DLP та розробити рекомендації щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***СХЕЙБАЛ Валентин*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***СХЕЙБАЛА Валентина*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Надія ЧУМАК
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **СХЕЙБАЛ Валентин** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 60 сторінок, 48 рисунків, 16 джерел.

Об'єкт дослідження – процес забезпечення захисту інформаційної системи від несанкціонованого доступу.

Предмет дослідження – методи та засоби захисту інформаційної системи від несанкціонованого доступу на основі DLP.

Мета роботи розробити рекомендації щодо захисту від несанкціонованого доступу до інформаційної системи з використанням DLP.

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

DLP-системи надають комплексний підхід до захисту конфіденційної інформації, забезпечуючи ідентифікацію, моніторинг та контроль даних. Вони дозволяють не тільки виявляти спроби витоку даних, але й запобігати їм, що робить їх важливим інструментом для забезпечення інформаційної безпеки. В умовах постійного зростання кіберзагроз і розвитку технологій, впровадження DLP-систем стає необхідністю для сучасних організацій.

В роботі досліджено проблему захисту інформаційної системи від несанкціонованого доступу, визначено його мету та завдання. Досліджено методи та засоби захисту захисту від несанкціонованого доступу на основі DLP .

На основі досліджень проведених в роботі запропоновано варіант системи на основі DLP. Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації методів та засобів захисту інформаційної системи від несанкціонованого доступу.

Галузь використання – кібербезпека інформаційних ресурсів компанії.

DLP, ІНФОРМАЦІЙНІ СИСТЕМИ, КІНЦЕВІ ТОЧКИ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DLP	—	Data Loss Prevention;
SIEM	—	Security information and event management;
IAM	—	Identity and Access Management;
PGP	—	Pretty Good Privacy;
НСД	—	Несанкціонований доступ;
IoT	—	Internet of Things;
EDR	—	Endpoint Detection Response;
IAM	—	Identity and Access Management;
HIPAA	—	Health Insurance Portability and Accountability Act;
AD	—	Active Directory;
UEBA	—	User and Entity Behavior Analytics;
GDPR	—	General Data Protection Regulation.

ВСТУП

Актуальність дослідження. У сучасному світі інформаційні системи стають основою діяльності багатьох організацій, що призводить до зростання значущості питань інформаційної безпеки. Захист від несанкціонованого доступу до конфіденційної інформації набуває критичного значення, оскільки витік даних призводить до серйозних фінансових втрат, репутаційних збитків та юридичних наслідків. У зв'язку з цим, дослідження шляхів і розробка рекомендацій щодо захисту від несанкціонованого доступу до інформаційних систем з використанням технологій Data Loss Prevention (DLP) є надзвичайно актуальними.

DLP-системи надають комплексний підхід до захисту конфіденційної інформації, забезпечуючи ідентифікацію, моніторинг та контроль даних. Вони дозволяють не тільки виявляти спроби витоку даних, але й запобігати їм, що робить їх важливим інструментом для забезпечення інформаційної безпеки. В умовах постійного зростання кіберзагроз і розвитку технологій, впровадження DLP-систем стає необхідністю для сучасних організацій.

Актуальність дослідження обумовлена також необхідністю адаптації існуючих методів і технологій до специфічних вимог різних галузей та організацій. Різноманітність загроз вимагає розробки індивідуальних підходів і рекомендацій, які б враховували унікальні аспекти кожної організації. Крім того, постійний розвиток методів атак зумовлює потребу у вдосконаленні технологій захисту і підвищенні ефективності DLP-рішень.

Таким чином, дослідження шляхів і розробка рекомендацій щодо захисту від несанкціонованого доступу до інформаційних систем з використанням DLP є важливими для забезпечення безпеки даних, мінімізації ризиків витоку інформації та підтримки стабільної діяльності організацій в умовах зростаючих кіберзагроз.

Об’єкт дослідження – процес забезпечення захисту інформаційної системи від несанкціонованого доступу.

Предмет дослідження – методи та засоби захисту інформаційної системи від несанкціонованого доступу на основі DLP.

Мета роботи: розробити рекомендації щодо захисту від несанкціонованого доступу до інформаційної системи з використанням DLP.

Наукові завдання:

проаналізувати проблеми забезпечення безпеки організації від несанкціонованого доступу;

дослідити методи та засоби захисту від несанкціонованого доступу;

розробити рекомендації щодо захисту від несанкціонованого доступу до інформаційної системи з використанням DLP.

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

Практичне значення одержаних результатів: розроблено рекомендації щодо захисту від несанкціонованого доступу до інформаційної системи з використанням DLP, а також рекомендації фахівцям з кібербезпеки щодо їх впровадження.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОРГАНІЗАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

1.1. Основні загрози інформаційним системам

Інформаційна безпека є ключовим аспектом сучасного цифрового світу, адже від неї залежить збереження конфіденційності, цілісності та доступності інформації. Інформаційні системи стикаються з різноманітними загрозами, які можуть призвести до витоку даних, їхньої модифікації або знищення.

Загроза (англ. threat) — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають атакою [1].

Кіберзагроза [1] — наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам держави у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Загроза інформаційній безпеці (англ. information security threat) — сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері.

Основні загрози інформаційній безпеці можна розділити на три групи:

— загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

— загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);

— загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі, гідності і т. ін.).

10 основних типів загроз інформаційній безпеці для IT-команд

1. Внутрішні загрози

Внутрішня загроза виникає, коли люди, близькі до організації, які мають дозвіл на доступ до її мережі, навмисно чи ненавмисно зловживають цим доступом, щоб негативно вплинути на критично важливі дані або системи організації.

Недбалі працівники, які не дотримуються бізнес-правил і політики своєї організації, спричиняють внутрішні загрози. Наприклад, вони можуть ненавмисно надсилати електронною поштою дані клієнтів стороннім особам, відкривати фішингові посилання в електронних листах або ділитися своєю реєстраційною інформацією з іншими. Підрядники, ділові партнери та сторонні постачальники є джерелом інших внутрішніх загроз [2].

Деякі інсайдери навмисно обходять заходи безпеки через зручність або необдумані спроби підвищити продуктивність. Зловмисники навмисно ухиляються від протоколів кібербезпеки, щоб видалити дані, викрасти дані для подальшого продажу чи використання, порушити роботу чи іншим чином завдати шкоди бізнесу.

2. Віруси та черв'яки

Віруси та черв'яки (хробаки) — це зловмисне програмне забезпечення, спрямоване на знищення систем, даних і мережі організації. Комп'ютерний вірус — це зловмисний код, який розмножується шляхом копіювання в іншу програму, систему або файл хоста. Він залишається неактивним, доки хтось свідомо чи ненавмисно не активує його, поширюючи інфекцію без відома чи дозволу користувача чи системної адміністрації.

Комп'ютерний черв'як (хробак) [1, 2] – це програма, що самовідтворюється, і для поширення не потрібно копіювати себе в програму-хост або взаємодії людини. Його основною функцією є зараження інших комп'ютерів, залишаючись активним у зараженій системі. Хробаки часто поширюються за допомогою частин ОС, які є автоматичними та невидимими для користувача. Як тільки хробак потрапляє в систему, він негайно починає розмножуватися, заражаючи комп'ютери та мережі, які не захищені належним чином.

3. Ботнети

Ботнет – це набір пристроїв, підключених до Інтернету, включаючи ПК, мобільні пристрої, сервери та пристрої Інтернету речей (IoT), які заражені та дистанційно керовані звичайним типом зловмисного програмного забезпечення.

Як правило, зловмисне програмне забезпечення ботнету шукає вразливі пристрої в Інтернеті. Мета зловмисника, який створює ботнет, полягає в тому, щоб заразити якомога більше підключених пристроїв, використовуючи обчислювальну потужність і ресурси цих пристроїв для автоматизованих завдань, які зазвичай залишаються прихованими для користувачів.

Зловмисники, часто кіберзлочинці, які контролюють ці бот-мережі, використовують їх для надсилання спаму електронною поштою, участі в кампаніях шахрайства з кліками та створення зловмисного трафіку для розподілених атак на відмову в обслуговуванні.

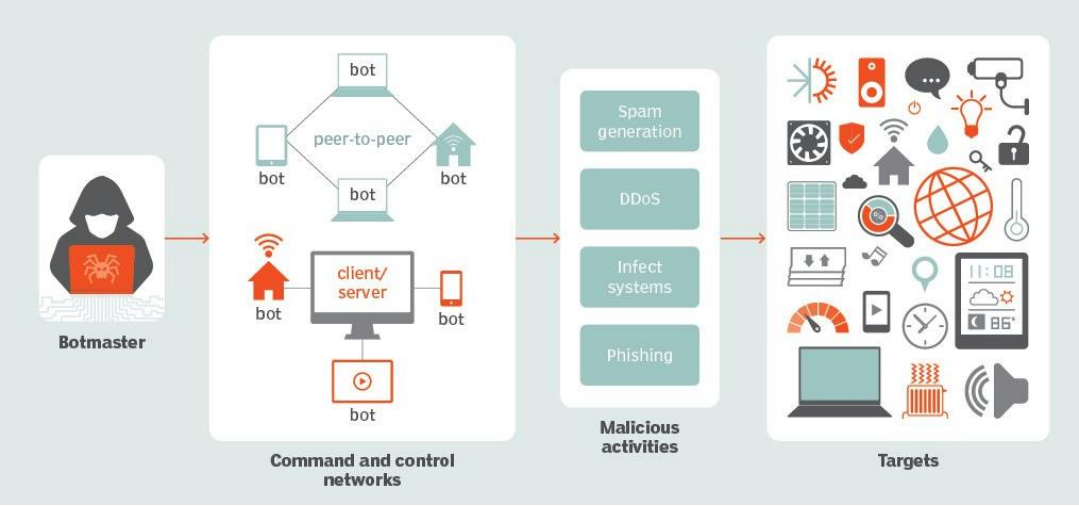


Рис. 1.1. Архітектура ботнету

4. Атаки завантажень (Drive-by Download)

Під час атаки Drive-by Download шкідливий код завантажується з веб-сайту через браузер в програму чи інтегровану ОС без дозволу або відома користувача. Користувачеві не потрібно нічого натискати, щоб активувати завантаження. Завантаження може розпочатися лише під час доступу або перегляду веб-сайту [2].

Кіберзлочинці можуть використовувати миттєві завантаження для впровадження банківських троянів, крадіжки та збору особистої інформації, а

також впровадження наборів експлойтів або іншого зловмисного програмного забезпечення в кінцеві точки.

5. Фішингові атаки

Фішингові атаки – це тип загроз інформаційній безпеці, який використовує соціальну інженерію, щоб обманом змусити користувачів порушити звичайні методи безпеки та надати конфіденційну інформацію, зокрема імена, адреси, облікові дані для входу, номери соціального страхування, дані кредитних карток та іншу фінансову інформацію [2].

У більшості випадків хакери надсилають підроблені електронні листи, які виглядають так, ніби вони надходять із законних джерел, таких як фінансові установи, eBay, PayPal, і навіть друзів і колег.

Під час фішингових атак хакери намагаються змусити користувачів виконати певні рекомендовані дії, наприклад натиснути посилання в електронних листах, які спрямовують їх на шахрайські веб-сайти, які запитують особисту інформацію або встановлюють шкідливе програмне забезпечення на їхні пристрої. Відкриття вкладень у електронних листах також може встановлювати на пристрої користувачів зловмисне програмне забезпечення, призначене для збору конфіденційної інформації, надсилання електронних листів їхнім контактам або надання віддаленого доступу до їхніх пристроїв.

6. Розподілені атаки на відмову в обслуговуванні

У розподіленій атаці типу «відмова в обслуговуванні» (DDoS) кілька скомпрометованих машин атакують ціль, наприклад сервер, веб-сайт або інший мережевий ресурс, роблячи ціль повністю непрацездатною. Потік запитів на з’єднання, вхідних повідомлень або неправильно сформованих пакетів змушує цільову систему сповільнюватися або виходити з ладу та вимикатися, відмовляючи в обслуговуванні законним користувачам або системам [2].

7. Програми-вимагачі

Під час атаки програм-вимагачів комп’ютер жертви блокується, зазвичай за допомогою шифрування, що не дозволяє жертві використовувати пристрій або дані, які на ньому зберігаються. Щоб відновити доступ до пристрою чи даних,

жертва має заплатити хакеру викуп, як правило, у віртуальній валюті, такій як біткойн. Програми-вимагачі можуть поширюватися через шкідливі вкладення електронної пошти, заражені програмні застосунки, заражені зовнішні пристрої зберігання даних і скомпрометовані веб-сайти.

8. Набори експлойтів

Набір експлойтів — це інструмент програмування, який дозволяє людині без досвіду написання програмного коду створювати, налаштовувати та поширювати зловмисне програмне забезпечення. Набори експлойтів відомі під різними назвами, зокрема набір для зараження, набір для злочинного програмного забезпечення, набір для атаки своїми руками та набір інструментів для зловмисного програмного забезпечення. Кіберзлочинці використовують ці набори інструментів для атаки на вразливі місця системи, щоб поширювати зловмисне програмне забезпечення або брати участь у інших зловмисних діях, таких як викрадення корпоративних даних, запуск атак на відмову в обслуговуванні або створення ботнетів [2].

9. Розширені постійні атаки загроз

Розширена постійна загроза (APT - Advanced persistent threat attacks) — це цілеспрямована кібератака, під час якої неавторизований зловмисник проникає в мережу та залишається непоміченим протягом тривалого періоду часу. Замість того, щоб завдати шкоди системі чи мережі, ціллю APT-атаки є моніторинг мережевої активності та викрадення інформації для отримання доступу, включаючи набори експлойтів і зловмисне програмне забезпечення.

Кіберзлочинці зазвичай використовують APT-атаки, щоб націлитися на цільові цілі, такі як великі підприємства та національні держави, крадучи дані протягом тривалого періоду.

10. Шкідлива реклама

Шкідлива реклама – це техніка, яку використовують кіберзлочинці для введення шкідливого коду в законні мережі онлайн-реклами та веб-сторінки. Цей код зазвичай перенаправляє користувачів на шкідливі веб-сайти або встановлює зловмисне програмне забезпечення на їхні комп’ютери чи мобільні пристрої. Комп’ютери користувачів можуть заразитися, навіть якщо вони нічого не клацнуть, щоб почати завантаження.

Кіберзлочинці можуть використовувати зловмисну рекламу для розгортання різноманітних зловмисних програм, які заробляють гроші, зокрема сценаріїв для майнінгу криптовалют, програм-вимагачів і банківських троянів.

Деякі веб-сайти відомих компаній, зокрема Spotify, The New York Times і Лондонська фондова біржа, ненавмисно відображали шкідливу рекламу, піддаючи користувачів ризику.

1.2. Важливість захисту від несанкціонованого доступу

Несанкціонований доступ до інформаційних систем може мати катастрофічні наслідки для організацій.

Несанкціонований доступ — отримання доступу до комп'ютерної системи або вчинення дій, які призводять до одержання доступу до інформації особою, яка не має прав на перегляд та/або модифікацію цієї інформації без дозволу керівництва або уповноважених ним осіб. (Постанова "Про затвердження Положення про захист інформації та кіберзахист у платіжних системах" від 19.05.2021 N 43).

Дедалі більш поширена загроза несанкціонованого доступу викликає серйозні занепокоєння щодо безпеки даних, конфіденційності та цілісності цифрових систем. Це становить значний ризик для окремих осіб, корпорацій і урядів.

Ризики та наслідки несанкціонованого доступу:

Крадіжка або знищення особистих даних

Коли неавторизовані особи отримують доступ до системи, вони часто націлюються на конфіденційні дані, такі як фінансові записи, особиста ідентифікаційна інформація, комерційна таємниця або інтелектуальна власність. Це вторгнення може призвести до значних фінансових втрат, шкоди репутації компанії та потенційних юридичних наслідків [2, 3].

Крім того, у деяких випадках зловмисник може не тільки викрасти дані, але й пошкодити, знищити або зашифрувати їх. Цей акт саботажу може завдати катастрофічної шкоди, особливо для підприємств, які значною мірою покладаються на їхні дані. Вплив таких випадків може бути руйнівним, від руйнування бізнес-операцій до значної втрати довіри серед клієнтів.

Крім того, викрадення або знищення особистої інформації також може мати серйозні наслідки для окремих осіб. Від крадіжки особистих даних до фінансового шахрайства особисті наслідки можуть бути тривалими, і їх важко одужати.

Крадіжка грошей або товарів через шахрайство

Ще один серйозний ризик, пов’язаний із неавторизованим доступом – це можливість шахрайства. Маючи доступ до конфіденційних даних, кіберзлочинці можуть здійснювати різноманітні шахрайські дії. Це шахрайство з кредитними картками, маніпуляції з банківськими рахунками або навіть створення фальшивого бізнесу.

Несанкціонований доступ дозволяє злочинцям вчиняти ці шахрайські дії, надаючи їм необхідну інформацію або доступ до фінансових ресурсів. Наприклад, вони використовують викрадену інформацію кредитної картки для незаконних покупок або маніпулювати банківськими системами для незаконного перенаправлення коштів.

Саботаж або псування організаційних систем

У деяких випадках неавторизований доступ використовується для саботажу організаційних систем або пошкодження веб-сайтів. Це порушення

функціонування мережі, впровадження зловмисного коду на веб-сайт або навіть взяття під контроль системи, викликаючи хаос і збої.

Ці дії завдають значної шкоди бізнесу. Вони не тільки призводять до фінансових втрат, але й псують репутацію компанії, що призводить до втрати довіри серед клієнтів [2, 3].

Фізичні пошкодження

Несанкціонований доступ також призводить до фізичних пошкоджень. Наприклад, якщо хакер отримує контроль над промисловою системою керування, він спричинює збій у роботі обладнання, що призводить до потенційних аварій або пошкодження обладнання.

Цей ризик особливо гострий у таких галузях, як виробництво, енергетика чи транспорт, де несправність обладнання призводить до значної загрози безпеці. Це підкреслює важливість надійних заходів безпеки не лише для захисту даних, але й для забезпечення фізичної безпеки працівників та інфраструктури.

1.3. Аналіз причин несанкціонованого доступу

Погано реалізована автентифікація

Одним із найпоширеніших способів несанкціонованого доступу є неправильно реалізовані процеси автентифікації. Автентифікація — це захід безпеки, який використовується для перевірки особи або пристрою, які намагаються отримати доступ до системи. Якщо процес автентифікації погано розроблений, реалізований або неправильно налаштований, неавторизованим особам стає легко обійти його та отримати доступ до системи.

Наприклад, коли система не блокує користувача після певної кількості невдалих спроб входу, вона залишає двері відкритими для атаки грубою силою, коли зловмисник намагається використовувати різні комбінації паролів, доки не знайде правильний.

Іншим прикладом погано реалізованої автентифікації є те, що система не вимагає регулярної зміни пароля. У такій ситуації неавторизована особа, якій вдається отримати дійсний пароль, продовжує використовувати його протягом тривалого періоду, не будучи виявленим.

Фішингові атаки

Одним із найпоширеніших способів несанкціонованого доступу є фішингові атаки. Це передбачає надсилання оманливих електронних листів або повідомлень, які обманом змушують одержувачів розкрити свої облікові дані або натиснути зловмисні посилання. Як тільки одержувач переходить за посиланням, зловмисник може отримати доступ до його облікових записів або заразити його системи шкідливим програмним забезпеченням.

Фішингові атаки особливо ефективні, оскільки вони використовують людські вразливості, а не технологічні. Представляючи себе надійною організацією, зловмисники маніпулюють особами, щоб ті мимоволі надали їм доступ. Це підкреслює важливість обізнаності та навчання з кібербезпеки як основного захисту від несанкціонованого доступу [2, 3].

Атаки на паролі

Іншим поширеним методом отримання несанкціонованого доступу є атаки на паролі. Це спроби вгадати або зламати пароль користувача за допомогою різних методів. Вони включають атаки грубої сили, коли пробуються всі можливі комбінації паролів, або атаки за словником, коли використовуються загальні слова чи фрази.

Атаки на паролі підкреслюють важливість надійних унікальних паролів як фундаментального рівня безпеки. Використання комбінації літер, цифр і символів, а також уникнення загальних слів або фраз може ускладнити зловмисникам вгадування вашого пароля.

Використання вразливостей програмного забезпечення

Неавторизований доступ також може статися через використання вразливостей програмного забезпечення. Це недоліки або слабкі сторони

програмного забезпечення, які використовують для отримання несанкціонованого доступу або виконання інших зловмисних дій.

Уразливість програмного забезпечення виникає з різних причин, наприклад, помилки кодування або застаріле програмне забезпечення. Зловмисники часто використовують ці вразливості для проникнення в системи, підкреслюючи важливість регулярних оновлень програмного забезпечення та виправлень як ключової частини кібербезпеки.

Внутрішні загрози

Іншим поширеним джерелом несанкціонованого доступу є внутрішні загрози. Інсайдерські загрози стосуються загроз безпеці, які походять зсередини організації, часто від співробітників, колишніх співробітників, підрядників або ділових партнерів, які мають законний доступ до мереж, систем або даних організації [2, 3].

Інсайдерські загрози можуть бути навмисними або ненавмисними. Навмисна внутрішня загроза виникає, коли особа з законним доступом навмисно зловживає ним, щоб завдати шкоди організації. Це може бути з таких причин, як шпигунство, особиста вигода чи помста. З іншого боку, ненавмисна внутрішня загроза виникає, коли особа ненавмисно спричиняє порушення безпеки , часто через недбалість або недостатню обізнаність.

Висновки до розділу 1

Отже, в розділі було проаналізовано загрози інформаційній системі, поняття НСД. Важливість захисту від несанкціонованого доступу його ризики на інформаційну систему організації та конфіденційних даних.

Проаналізовані основні причини несанкціонованого доступу та їх наслідки для організації.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

2.1. Дослідження сучасних методів захисту

Блокування несанкціонованого доступу відіграє основну роль у запобіганні витоку даних. Однак надійна програма безпеки використовує «поглиблений захист» – кілька рівнів захисту безпеки, намагаючись пом’якшити атаки задовго до того, як зловмисники досягнуть чутливої системи. Додаткові рівні безпеки включають захист мережі, захист кінцевої точки та захист даних.

Типове порушення безпеки відбувається в три етапи:

Дослідження — зловмисник шукає слабкі місця або вразливі місця в організаційних системах, людях або процесах.

Мережева/соціальна атака — зловмисник намагається проникнути на периметр мережі, уникаючи захисту мережі або використовуючи соціальну інженерію, щоб обманом змусити людей надати доступ, дані чи облікові дані.

Ексфільтрація — як тільки зловмиснику вдається отримати доступ, він може викрасти цінні активи або завдати шкоди в точці входу, а також виконати бічний рух, щоб отримати доступ до додаткових, більш цінних систем [2-5].

Негайні ризики безпеці через неавторизований доступ

Отримавши несанкціонований доступ до організаційних систем або облікових записів користувачів, зловмисники можуть:

— викрасти або знищити особисті дані;

— крадіжка грошей або товарів шляхом шахрайства;

— крадіжка ідентифікаторів користувачів;

— компрометація системи та використання її для нелегітимної чи злочинної діяльності;

— саботувати організаційні системи або псувати веб-сайти;

— заподіяти фізичні збитки – отримавши доступ до підключених пристроїв.

Довгострокові наслідки успішного порушення даних

— шкода репутації та довірі;

— порушення безперервності бізнесу;

— зниження фінансової оцінки або цін акцій;

— витрати на контроль збитків і розслідування порушень;

— штрафи, накладені урядом або стандартами безпеки;

— виплата збитків постраждалим сторонам;

Найкращих методи запобігання несанкціонованому доступу

1. Політика надійних паролів

Застосування найкращих практик для паролів користувачів — змусьте користувачів вибирати довгі паролі, включаючи літери, цифри та спеціальні символи, і часто змінювати паролі. Навчіть користувачів уникати використання фраз, які можна вгадати під час атаки грубою силою, інформуйте їх про регулярне оновлення паролів і скажіть їм уникати передачі паролів між системами [2-5]..

Просто встановити політику паролів може бути недостатньо. Розгляньте можливість використання інструментів, таких як керування корпоративними паролями або управління ідентифікацією та доступом (IAM), щоб централізовано керувати обліковими даними користувача та гарантувати, що вони відповідають найкращим практикам безпеки.

2. Двофакторна автентифікація (2FA) і багатофакторна автентифікація

Облікові дані, засновані на іменах користувачів, паролях, відповідях на питання безпеки тощо, відомі більш загально як фактори безпеки, але вони за своєю суттю слабкі, і їх легко скомпрометувати.

Один із найкращих способів запобігти несанкціонованому доступу у вашій організації – це доповнити фактори додатковими методами автентифікації:

Фактори володіння — аутентифікація за допомогою об’єктів, якими володіє користувач. Наприклад, мобільний телефон, маркер безпеки або фізична картка.

Фактори приналежності — автентифікація за допомогою чогось, чим є чи має користувач. Це включає біометричну автентифікацію за допомогою відбитків пальців, сканування райдужної оболонки ока або розпізнавання голосу.

3. Практики фізичної безпеки

Якою б важливою не була кібербезпека, не потрібно нехтувати фізичною безпекою. Навчіть користувачів завжди блокувати пристрої, коли відходять від своїх столів, і не записувати паролі та не залишати конфіденційні документи відкритими. Дотримуйтеся чіткої політики щодо замикання дверей офісу та переконайтеся, що лише уповноважені особи можуть входити в конфіденційні зони вашого фізичного приміщення.

4. Моніторинг активності користувача

Дуже важливо стежити за тим, що відбувається з обліковими записами користувачів, виявляти аномальну активність, наприклад багаторазові спроби входу, вхід у незвичайний час або вхід користувачів до систем або даних, до яких вони зазвичай не мають доступу. Існує кілька стратегій моніторингу користувачів і облікових записів [2-5].:

Аналіз журналів — аналітики безпеки можуть отримати доступ до журналів конфіденційних корпоративних систем і виявити підозрілу активність

Сповіщення на основі правил — інструменти безпеки сповіщають співробітників служби безпеки про шаблони підозрілої активності, такі як багаторазові спроби входу або неправильний вхід до конфіденційних систем

Поведінкова аналітика — поведінкова аналітика користувачів і подій (UEBA) відстежує користувачів і системи, встановлює базову лінію нормальної активності та виявляє будь-яку поведінку, яка представляє аномалію та може бути шкідливою.

5. Безпека кінцевої точки

Історично більшість порушень безпеки були результатом проникнення через периметр мережі. Сьогодні багато атак обходять захист мережі, націлюючись безпосередньо на кінцеві точки, такі як робочі станції співробітників, сервери, хмарні екземпляри. Встановлення антивіруса на кожній кінцевій точці є основним заходом безпеки.

Окрім антивірусної програми, багато організацій впроваджують комплексні заходи захисту кінцевих точок, які включають:

Антивірус нового покоління (NGAV) – здатний виявляти зловмисне програмне забезпечення та інші загрози, навіть якщо вони не відповідають відомим шаблонам або сигнатурам

Виявлення та реагування на кінцеву точку (EDR) – забезпечує видимість і захисні заходи на самій кінцевій точці, коли відбуваються атаки на кінцеві пристрої.

Захист від витоку даних (DLP) – забезпечує запобігання витоку конфіденційних файлів за межі мережі компанії.

2.2. Поняття, принципи та компоненти DLP

Data Loss Prevention (DLP) – це комплекс заходів, технологій та інструментів, спрямованих на запобігання витоку конфіденційної інформації з організації. DLP-системи дозволяють виявляти, моніторити та захищати чутливі дані, забезпечуючи їх безпеку незалежно від того, де вони знаходяться – на пристроях, у мережі чи в хмарних сховищах. Основна мета DLP – забезпечити контроль над даними, мінімізуючи ризик їхнього витоку або несанкціонованого доступу [4].

Принципи роботи DLP

1. Ідентифікація та класифікація даних:

DLP-системи використовують різні методи для ідентифікації та класифікації чутливих даних, такі як вміст файлів, метадані, шаблони та регулярні вирази. Це дозволяє визначити, які дані є конфіденційними і потребують особливого захисту.

2. Моніторинг та контроль:

DLP-системи постійно моніторять всі дії з даними, включаючи їх передачу по мережі, копіювання на зовнішні носії або завантаження в хмарні сервіси. Система вміє автоматично блокувати або сповіщати про підозрілі дії, які можуть призвести до витоку даних.

3. Впровадження політик безпеки:

Організації визначають політики безпеки, що регламентують, як чутливі дані використовуються та передаються. DLP-системи забезпечують дотримання цих політик шляхом застосування відповідних заходів контролю та обмежень.

4. Звітування та аналітика:

DLP-системи генерують звіти та надають аналітичні дані щодо інцидентів безпеки, що дозволяє організаціям проводити розслідування та коригувати політики для підвищення ефективності захисту.

Основні компоненти DLP-систем

1. Агентська частина:

DLP-агенти встановлюються на кінцевих пристроях (комп'ютери, мобільні пристрої) і забезпечують моніторинг та контроль дій користувачів з чутливими даними. Вони відстежують операції копіювання, передачі та зміни даних, а також можуть застосовувати політики блокування або шифрування.

2. Мережева частина:

Цей компонент забезпечує моніторинг та контроль передачі даних по мережі. Мережева DLP-система аналізує трафік, виявляючи чутливі дані, що передаються через електронну пошту, веб-запити, FTP та інші мережеві протоколи. Вона здатна блокувати або перехоплювати підозрілі передачі даних [4].

3. Центральний сервер управління:

Це головний компонент DLP-системи, який забезпечує централізоване управління політиками безпеки, збір даних від агентів та мережевих компонентів, аналіз інцидентів та генерацію звітів. Центральний сервер дозволяє адміністраторам налаштовувати правила, моніторити активність та реагувати на загрози.

4. Системи зберігання даних:

DLP-системи включають засоби для захисту даних, що зберігаються на серверах, у базах даних та в хмарних сховищах. Вони забезпечують шифрування, контроль доступу та моніторинг дій з даними, запобігаючи несанкціонованому доступу або витоку.

2.3. Архітектура та функціонал DLP-системи

Safetica ONE — це універсальне рішення для запобігання втратам даних та захисту від несанкціонованого доступу та 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, дає можливість отримувати інформацію про інциденти безпеки за допомогою миттєвих сповіщень та детальних звітів. Safetica ONE проста у розгортанні та доступна для підприємств будь-якого розміру[5-8].

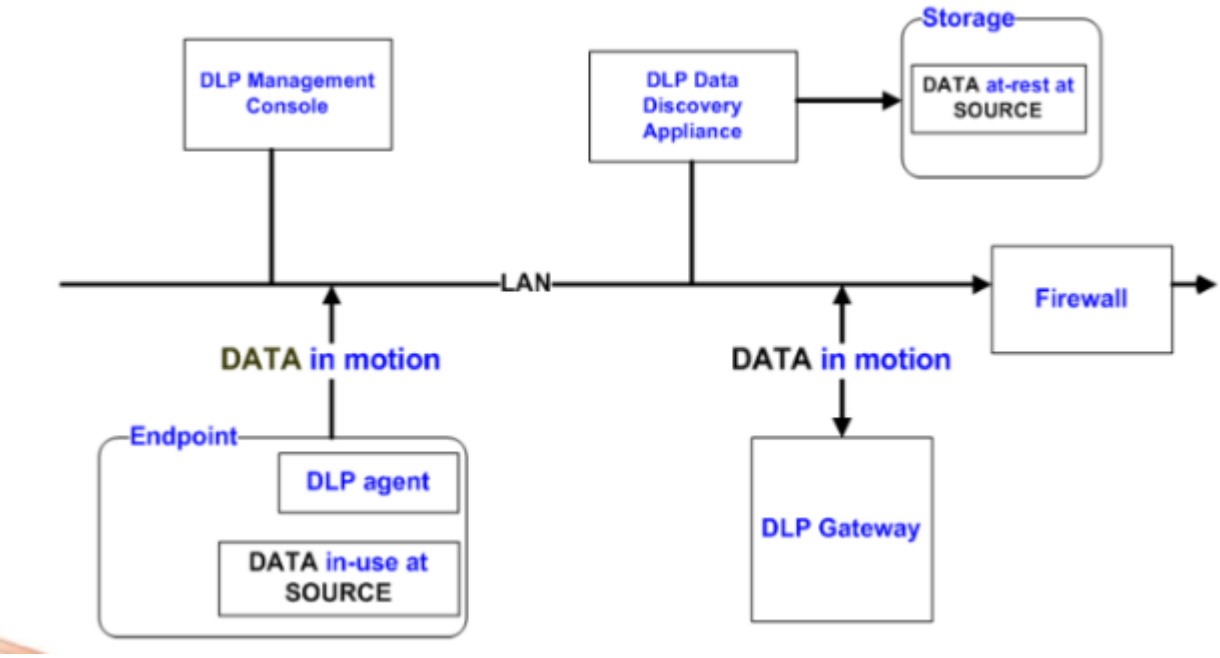


Рис. 2.1. Типова архітектура DLP системи [8]

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

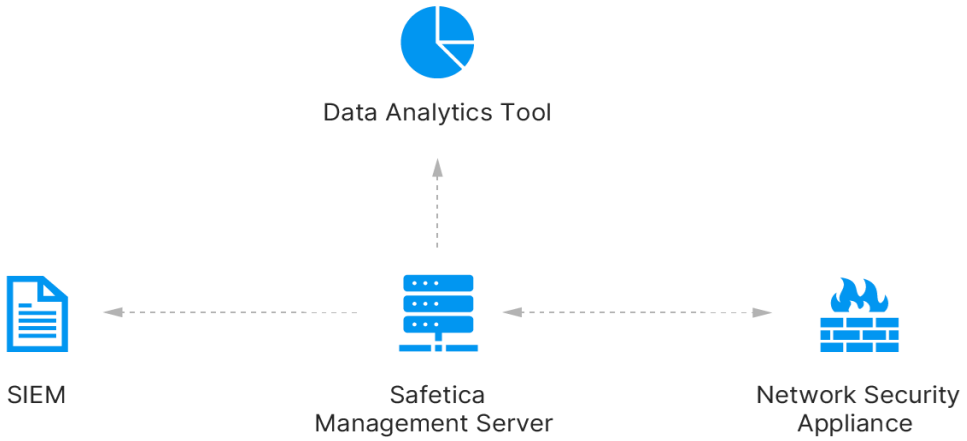


Рис.2.2. Схема надсилання звітів Safetica

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

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

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

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

Контролює корпоративні мобільні пристрої та відстежує дані, переміщені з

хмарного середовища Office 365 (рис.2.3).

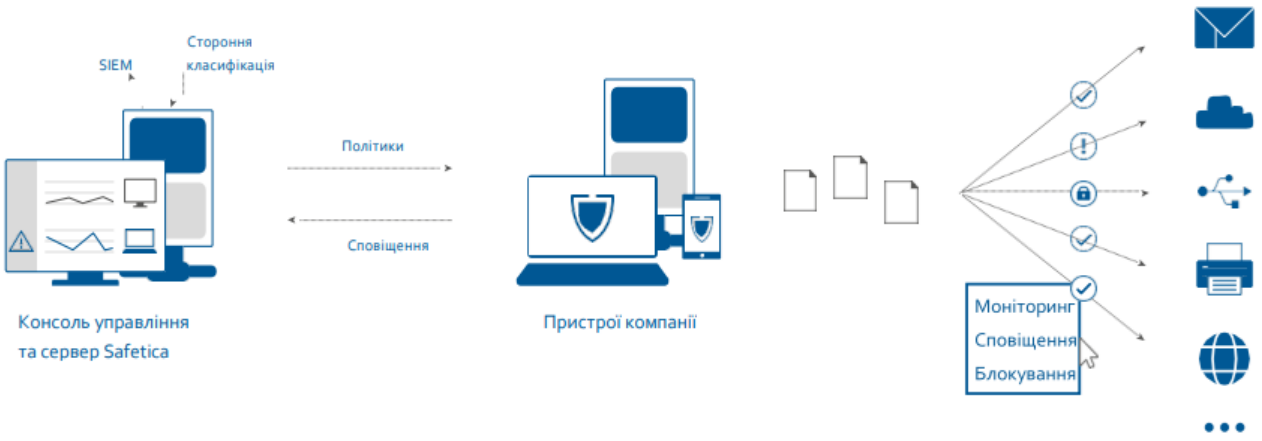


Рис.2.3. Схема роботи Safetica

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

Safetica захищає усі конфіденційні дані, перш ніж вони опиняться за межами компанії, незалежно від того, де вони зберігаються та як переміщуються (рис.2.4). Забезпечує швидкий та легкий для розуміння огляд усіх можливих загроз з єдиної консолі.

При правильному впровадженні даної системи, можливо домогтися повного захисту від витоку даних та несанкціонованого доступу. Також, система допомагає у проведенні аудиту для визначення конфіденційної інформації в організації.

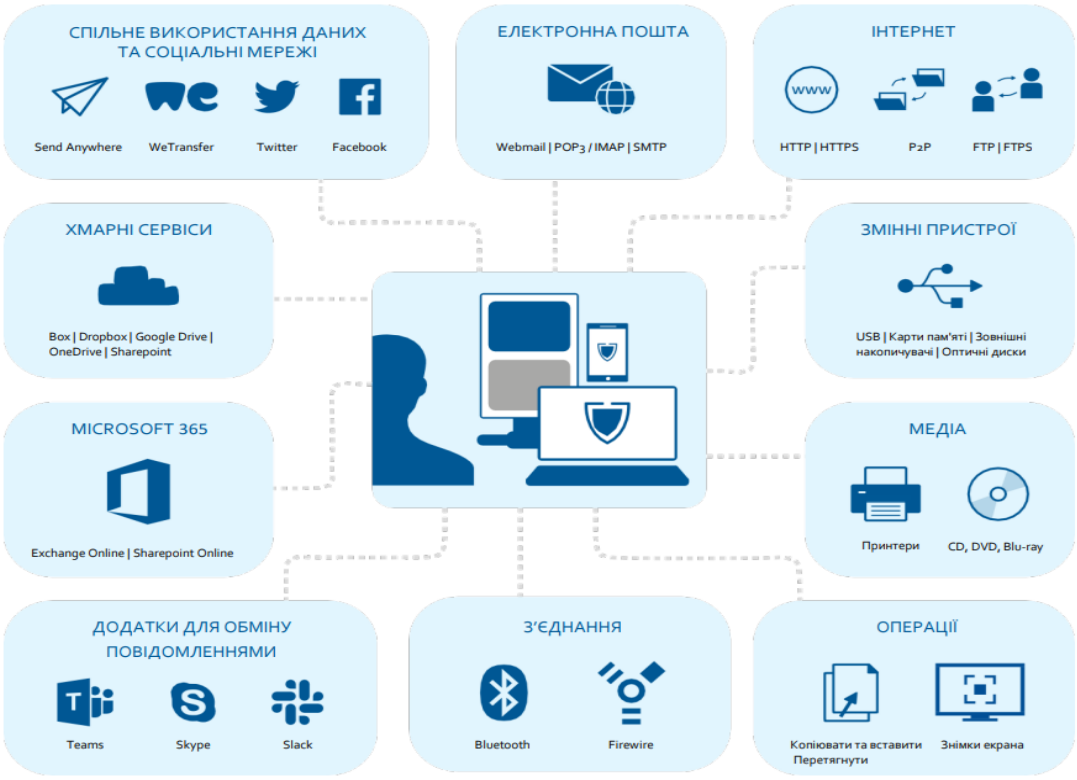


Рис.2.4. Канали переміщення інформації, з якими працює Safetica

На рис. 2.5 проілюстровано архітектуру DLP Safetica ONE де:

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

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

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

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

Рис. 2.5. Архітектура рішення Safetica ONE

Управління усіма функціями та компонентами Safetica (клієнтами, серверами, базами даних) здійснюється за допомогою веб- або настільної консолі. У ній також відображаються дані моніторингу, статистична інформація та графіки.

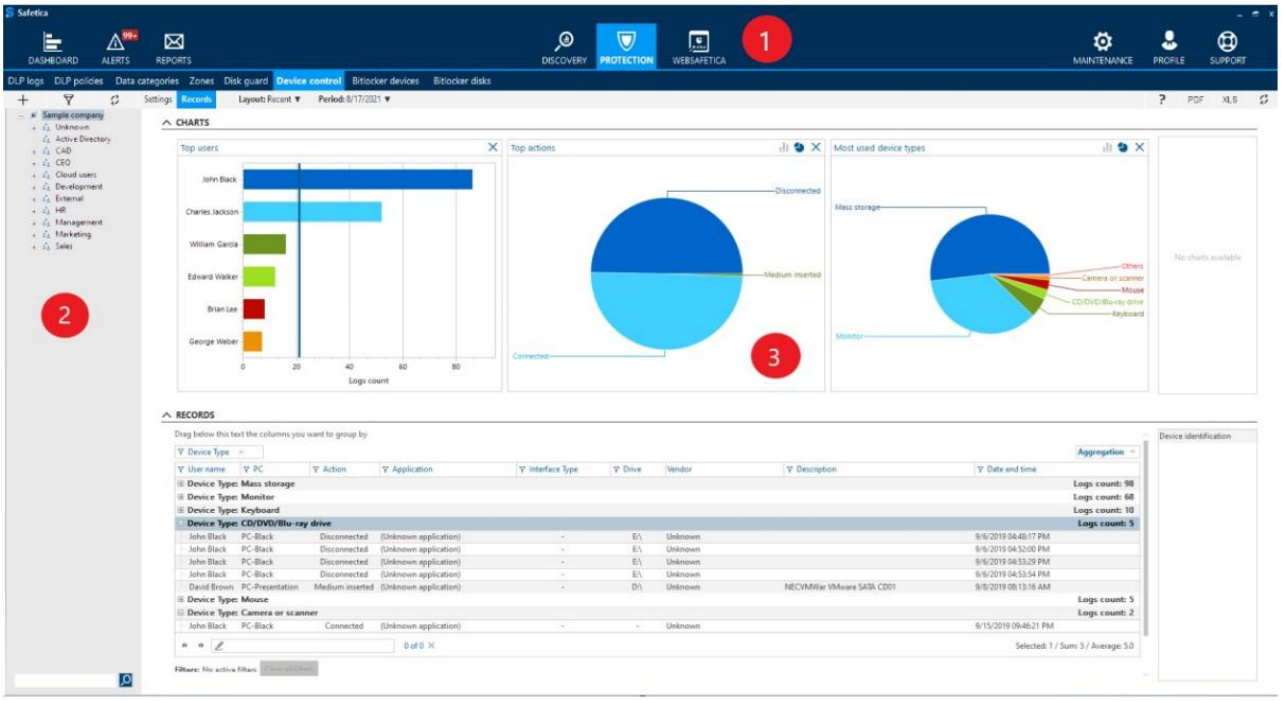


Рис. 2.6. Інтерфейс консолі управління

1. Головне меню

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

Discovery використовується лише режим Записів:

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

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

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

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

• Сповіщення (Alerts) — автоматичне налаштування сповіщень.

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

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

• Discovery;

• Protection;

• WebSafetica.

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

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

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

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

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

2. Дерево користувачів

Дерево користувачів знаходиться на лівій стороні консолі під верхньою панеллю інструментів. Всі сервіси Safetica, з якими ви з'єднані, відображаються в дереві. Нове підключення до сервера можна налаштувати в розділі Профіль (Profile). Кожен сервер в дереві містить користувачів та комп'ютери, які до нього підключені. Вибрані елементи у дереві, параметри або дані, отримані за допомогою відповідних функцій, відображаються в області відображення або перегляду (розділ 3 на малюнку).

3. Область відображення (перегляду)

Область відображення або область перегляду використовується для візуалізації даних та налаштування окремих функцій. Зміст області перегляду змінюється залежно від функції, яку переглядають та поточного режиму (налаштування або записів). Щоб переключитися між окремими функціями, потрібно натиснути на один з модулів у головному меню, а потім обрати необхідну функцію[8-11].

Висновки до розділу 2

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

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ З ВИКОРИСТАННЯМ DLP

3.1. Налаштування та встановлення DLP та її компонентів

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

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

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

Інсталяція вручну:

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

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

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

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

5. Інсталювати агент на робочі станції.

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

Після розгортання всіх компонентів та перевірки правильності встановлення, можна почати роботу з Safetica[11-16].

Автоматична інсталяція

Детально розглянемо лише Автоматичну інсталяцію, яка встановлює серверний компонент, адміністративні консолі, включаючи WebSafetica, IIS вебсервер і сервер баз даних Microsoft SQL Server Express на поточному комп'ютері. Клієнти встановлюються під час першого запуску Safetica після інсталяції. Необхідно переконатися, що комп'ютер має достатню обчислювальну потужність для роботи з базою даних, сервером, а також WebSafetica (Детальні умови стосовно вимог див. Install Manual на офіційному сайті Safetica One [11-16]).

Після запуску універсального інсталятора Safetica необхідно виконати наступні дії:

1. Обрати мову інсталятора (рис.3.1).

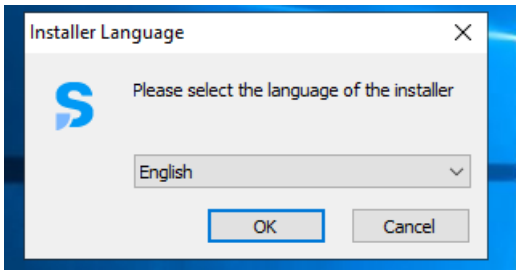


Рис. 3.1. Вікно вибору мови інсталятора

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

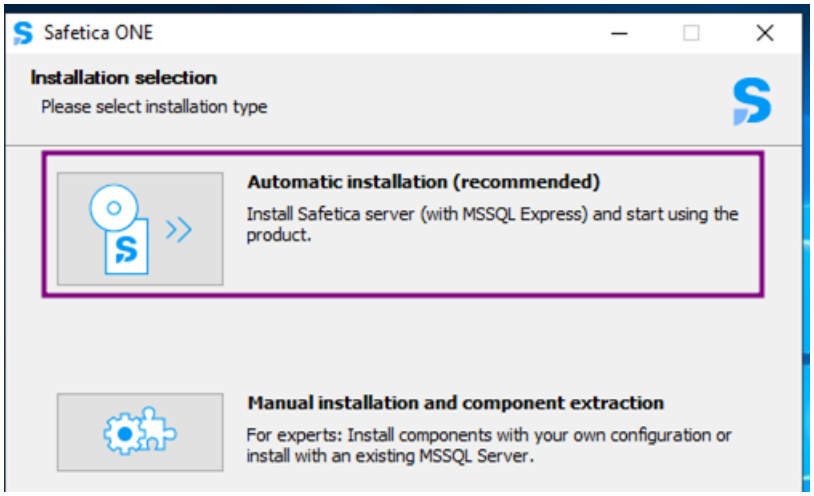


Рис. 3.2. Вікно вибору Автоматичної інсталяції

3. Натиснути «Далі», щоб підтвердити, що обране середовище відповідає вимогам до апаратного забезпечення (рис.3.3).

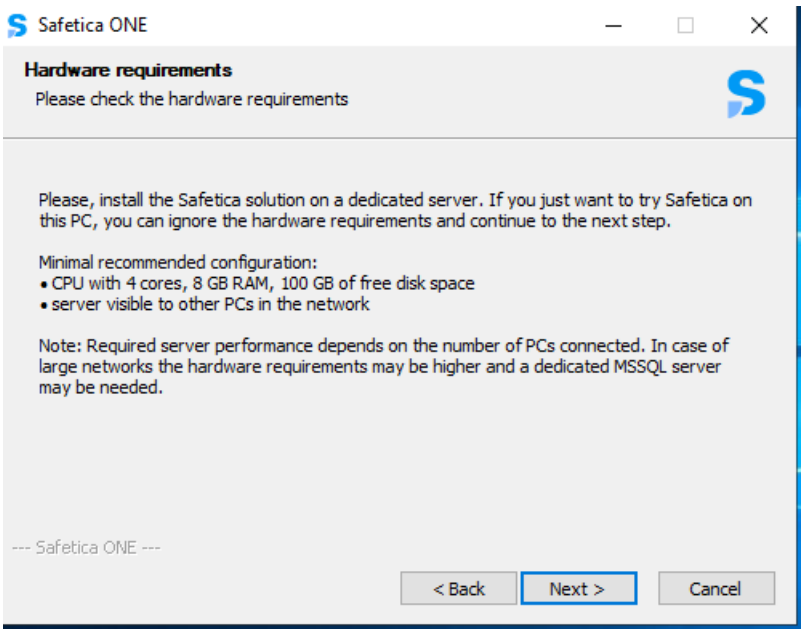


Рис. 3.3. Вимоги апаратного забезпечення

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

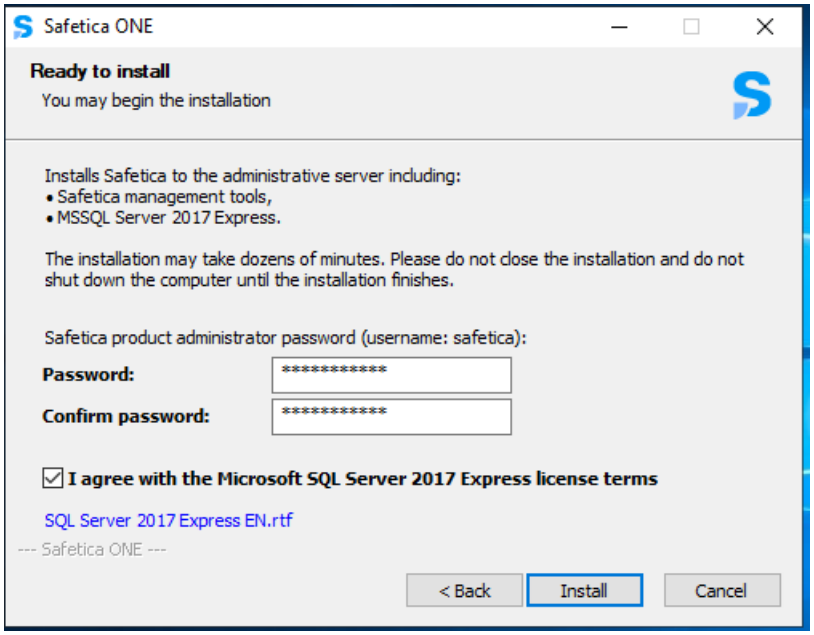


Рис. 3.4. Вікно створення паролю адміністратора

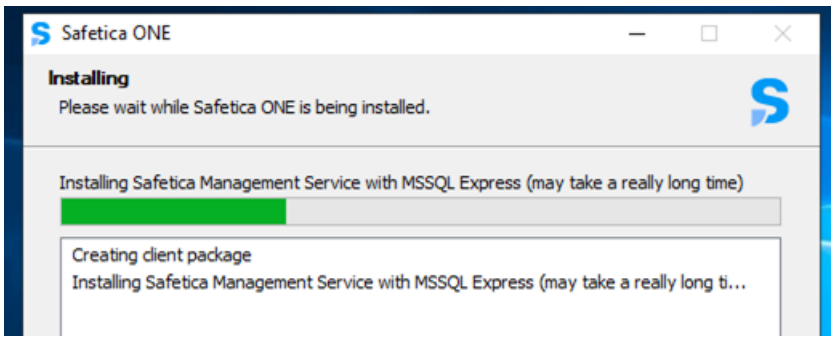


Рис. 3.5. Вікно встановлення Safetica Management Service

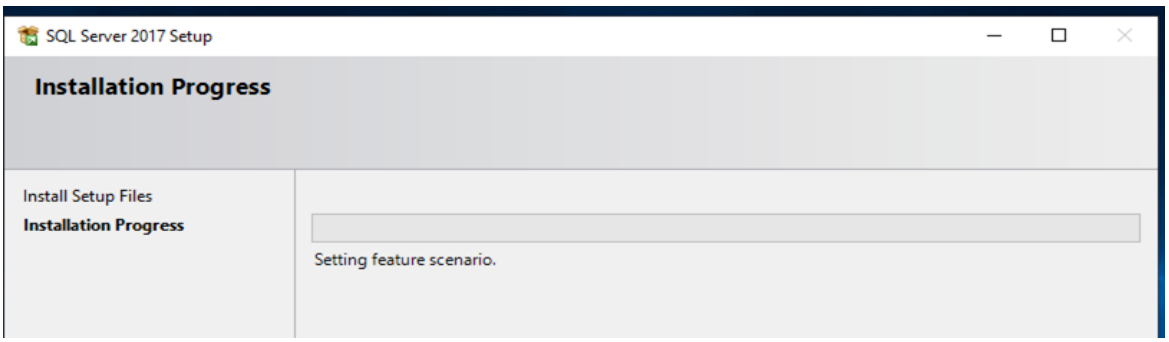


Рис. 3.6. Вікно встановлення SQL Server

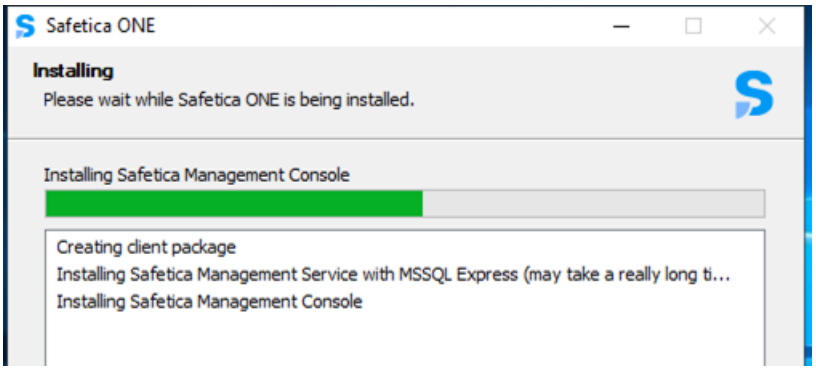


Рис. 3.7. Вікно встановлення Safetica Management Console

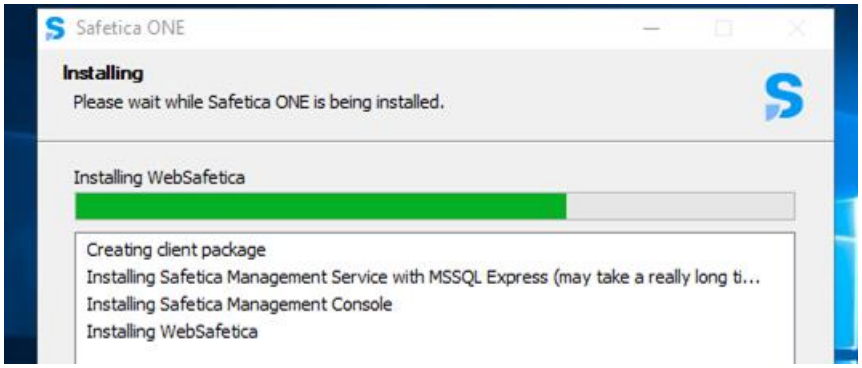


Рис. 3.8. Вікно встановлення WebSafetica

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

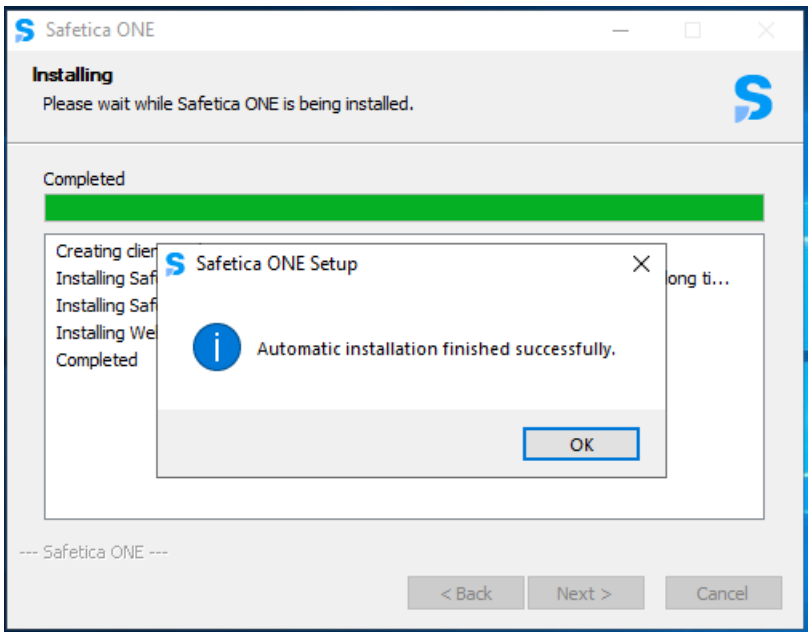


Рис. 3.9. Вікно підтвердження інсталяції

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

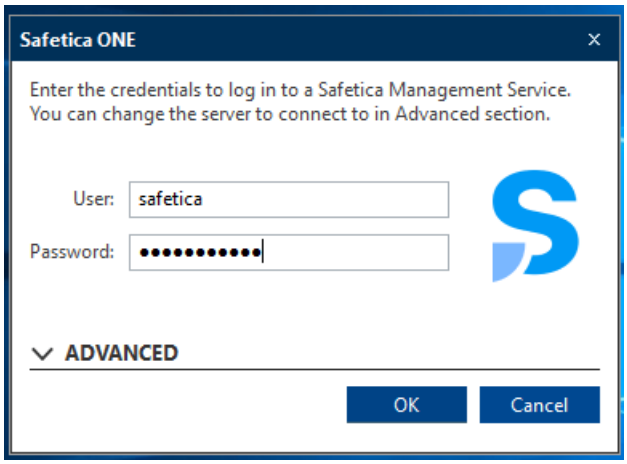


Рис. 3.10. Вікно входу в консоль управління

7. Після запуску консолі управління Safetica відкриється майстер початкового налаштування. Під час другого етапу можна додати сервер SMTP-сервер, на який Safetica буде надсилати сповіщення та звіти. Можна пропустити дане налаштування

і вказати дані пізніше (рис.3.11).

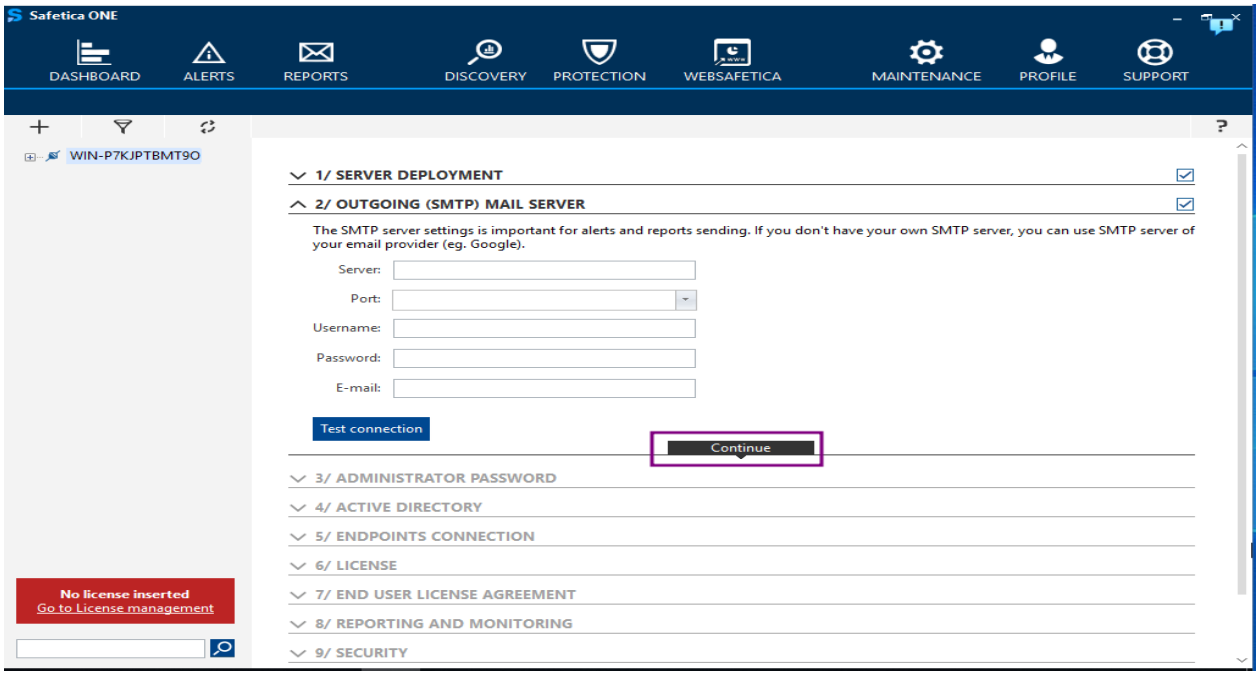


Рис. 3.11. Вікно налаштування підключення до поштового серверу

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

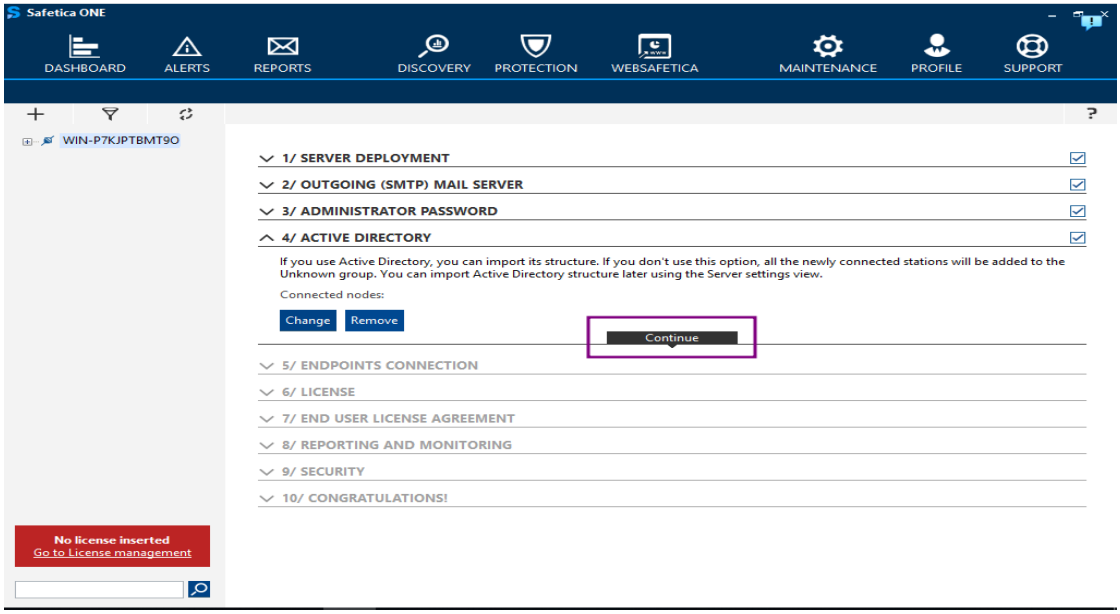


Рис. 3.12. Вікно налаштування підключення до Active Directory

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

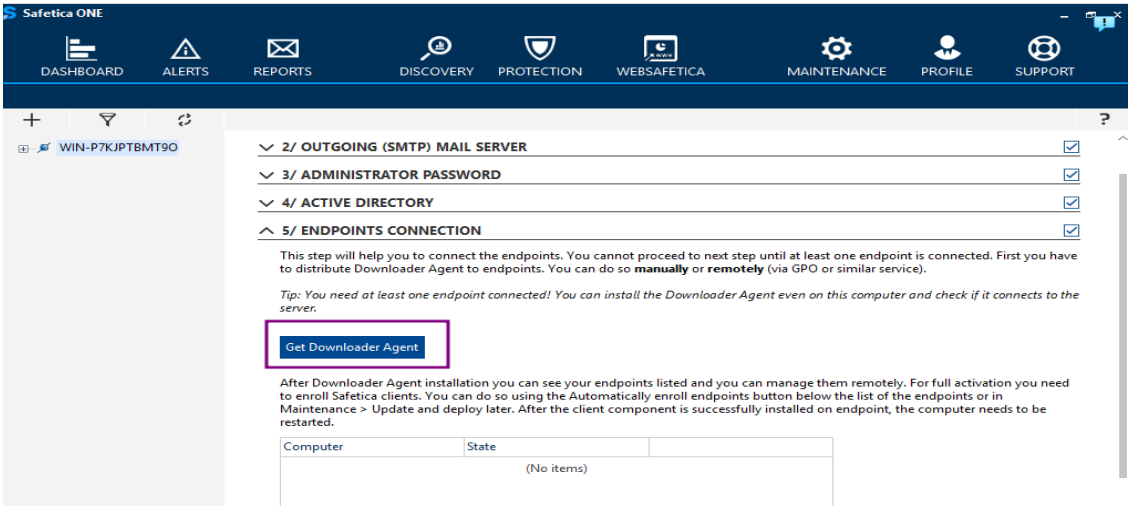


Рис. 3.13. Вікно для завантаження агента

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

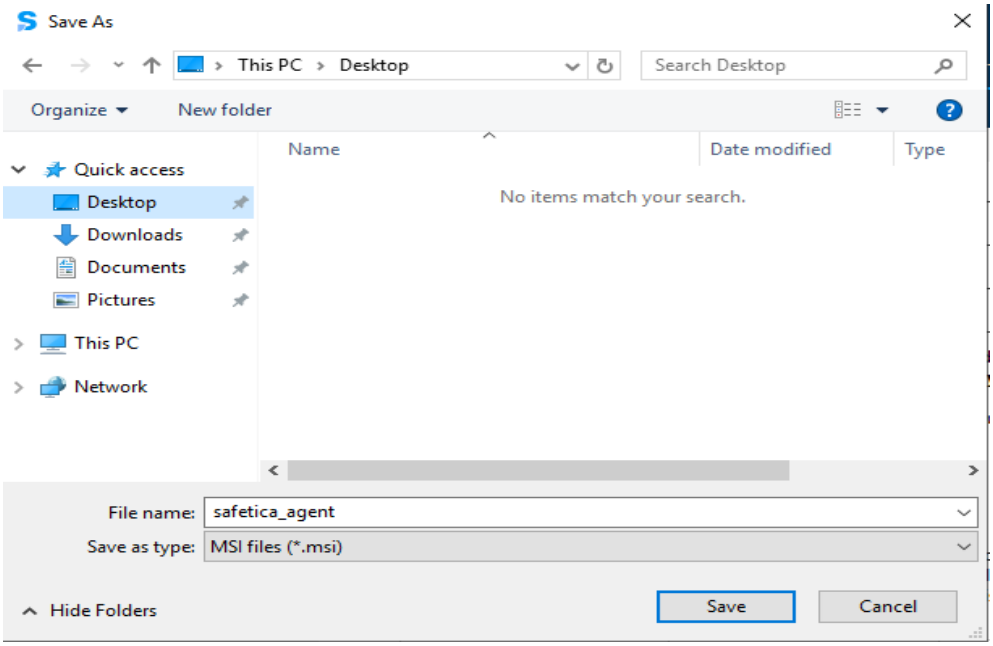


Рис. 3.14. Вікно вибору шляху завантаження

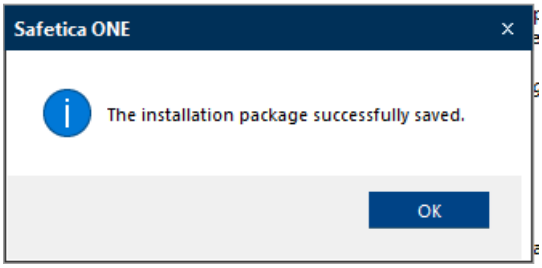


Рис. 3.15. Вікно успішного завантаження інсталятора агентам

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

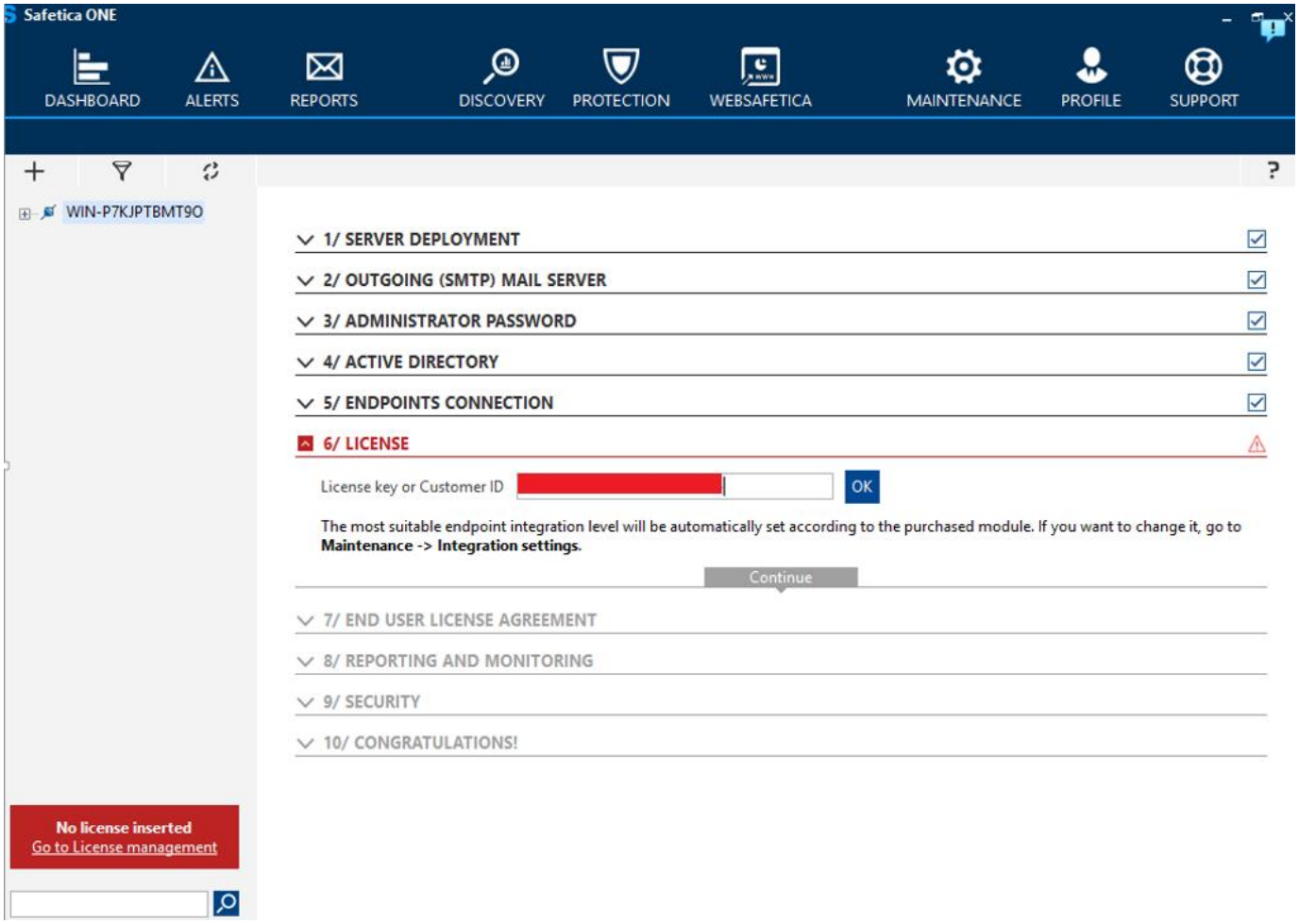


Рис. 3.16. Вікно вводу ліцензійного ключа

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

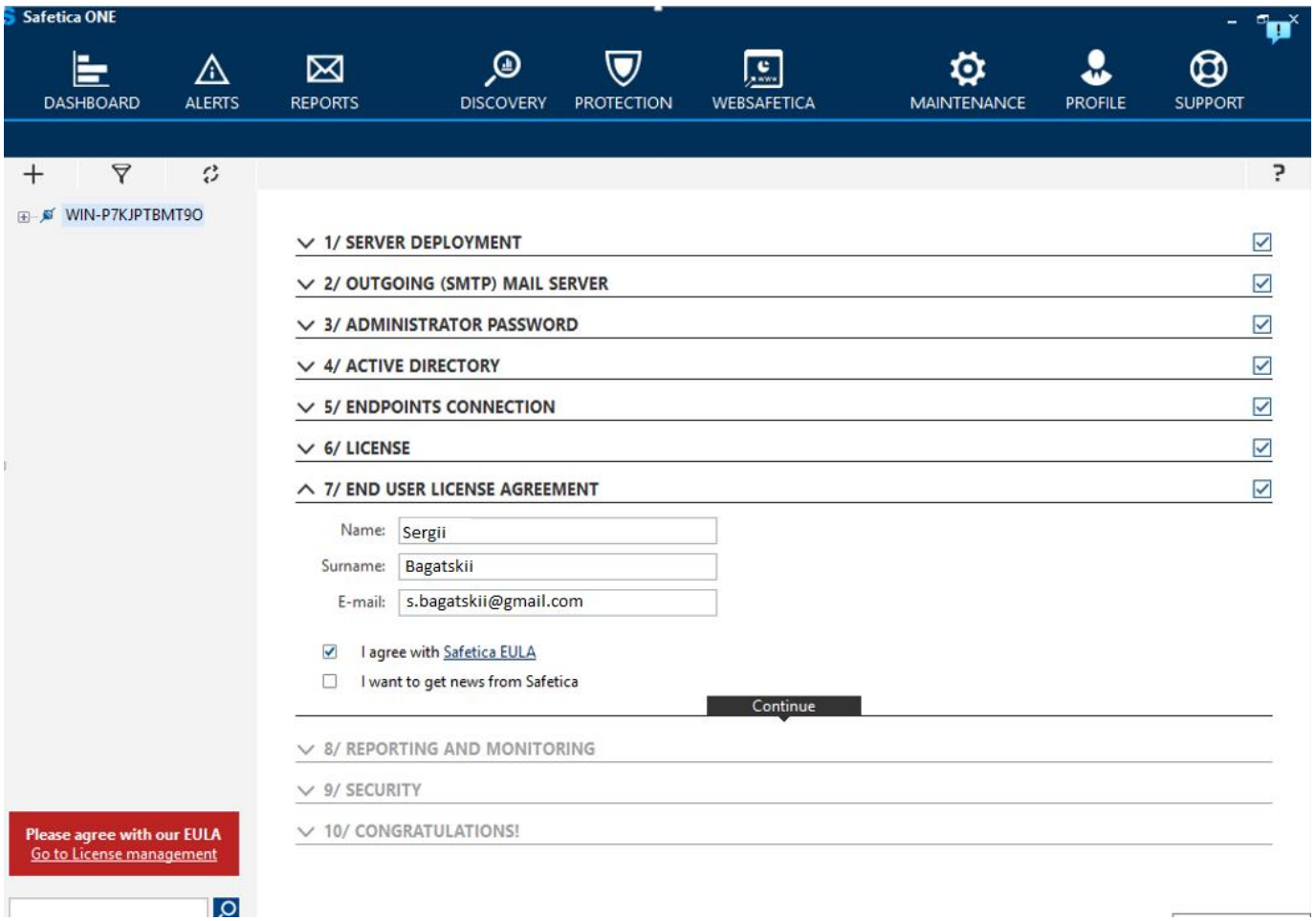


Рис. 3.17. Вікно вводу даних адміністратора

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

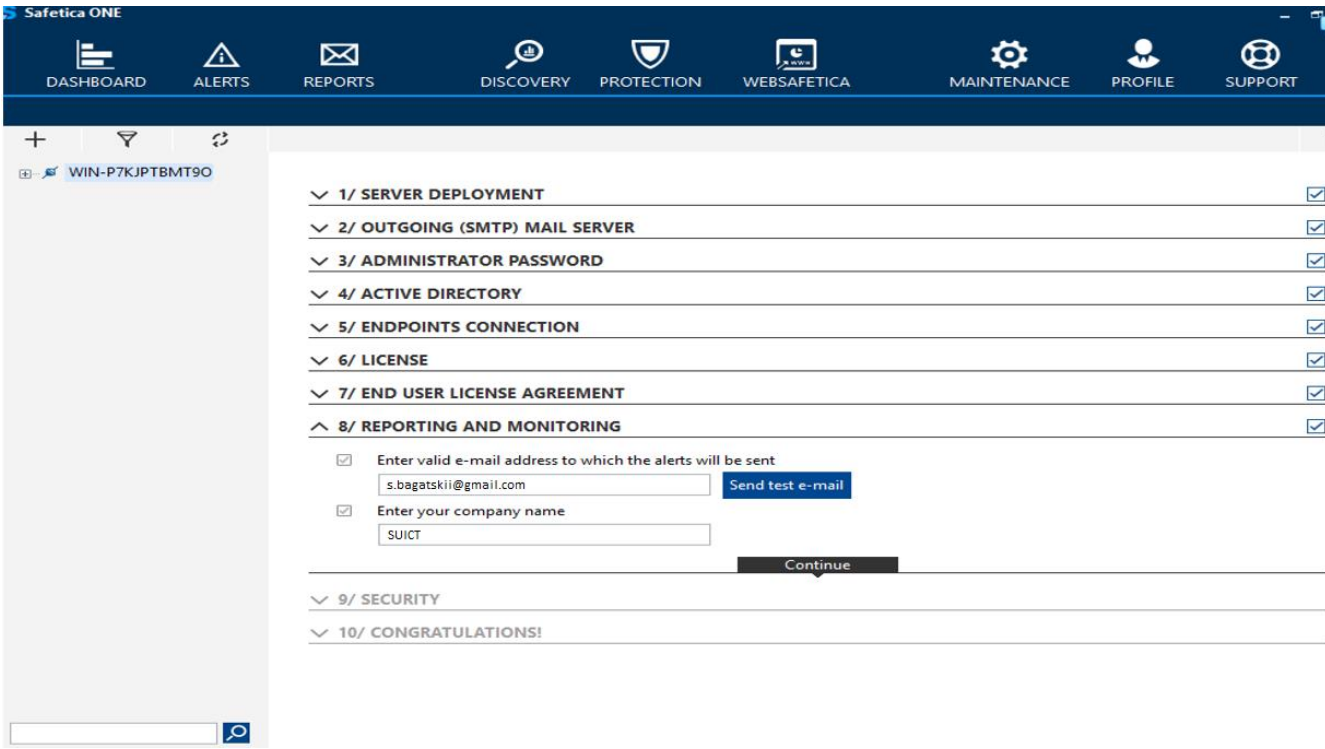


Рис. 3.18. Вікно для вводу назви компанії

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

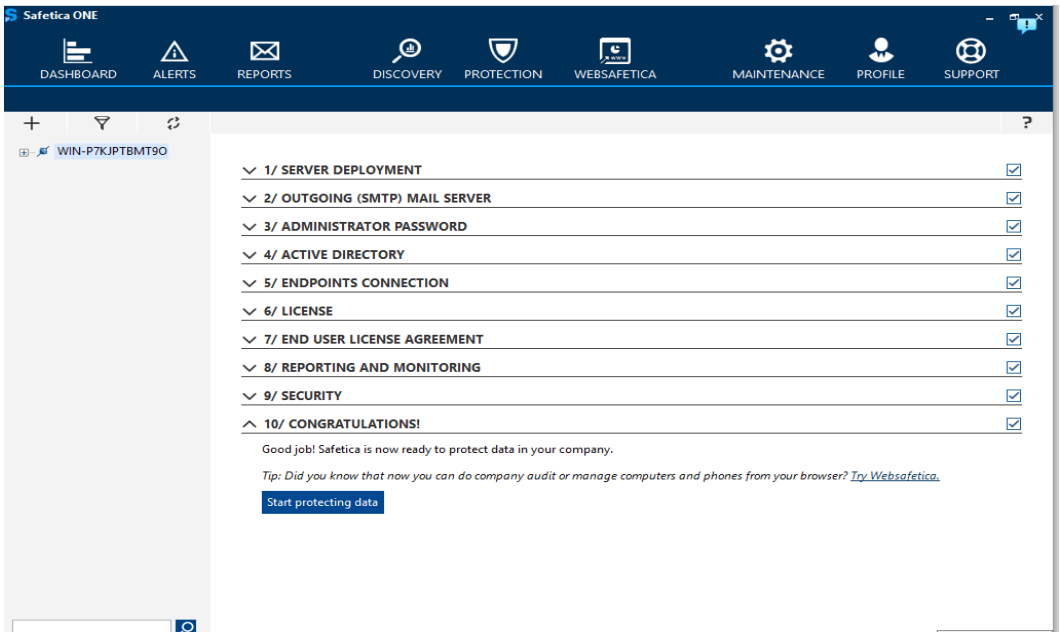


Рис. 3.19. Вікно підтвердження успішного налаштування системи

3.2. Оптимізація та підвищення ефективності DLP-системи

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

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

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

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

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

Існує кілька послідовностей, як налаштувати захист DLP в розділі Protection. Для початку потрібно визначити, які саме дані вважати конфіденційними. Для цього потрібно провести відповідний аудит всередині організації та вирішити, які будуть ступені захищеності файлів. Safetica пропонує декілька видів класифікацій

конфіденційних даних, щоб потім використовувати їх під час створення політик:

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

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

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

• На основі властивостей файлу (Based on file properties (File properties)) – категорії даних властивостей файлу дозволяють захищати файли на основі їх властивостей, таких як розширення файлів, незалежно від їх вмісту чи класифікації. Наприклад, ви можете захистити всі вихідні файли .pdf або .cad. Ці категорії також можуть розширювати існуючі політики DLP для захисту файлів, які не можна перевірити на предмет класифікації або конфіденційних даних (наприклад, зашифрованих файлів)[11-16].

Після проведення аналізу та прийняття рішення стосовно класифікації файлів потрібно обрати, під який саме класифікатор в Safetica підпадають ті чи інші дані. Створити відповідні категорії даних, для подальшого їх використання. У розділі Категорії даних можна створити необмежену кількість категорій даних. Категорії

даних використовуються для класифікації файлів на різні групи залежно від того, хто, де і як може з ними працювати. Після створення категорій даних для них створюються різні DLP-політики і таким чином захищаються класифіковані дані.

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

Створення політики з розпізнавання IBAN та номерів карток

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

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

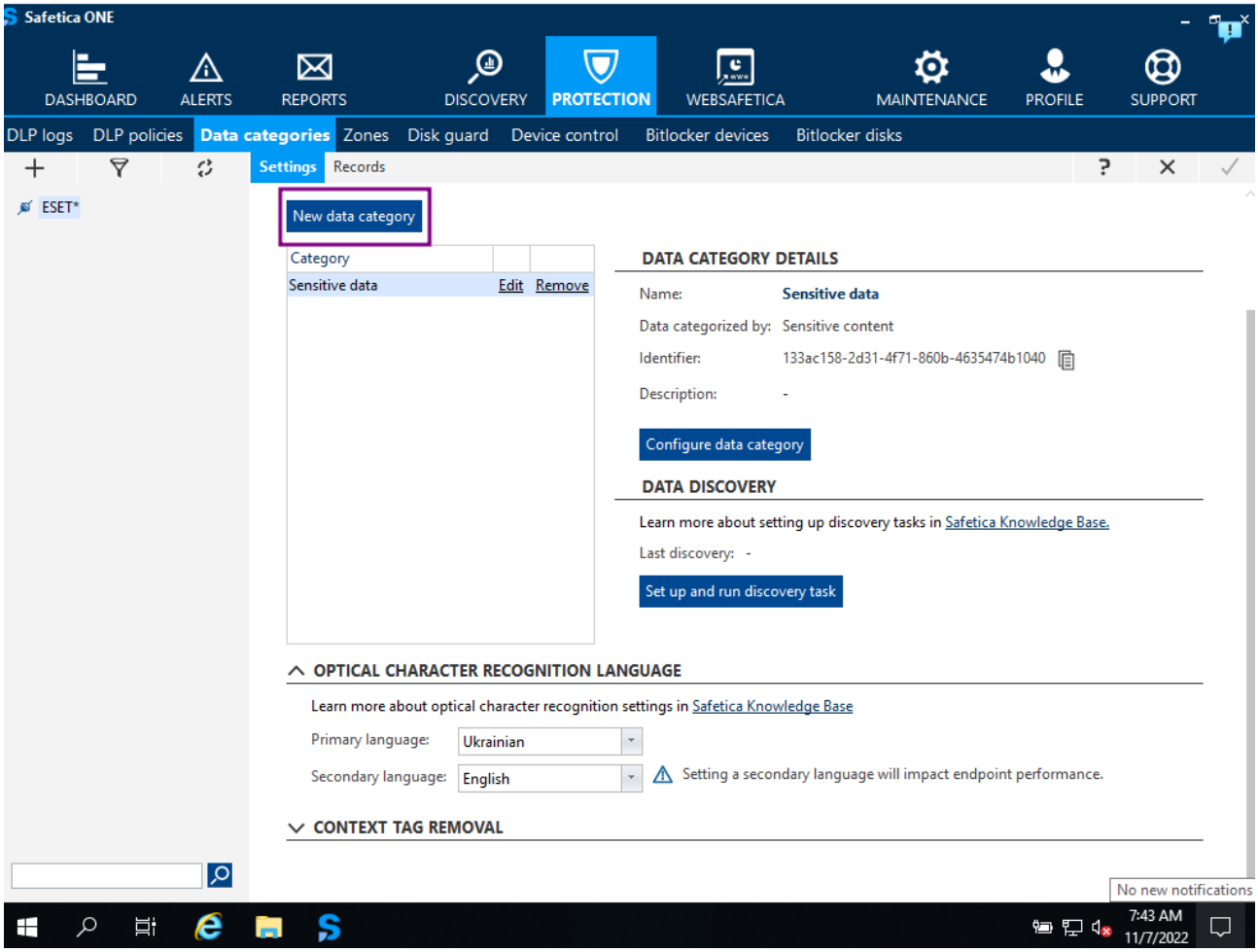


Рис. 3.20. Вікно підрозділу Data categories

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

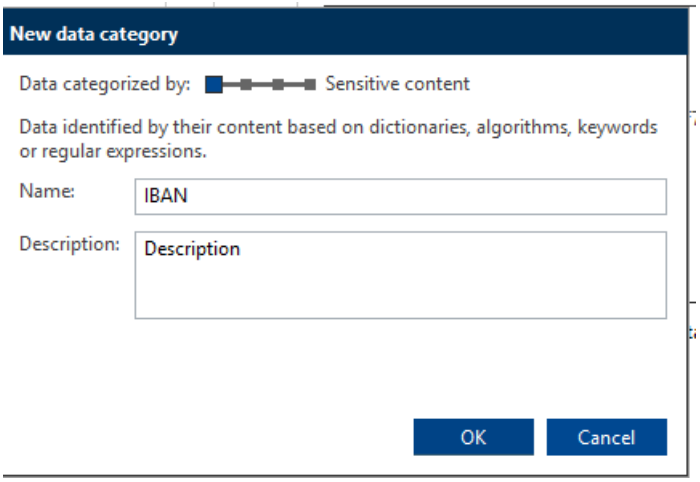


Рис. 3.21. Вікно вибору типу категорії даних

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

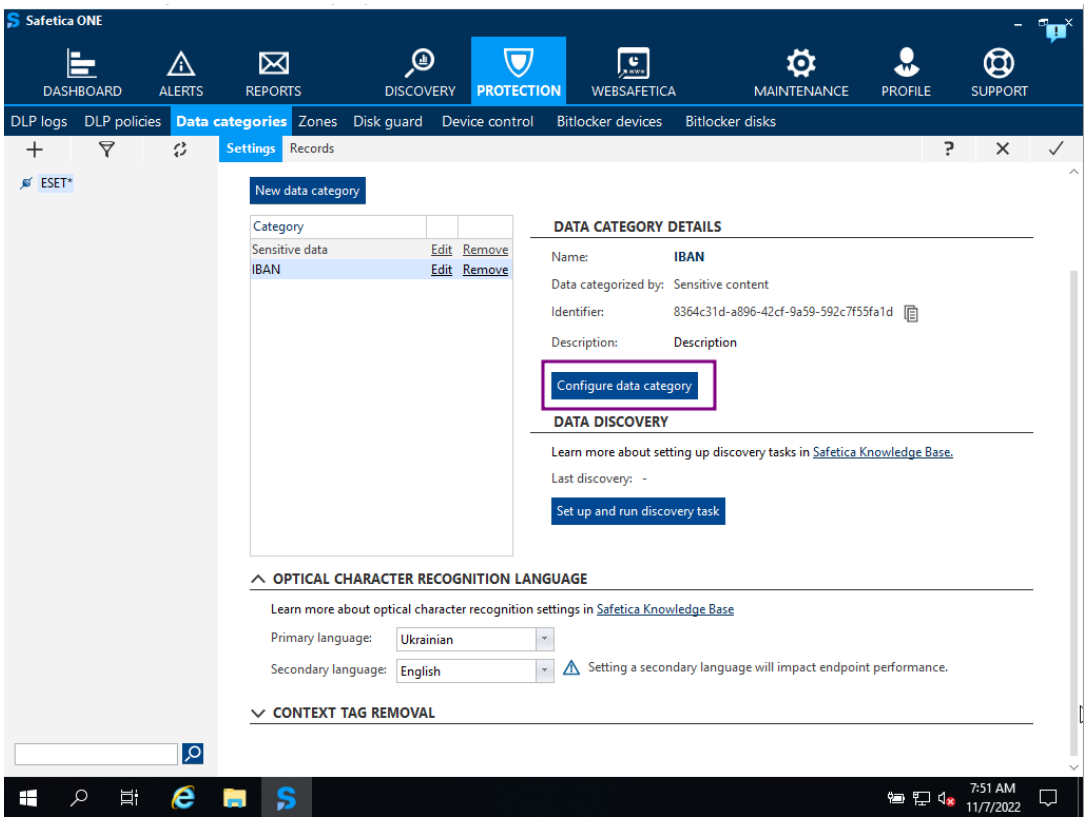


Рис. 3.22. Вікно вибору налаштування категорії даних

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

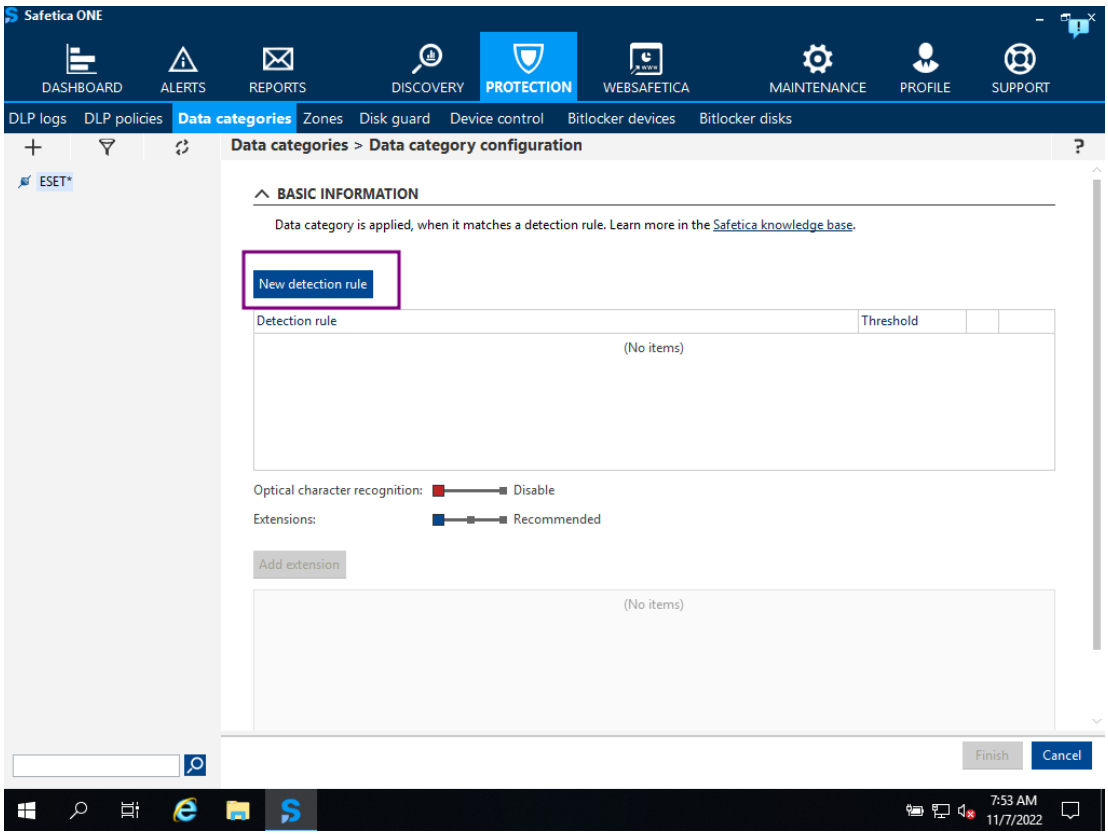


Рис. 3.23. Вікно налаштувань категорії даних

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

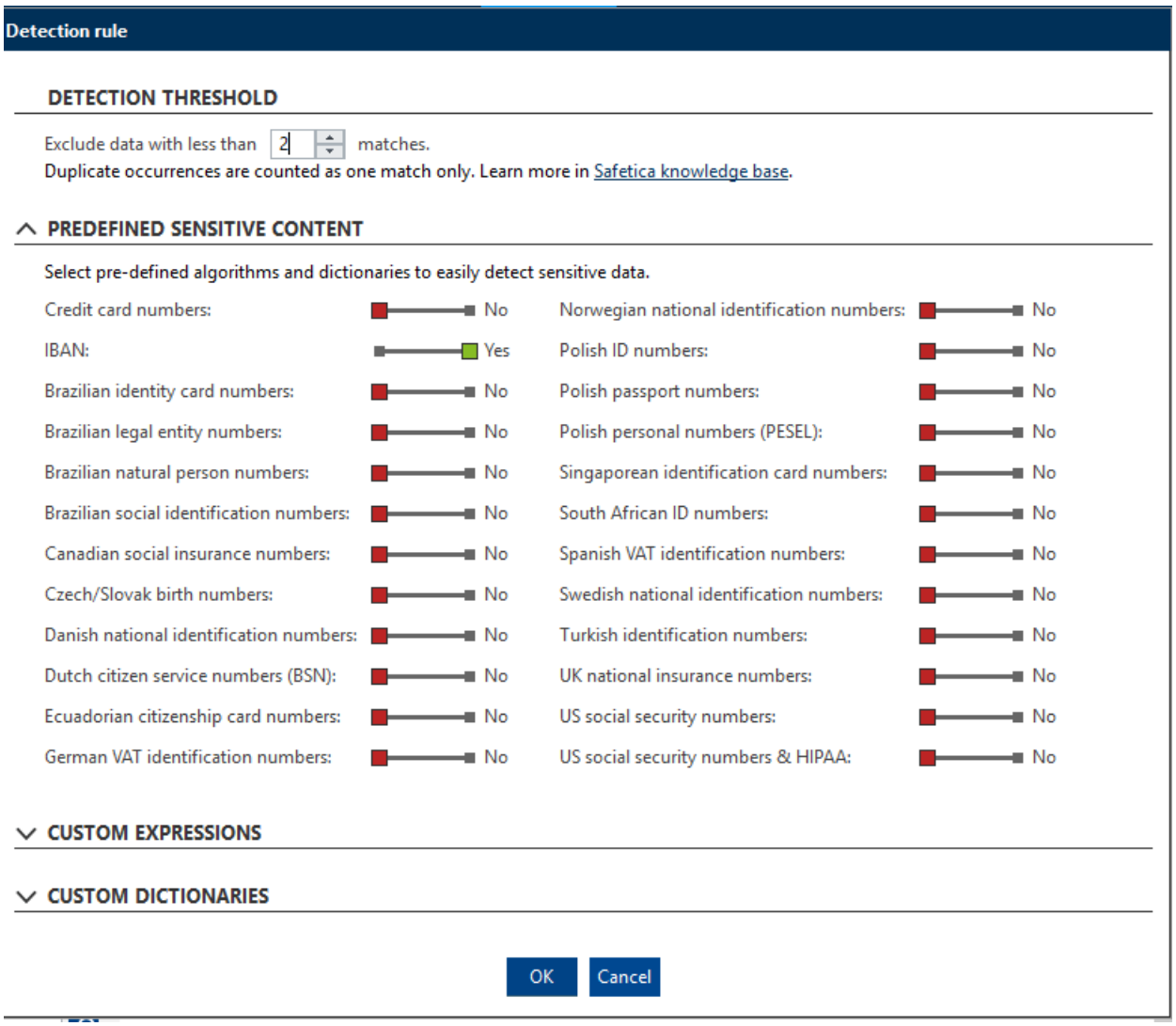


Рис. 3.24. Вікно створення правила розпізнавання IBAN

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

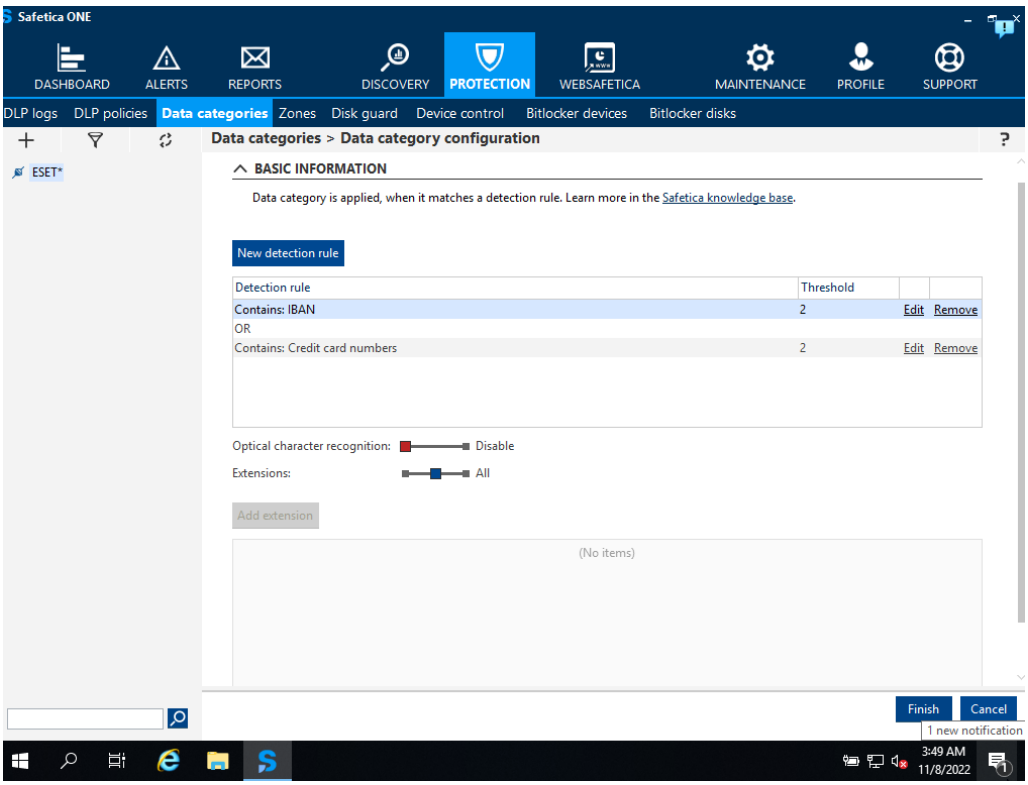


Рис. 3.25. Вікно створеного правила розпізнавання

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

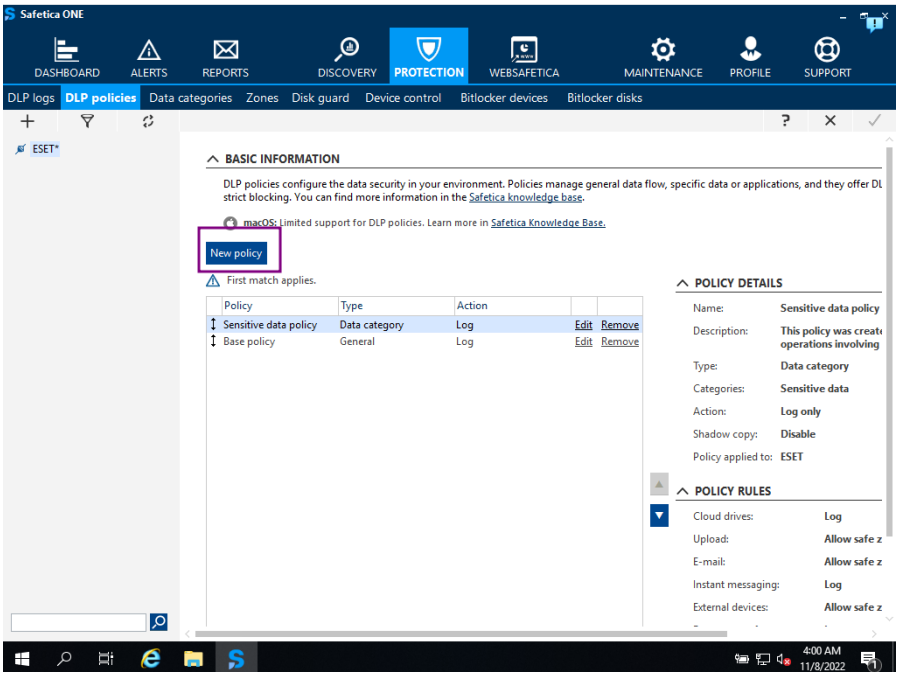


Рис. 3.26. Вікно підрозділу DLP policies

У новій вкладці потрібно обрати тип політики, яку необхідно створити. Потрібно обрати тип Data та обрати категорію даних, яку попередньо створили.

Далі «Next» (рис.3.27).

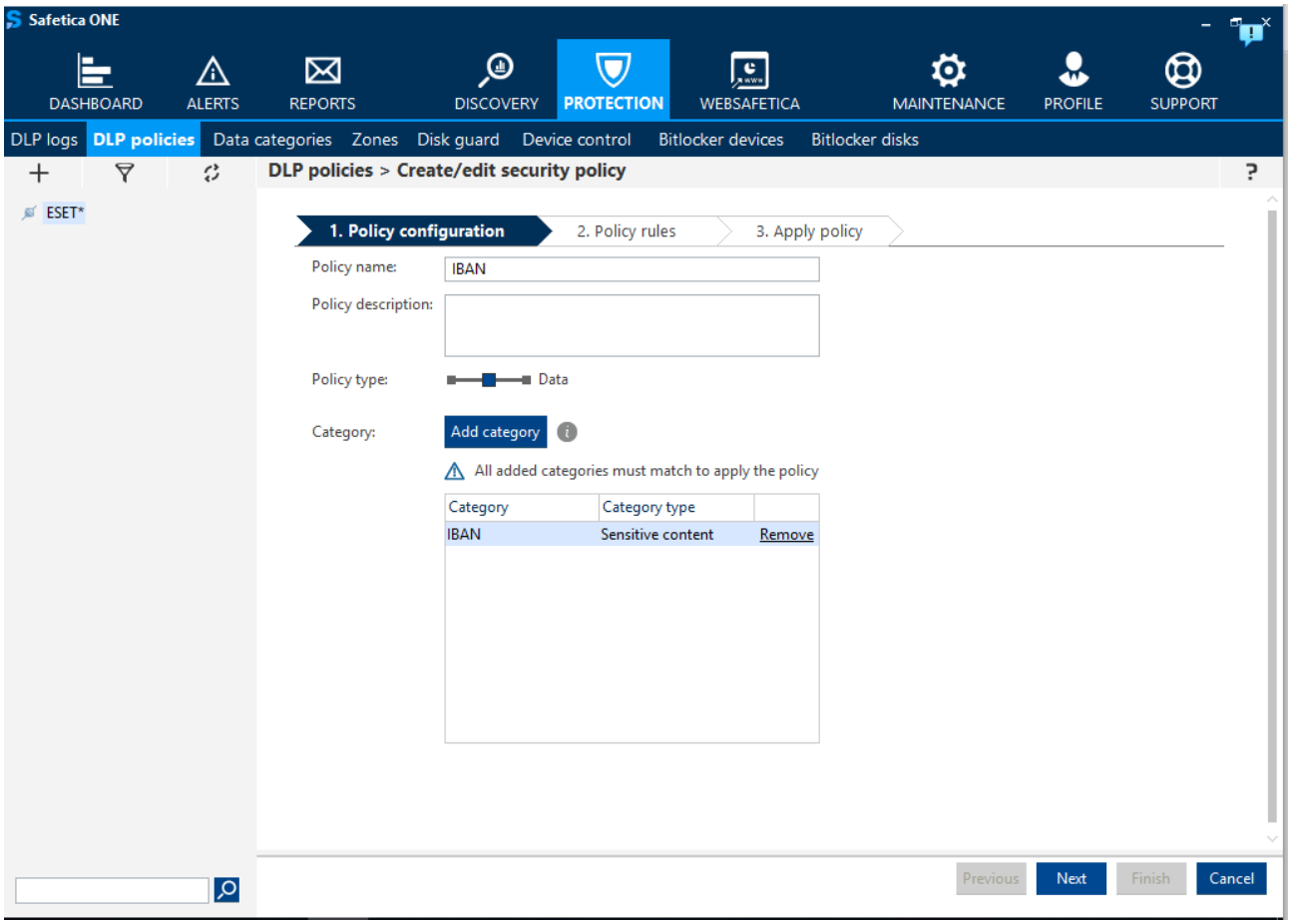


Рис. 3.27. Вікно вибору типу політики

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

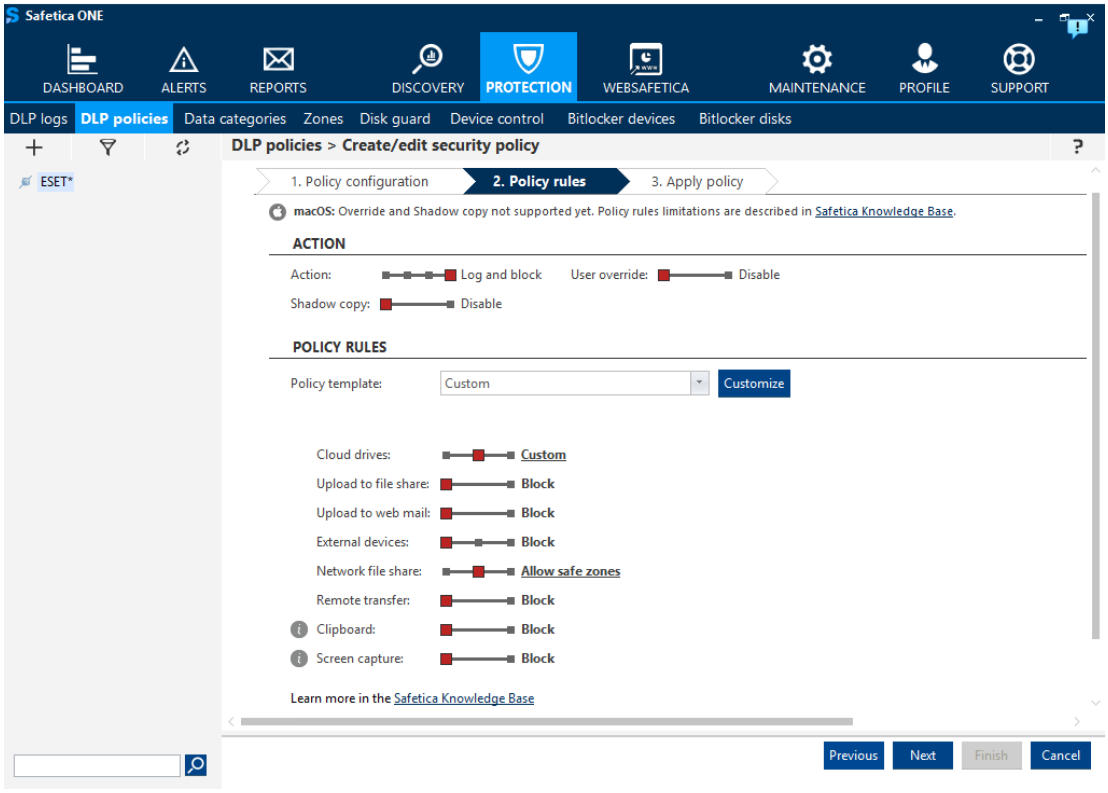


Рис. 3.28. Вікно вибору налаштувань політики

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

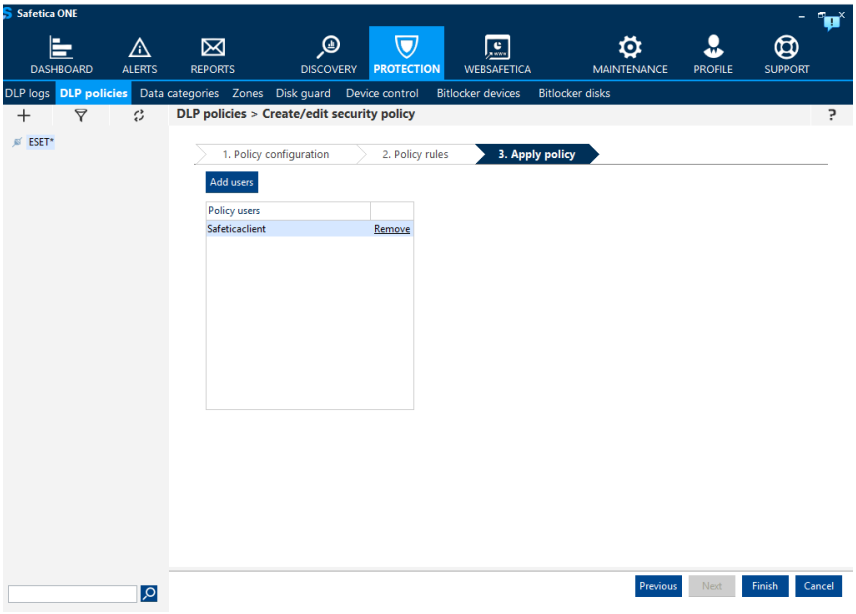


Рис. 3.29. Вікно вибору ПК чи користувачів

Зберігаємо налаштування в підрозділі DLP policies.

Створення політики з використанням тегів

Наступна категорія даних доступна, якщо помістити документ у відповідну папку. Тобто після перегляду всі документи сортуються за важливістю, а потім поміщаються в папки з відповідними правами доступу. Щоб мінімізувати ризик витоку такої важливої інформації, потрібно використовувати контекстні категорії даних правил. З відповідними налаштуваннями призначаються відповідні теги кожному документу на основі файлової системи. Кінцеві користувачі не можуть видалити або змінити цю мітку, усі ці дії виконуються лише в консолі адміністратора. Тег залишається в документі, і якщо розширення перейменовано або змінено розширення, тег залишається на місці, навіть якщо відповідний документ заархівовано, оскільки він призначений на основі файлової системи [11-14].

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

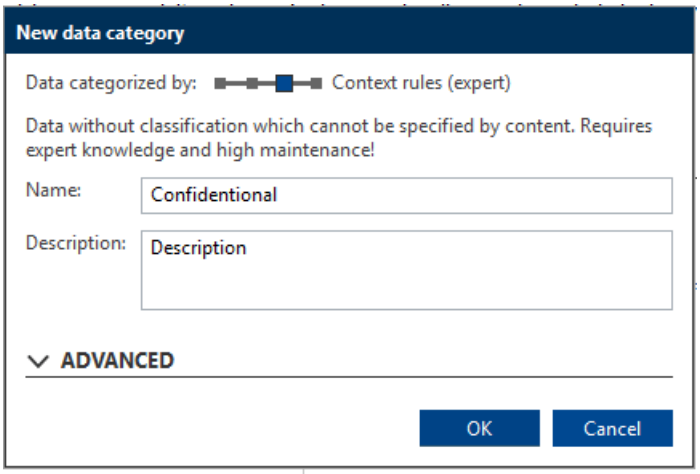


Рис. 3.30. Вікно вибору типу категорії даних

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

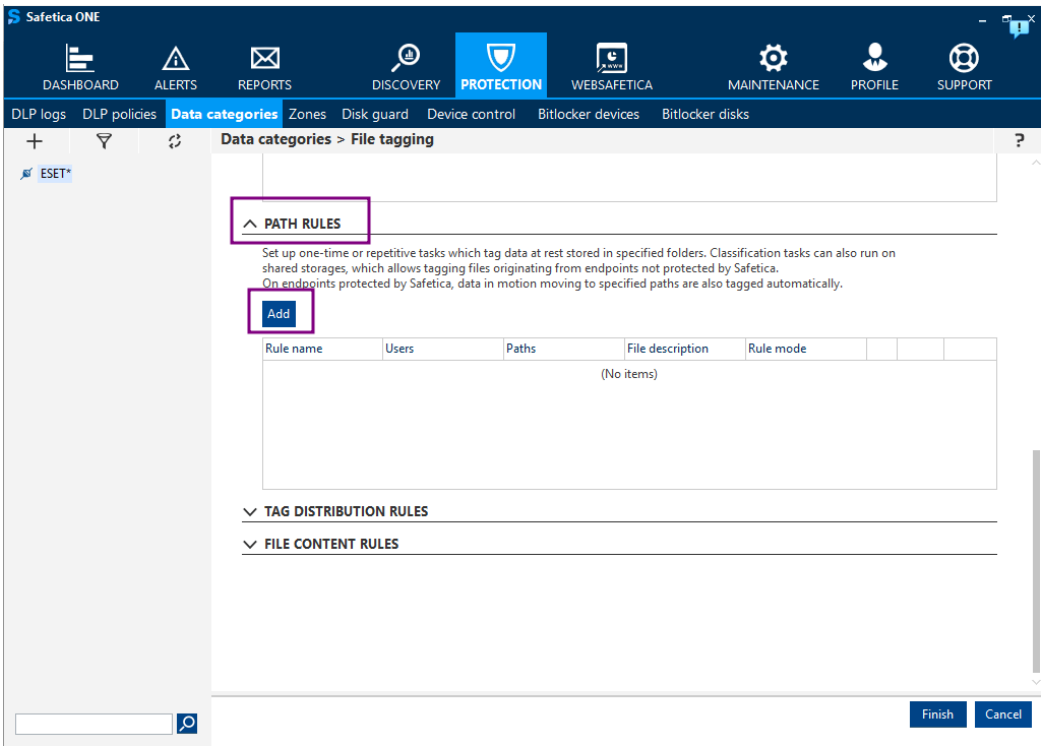


Рис. 3.31. Вікно створення правила тегування

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

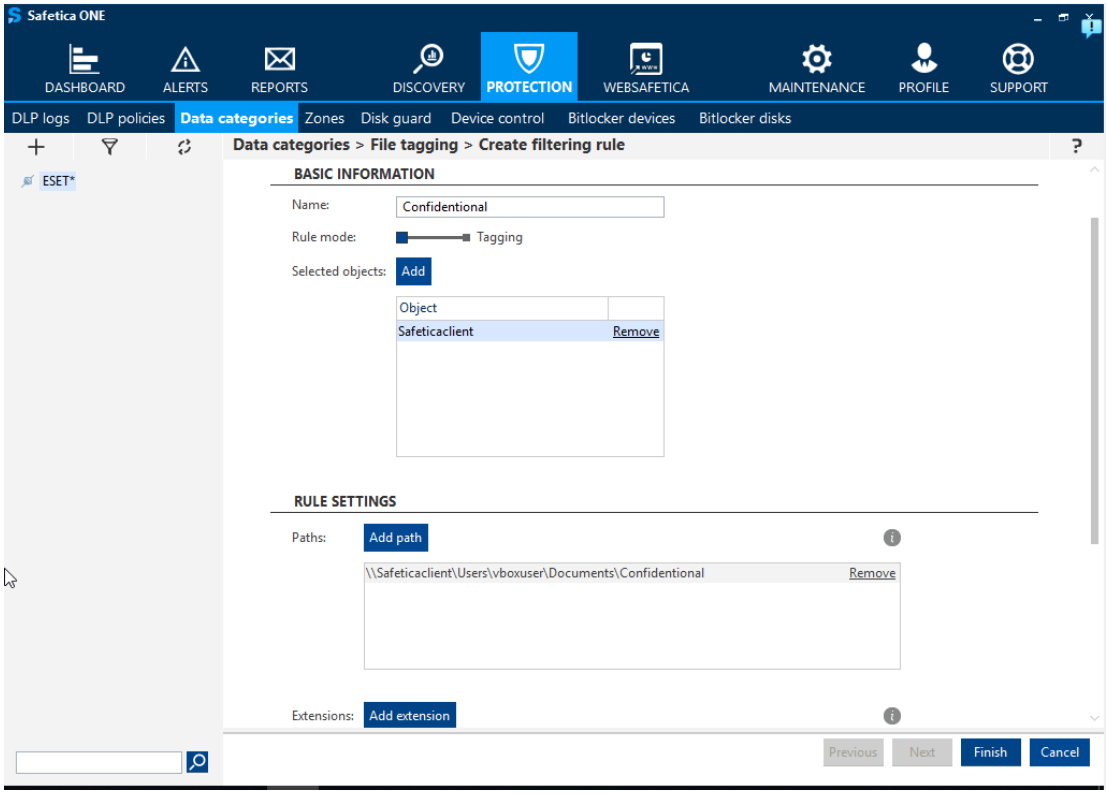


Рис. 3.32. Вікно створення правила тегування

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

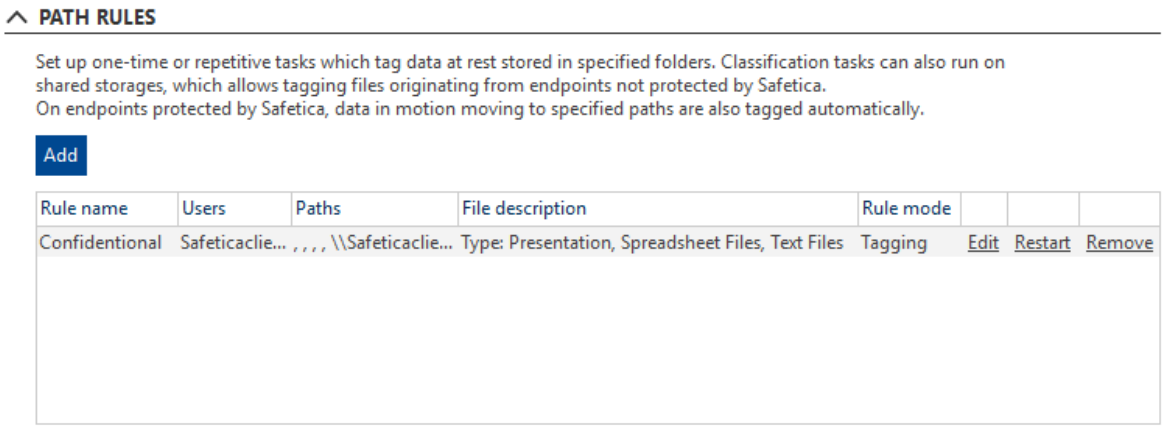


Рис. 3.33. Створене правило тегування

Після успішного створення категорії даних перейти до створення політики. В новому вікні вводимо назву політики та обираємо тип Data. Далі обирати із випадаючого списку попередньо створену категорію даних Context rule. Після цього перейти до налаштування політки натиснувши «Next». Використати дію Log and

block, щоб мінімізувати можливий витік конфіденційний тегованих файлів. Налаштовати правила політики та натиснути «Next». Далі обирати ПК та\або користувачів, до яких буде застосовуватися політика і натиснути «Finish» (рис.3.34).

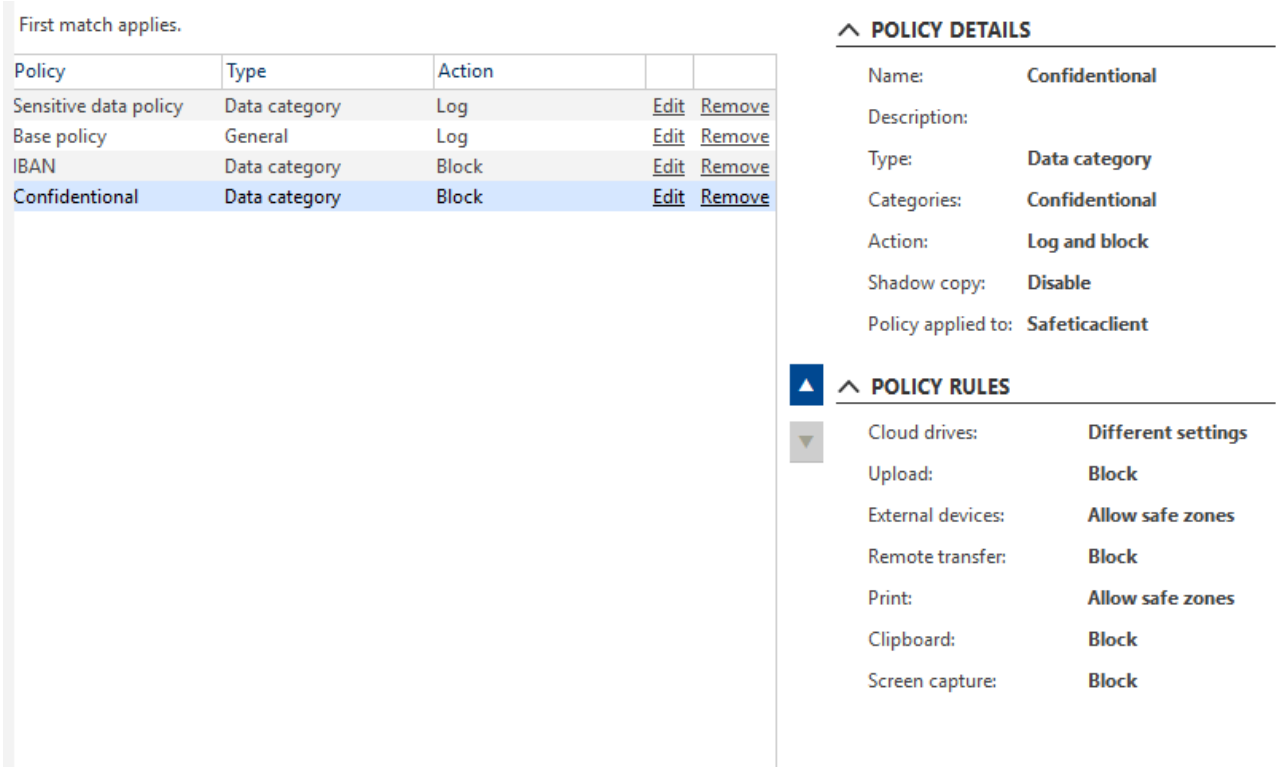


Рис. 3.34. Перегляд налаштувань політики

Перевірити правильність налаштувань та зберегти політику.

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

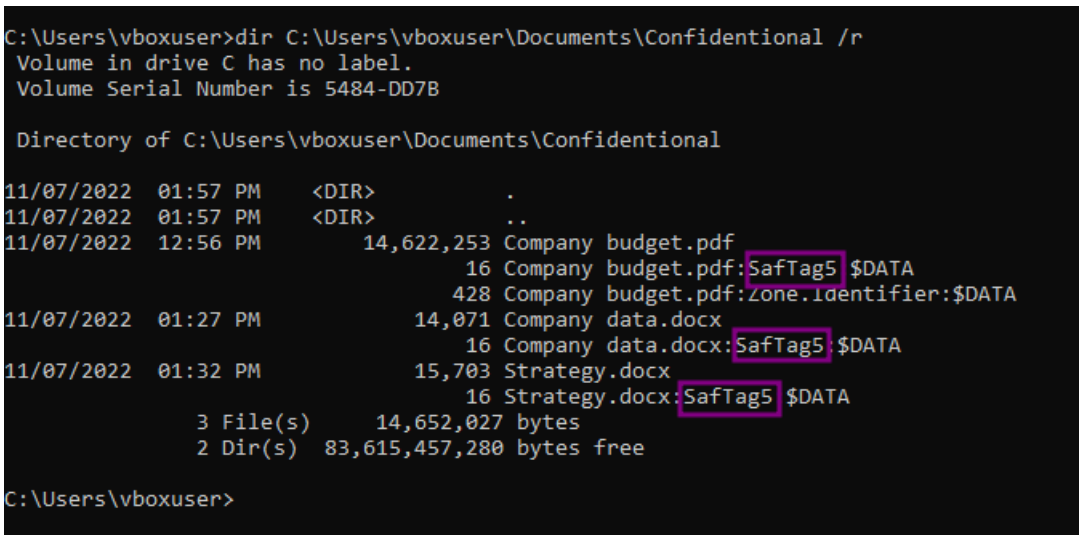


Рис. 3.35. Вивід команди з детальною інформацією про файли

Створення політики з використанням WebSafetica

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

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

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

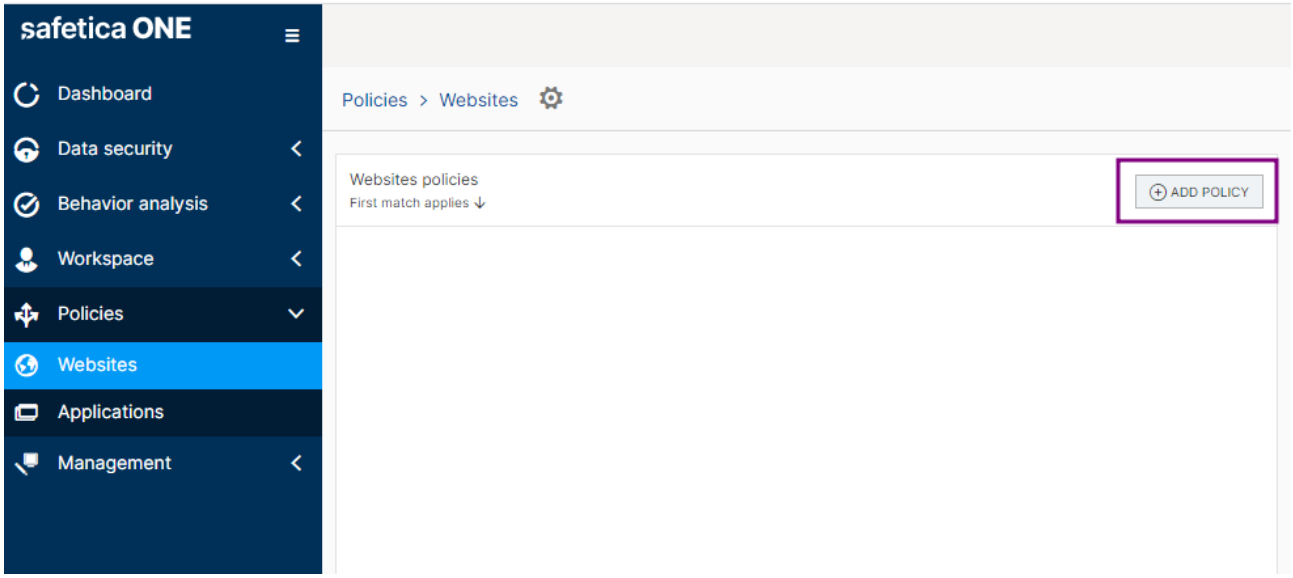


Рис. 3.36. Вікно додавання нової політики

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

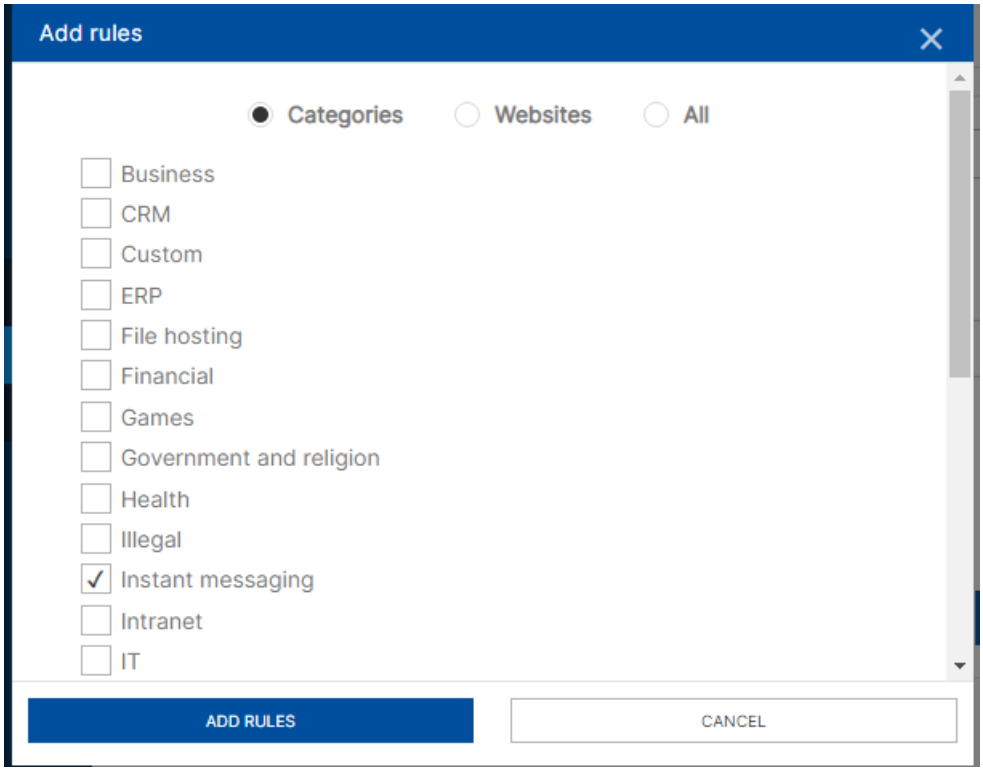


Рис. 3.37. Вікно налаштування правила блокування

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

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

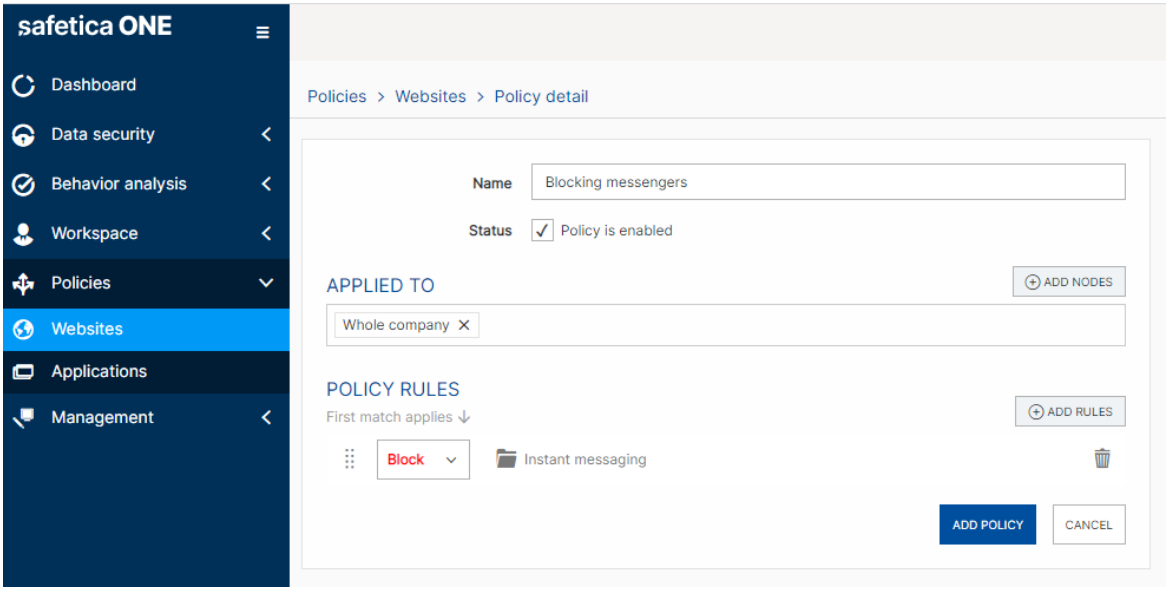


Рис. 3.38. Вікно перегляду налаштувань політики

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

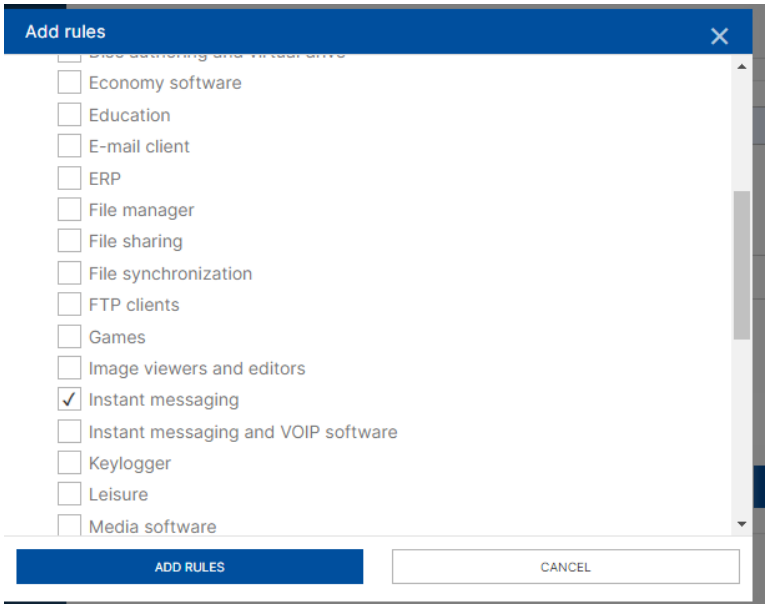


Рис. 3.39. Вікно вибору політики блокування

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

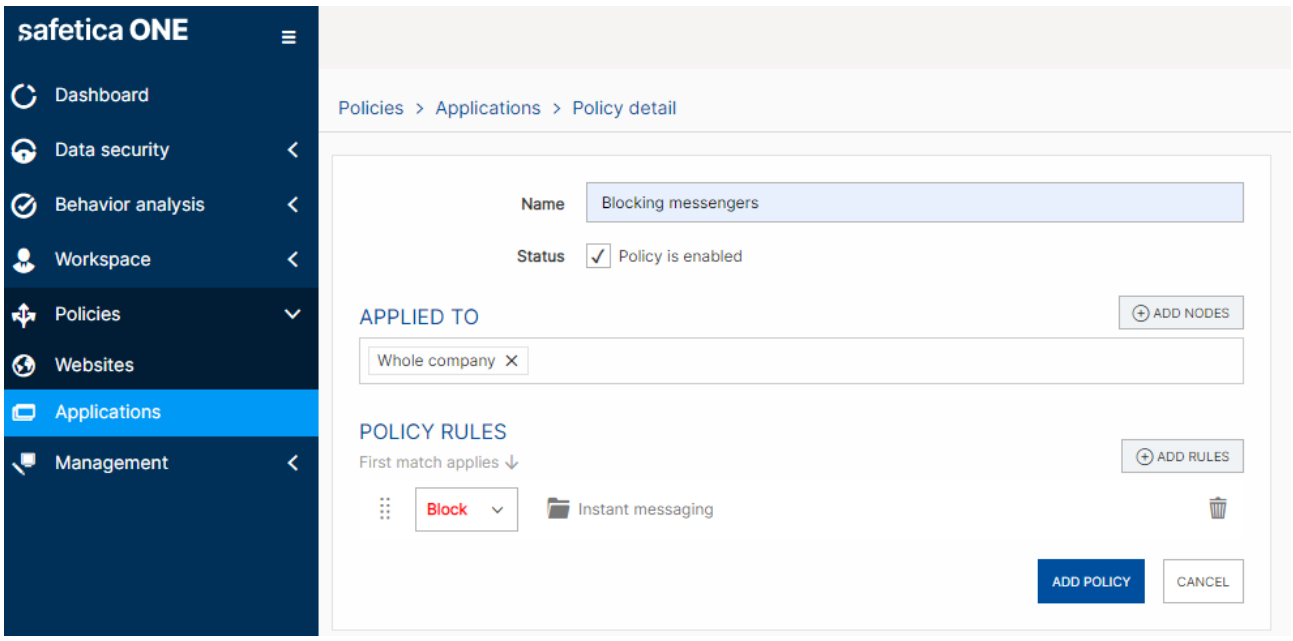


Рис. 3.40. Вікно перегляду налаштувань

Обидві політики успішно створені та застосовані до відповідних ПК.

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

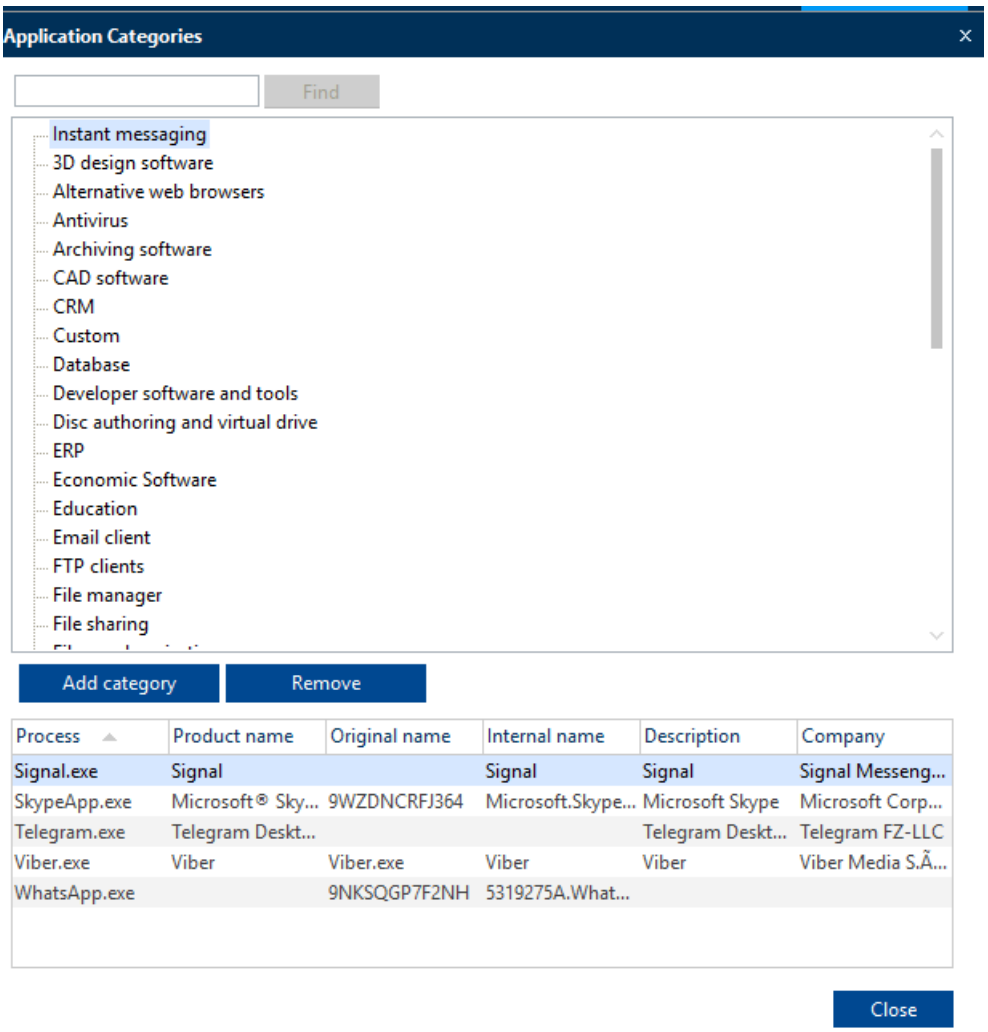


Рис. 3.41. Вікно перегляду категорій додатків

3.3. Розроблення рекомендацій щодо захисту від несанкціонованого доступу до інформаційної системи з використанням DLP

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

1. Необхідно проаналізувати діяльність організації та сценарії витоку даних.
2. Розмежувати типи даних до відповідної категорії.
3. Оцінити наслідки та втрати витоку даних.
4. Вірно налаштувати DLP систему для протидії вторгнень.

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

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

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

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

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

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

11. Регулярне проведення аудиту ефективності технології DLP.

Висновки до розділу 3

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

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

ВИСНОВКИ

У сучасному цифровому світі, де інформація стає все більш цінним ресурсом, забезпечення її безпеки набуває критичного значення. Несанкціонований доступ до інформаційних систем може призвести до серйозних наслідків, включаючи витік конфіденційних даних, фінансові втрати, репутаційні ризики та порушення нормативних вимог. Відповідно, питання захисту від несанкціонованого доступу є надзвичайно актуальним для організацій усіх рівнів та галузей.

В першому розділі було проаналізовано загрози інформаційній системі, поняття НСД. Важливість захисту від НСД його ризики на інформаційну систему організації та конфіденційних даних. Проаналізовані основні причини несанкціонованого доступу та їх наслідки для організації.

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

В третьому розділі було встановлено та налаштовано систему DLP Safetica One. Проведена детальна оптимізація для підвищення ефективності системи DLP. Розроблено рекомендації щодо застосування технології DLP Safetica One.

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

ПЕРЕЛІК ПОСИЛАНЬ

1. Національний кластер кібербезпеки «Глосарій». URL: https://cybersecuritycluster.org.ua/glossary/ (дата звернення: 15.04.2024).
2. Contributor T. Top 10 Types of Information Security Threats for IT Teams | TechTarget. Security. URL: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams (date of access: 15.04.2024).
3. Bakharev N. Unauthorized Access: Risks, Examples, and 6 Defensive Measures. brightsec. URL: https://brightsec.com/blog/unauthorized-access-risks-examples-and-6-defensive-measures/#:~:text=When%20unauthorized%20individuals%20gain%20access,reputation,%20and%20potential%20legal%20repercussions. (date of access: 15.04.2024).
4. 5 Ways to Effectively Prevent Data Leakage. SecurityScorecard. URL: https://securityscorecard.com/blog/ways-to-prevent-a-data-leakage/ (date of access: 15.04.2024).
5. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 15.04.2024).
6. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI : станом на 8 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 15.04.2024).
7. Кондратенко М. Система запобігання витоку інформації на підприємстві : Дипломна робота "Бакалавра". Київ, 2021. 56 с.
8. Гончаренко Є. О. Вибір підходу до оцінки ризиків інформаційної безпеки для підприємств роздрібної торгівлі : Магістерська дисертація. Київ, 2018. 92 с.
9. Методи і способи захисту інформації. Pidru4niki. URL: https://pidru4niki.com/1801051351329/ekonomika/metodi_sposobi_zahistu_informatsiyi (дата звернення: 15.04.2024).

10. What Is DLP and How Does It Work? | Trellix. Trellix | Revolutionary Threat Detection and Response. URL: https://www.trellix.com/security-awareness/data-protection/how-data-loss-prevention-dlp-technology-works/ (date of access: 10.05.2024).

11. Boehm A. What is Data Loss Prevention (DLP)? [Guide] - CrowdStrike. crowdstrike.com. URL: https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/ (date of access: 10.05.2024).

12. What is DLP? Data Loss Prevention, Meaning & Definition. Netskope. URL: https://www.netskope.com/security-defined/what-is-data-loss-prevention-dlp (date of access: 10.05.2024).

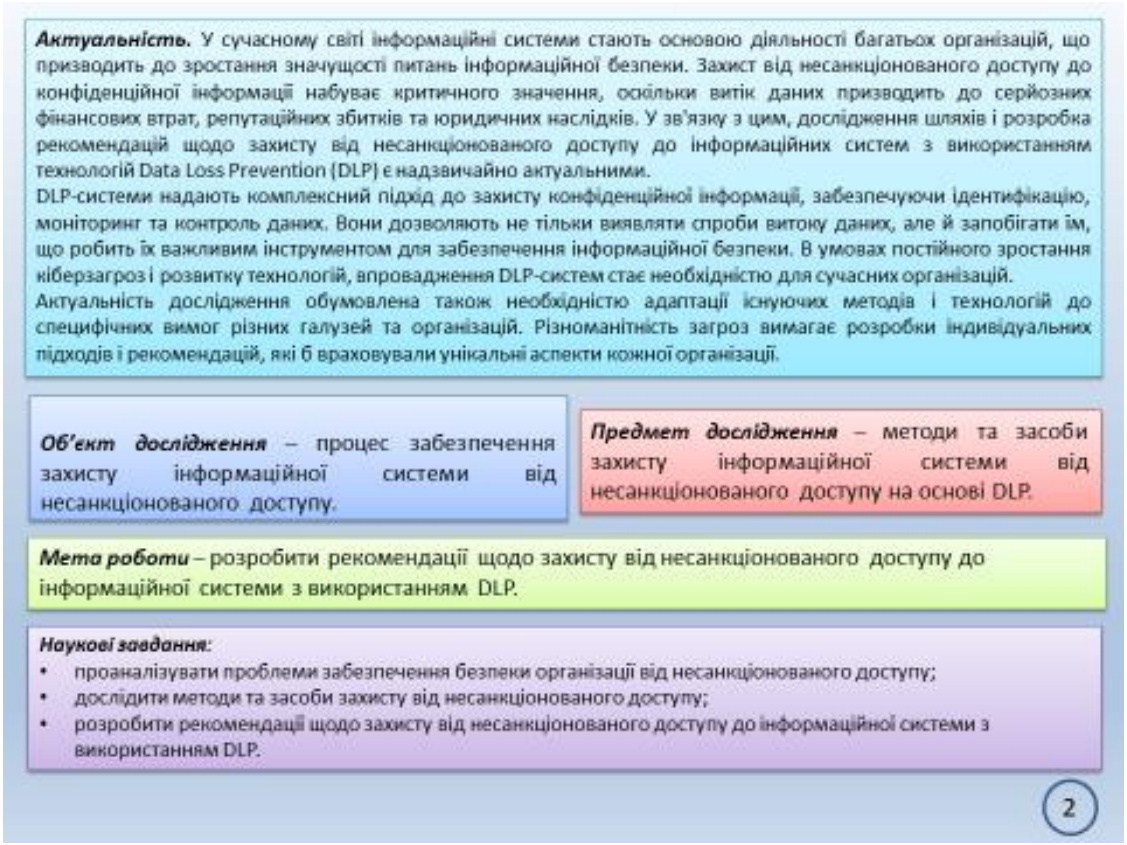
13. DLP Systems: Models, Architecture and Algorithms. Share & Discover Presentations | SlideShare. URL: https://www.slideshare.net/liwei_ren/dlp-systems-models-architecture-and-algorithms (date of access: 11.05.2024).

14. Safetica ONE â Data loss prevention software | Safetica. Safetica | Data loss prevention (DLP). URL: https://www.safetica.com/products-safetica-one (date of access: 10.05.2024).

15. Data Loss Prevention Safetica ONE Product Overview. Malware Protection & Internet Security | ESET. URL: https://www.eset.com/fileadmin/ESET/INT/Products/Business/Safetica/Safetica_ONE_Product_Overview.pdf (date of access: 14.05.2024).

16. Safetica ONE Complete Documentation. HubSpot | Redirecting... URL: https://app.hubspot.com/documents/7097913/view/85697610?accessId=dc5c3b (date of access: 14.05.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)



Основні загрози інформаційним системам

3

1. Внутрішні загрози
Внутрішня загроза виникає, коли люди, близькі до організації, які мають дозвіл на доступ до її мережі, навмисно чи ненавмисно зловживають цим доступом, щоб негативно вплинути на критично важливі дані або системи організації.

2. Віруси та черв'яки
Віруси та черв'яки (хробаки) — це зловмисне програмне забезпечення, спрямоване на знищення систем, даних і мережі організації.

3. Ботнети
Ботнет – це набір пристроїв, підключених до Інтернету, включаючи ПК, мобільні пристрої, сервери та пристрої Інтернету речей (IoT), які заражені та дистанційно керовані звичайним типом зловмисного програмного забезпечення .

4. Атаки завантажень (Drive-by Download)
Під час атаки Drive-by Download шкідливий код завантажується з веб-сайту через браузер в програму чи інтегровану ОС без дозволу або відома користувача.

5. Фішингові атаки
Фішингові атаки – це тип загроз інформаційній безпеці, який використовує соціальну інженерію, щоб обманом змусити користувачів порушити звичайні методи безпеки та надати конфіденційну інформацію, зокрема імена, адреси, облікові дані для входу, номери соціального страхування, дані кредитних карток та іншу фінансову інформацію

6. Розподілені атаки на відмову в обслуговуванні
У розподіленій атаці типу «відмова в обслуговуванні» (DDoS) кілька скомпрометованих машин атакують ціль, наприклад сервер, веб-сайт або інший мережевий ресурс, роблячи ціль повністю непрацездатною.

7. Програми-вимагачі
Під час атаки програм-вимагачів комп'ютер жертви блокується, зазвичай за допомогою шифрування, що не дозволяє жертві використовувати пристрій або дані, які на ньому зберігаються.

8. Набори експлойтів
Набір експлойтів — це інструмент програмування, який дозволяє людині без досвіду написання програмного коду створювати, налаштовувати та поширювати зловмисне програмне забезпечення.

9. Розширені постійні атаки загроз
Розширена постійна загроза (APT - Advanced persistent threat attacks) — це цілеспрямована кібератака, під час якої неавторизований зловмисник проникає в мережу та залишається непоміченим протягом тривалого періоду часу.

10. Шкідлива реклама
Шкідлива реклама – це техніка, яку використовують кіберзлочинці для введення шкідливого коду в законні мережі онлайн-реклами та веб-сторінки.

Визначення категорій,типів конфіденційних даних та оцінка витоку конфіденційної інформації

4

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

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

Категорії та типи конфіденційних даних:
1. Особисті дані: ім'я та прізвище; адреса; номер телефону; адреса електронної пошти; соціальний номер (в США, наприклад, Social Security Number).
2. Фінансова інформація: карткові дані (номер картки, термін дії, CVV-код); банківські реквізити (реквізити рахунку, код банку); платіжні історії, фінансові звіти.
3. Медична інформація: історія захворювань; результати аналізів; інформація про прийом лікарських засобів; діагнози та лікування.
4. Комерційна та конфіденційна інформація компаній: бізнес-плани; фінансові документи; конфіденційні угоди та контракти.
5. Конфіденційна технічна інформація: патенти та реєстраційні дані; технічні специфікації; програмний код.
6. Державна інформація: військові стратегії; розвідувальні дані; класифіковані документи.

Основні кроки у процесі оцінки наслідків витоку конфіденційної інформації у разі НСД включають:

- визначення та ідентифікація витоку;
- оцінка важливості даних;
- оцінка потенційних втрат;
- оцінка репутаційних втрат;
- оцінка впливу на ділову діяльність;
- визначення заходів та стратегій;
- оцінка відповідальності;
- комунікація та повідомлення сторонам зацікавленим;
- моніторинг та вдосконалення.

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

Ключові методи запобігання несанкціонованому доступу

5

1. Політика надійних паролів.

2. Двофакторна автентифікація (2FA) і багатофакторна автентифікація.

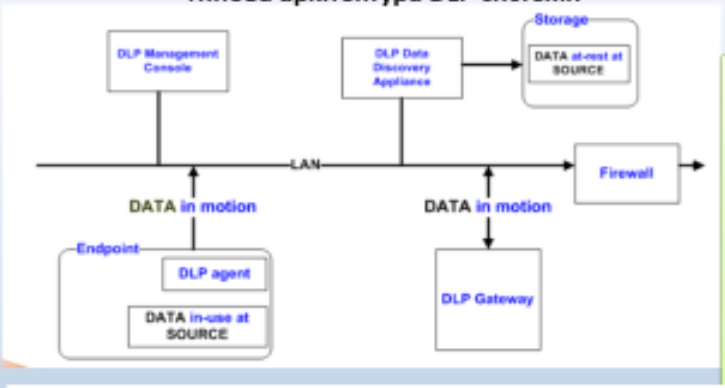
3. Фізична безпека

4. Моніторинг активності користувача:
- **аналіз журналів;**
- **сповіщення на основі правил;**
- **поведінкова аналітика.**

5. Безпека кінцевої точки:
- антивірус нового покоління (NGAV);
- виявлення та реагування на кінцеву точку (EDR);
- захист від витоку даних (DLP).

Типова архітектура DLP системи

6



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.

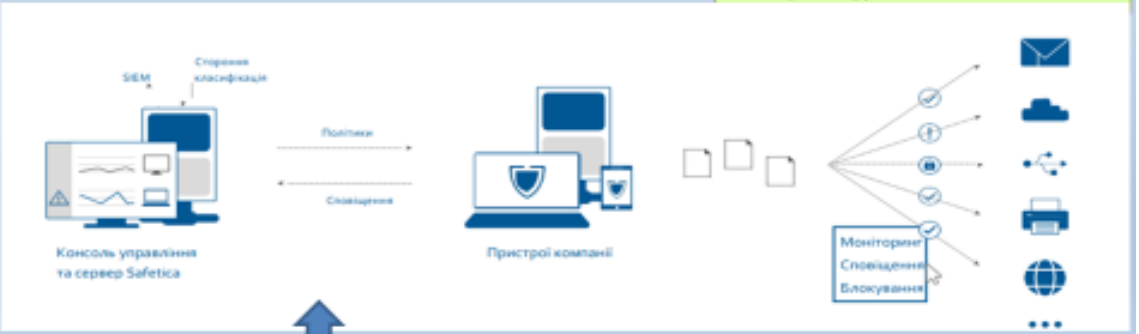


Схема роботи Safetica

Архітектура рішення Safetica ONE

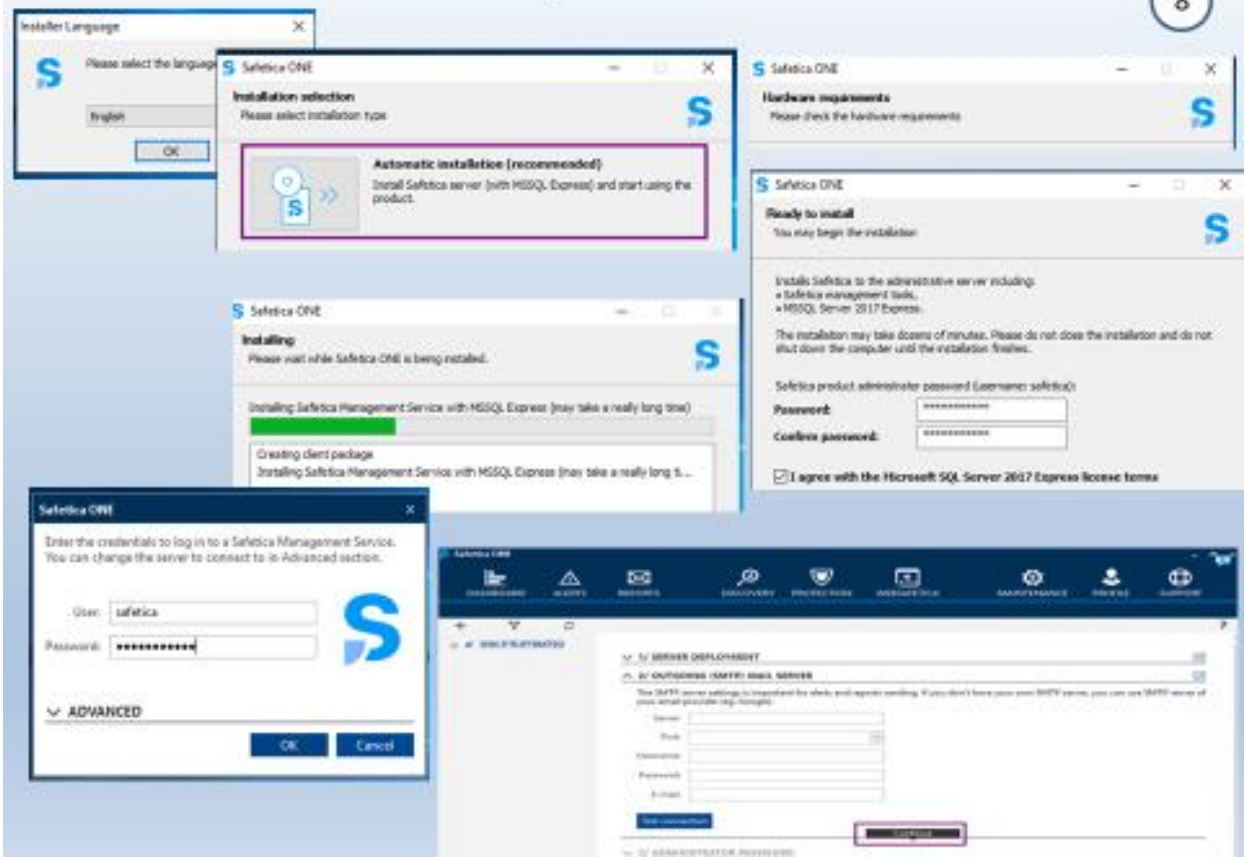
7

1. Комп'ютери та ноутбуки з Safetica Endpoint client: здійснюється запис дій і впровадження політики через додаток клієнта.
2. Safetica management services і бази даних SQL: дані автоматично передаються із мережевих комп'ютерів до сервера разом із синхронізованими даними ноутбука при підключенні до мережі. Налаштування клієнта синхронізується в зворотному порядку.
3. Safetica management console з налаштуваннями та результатами: всі дані доступні для перегляду в додатку керування, де також можуть бути змінені будь-які параметри.
4. Сервери Safetica management services в інших відгалудженнях: Safetica підтримує декілька відгалуджень із допомогою єдиної консолі керування.

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

Встановлення та налаштування DLP та її компонентів

8



Оптимізація та підвищення ефективності DLP-системи

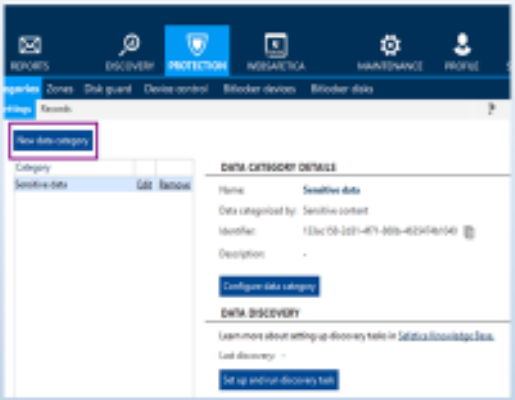
Успішна інтеграція будь-якого продукту в систему – це лише перший крок у використанні його функцій.

Рішення Safetica DLP складається з двох основних модулів: Discovery та Protection.

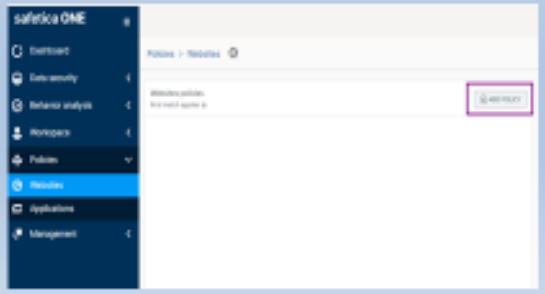
Розділ Discovery (огляд/виявлення) містить огляд потенційних проблем безпеки та дозволяє краще зрозуміти процеси безпеки. З його допомогою перевіряються конфіденційні файли, витік яких може становити загрозу безпеці.
Розділ Protection (захист) забезпечує захист конфіденційних корпоративних даних від несанкціонованого використання, та таким чином дозволяє запобігти фінансовим втратам та шкоді репутації.

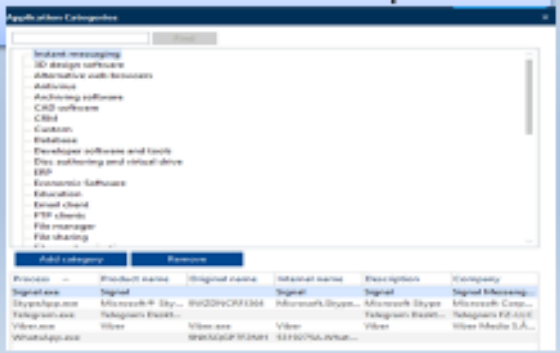
Для налаштування захисту спочатку потрібно визначити, які саме дані вважаються конфіденційними. Для цього потрібно провести відповідний аудит всередині організації та вирішити, які будуть ступені захищеності файлів. Safetica пропонує декілька видів класифікацій конфіденційних даних, щоб потім використовувати їх під час створення політик:
• на основі конфіденційного вмісту (Based on content (Sensitive content))
• на основі тегів сторонніх програм (Існуюча класифікація) (Based on data tagging by thirdparty applications (Existing classification))
• на основі контексту (Based on context (Context rules))
• на основі властивостей файлу (Based on file properties (File properties))
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 дозволяється створити необмежену кількість категорій даних. Категорії даних використовуються для класифікації файлів на різні групи залежно від того, хто, де і як може з ними працювати. Після створення категорій даних для них створюються різні DLP-політики і таким чином захищаються класифіковані дані.

Створення політики з розпізнавання IBAN та номерів карток



Аналогічним чином створюються політики з використанням тегів та політики з використанням WebSafetica та блокування месенджерів





Рекомендації щодо застосування технології протидії витокам даних в організації на основі DLP

11

Проаналізувавши попередні розділи та можливості технологій протидії витокам даних, було розроблено рекомендації щодо застосування технології протидії витокам даних в організації на основі DLP Safetica One приведені нижче.

Recommendations

1. Необхідно проаналізувати діяльність організації та сценарії витоку даних.
2. Розмежувати типи даних до відповідної категорії.
3. Оцінити наслідки та втрати витоку даних.
4. Вірно налаштувати DLP систему для протидії вторгнень.
5. Оптимізувати ефективність системи за допомогою тонких налаштувань політик безпеки та різних сервісів.
6. Поетапне впровадження DLP, починаючи з обмежених ділянок організації.
7. Навчання персоналу щодо правил та політик організації. Важливо зрозуміти, як працівники повинні поводитися з конфіденційною інформацією та як реагувати на повідомлення від системи.
8. Налаштування DLP для автоматичної реакції на порушення політики та введення механізмів попереджень для персоналу.
9. Постійний моніторинг роботи технології DLP та регулярне оновлення її правил та бази даних.
10. Інтеграція DLP з іншими засобами безпеки, такими як антивірусні програми, брандмауери, IDS/IPS та SIEM для створення комплексної системи безпеки.
11. Регулярне проведення аудиту ефективності технології DLP.

ВИСНОВКИ

12

У сучасному цифровому світі, де інформація стає все більш цінним ресурсом, забезпечення її безпеки набуває критичного значення. Несанкціонований доступ до інформаційних систем може призвести до серйозних наслідків, включаючи витік конфіденційних даних, фінансові втрати, репутаційні ризики та порушення нормативних вимог. Відповідно, питання захисту від несанкціонованого доступу є надзвичайно актуальним для організацій усіх рівнів та галузей.

В роботі було проаналізовано загрози інформаційній системі, поняття НСД. Важливість захисту від НСД його ризики на інформаційну систему організації та конфіденційних даних. Проаналізовані основні причини несанкціонованого доступу та їх наслідки для організації.

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

Встановлено та налаштовано систему DLP Safetica One. Проведена детальна оптимізація для підвищення ефективності системи DLP. Розроблено рекомендації щодо застосування технології DLP Safetica One.

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