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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія використання автоматизованого управління політиками безпеки на базі ESET Protect»

зі спеціальності *125 Кібербезпека та захист інформації*
(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

_____ Ярослав ШКЛЯР
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62
ШКЛЯР Ярослав
(прізвище, ім'я)

Керівник д-р філос., доц., МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DBIR	—	Data Breach Investigations Report
EDR	—	Endpoint Detection and Response
ПЗ	—	програмне забезпечення
ШІ	—	штучний інтелект
GDPR	—	General Data Protection Regulation
EPP	—	Endpoint Protection Platform
AV	—	Antivirus
ІБ	—	інформаційна безпека
ОС	—	операційна система
CVE	—	Common Vulnerabilities and Exposures
CMS	—	Centralized Management System
SOC	—	Security Operations Center
SIEM	—	Security Information and Event Management
RD	—	Rogue Detection Sensor
HIPS	—	Host-based Intrusion Prevention System

ВСТУП

Актуальність дослідження.

Сучасний етап розвитку інформаційних технологій характеризується експоненціальним зростанням кількості та складності кіберзагроз. Традиційні методи захисту, які покладаються на локальне адміністрування антивірусного ПЗ, виявляються неефективними проти скоординованих атак програм-вимагачів (Ransomware), цільового фішингу та загроз «нульового дня». В умовах, коли периметр корпоративної мережі стає розмитим через віддалену роботу, відсутність централізованого контролю над станом захищеності кожної робочої станції створює критичні вразливості, якими зловмисники користуються для проникнення в інфраструктуру.

Ключовою проблемою залишається «людський фактор» та складність підтримки актуальності налаштувань у великих мережах. Ручне оновлення баз даних, неконтрольоване підключення змінних носіїв та несвоєчасне встановлення патчів безпеки призводять до явища «дрейфу конфігурацій», коли реальний стан системи не відповідає затвердженим стандартам безпеки. Це вимагає переходу від реактивних методів реагування до проактивних систем управління, здатних автоматично застосовувати політики безпеки та виправляти недоліки без втручання адміністратора.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології використання автоматизованого управління політиками безпеки на базі ESET Protect та розробка рекомендацій щодо її застосування.

Об’єкт дослідження – процес автоматизованого управління політиками безпеки.

Предмет дослідження – технологія використання автоматизованого управління політиками безпеки на базі ESET Protect.

Мета роботи – дослідження технології використання автоматизованого управління політиками безпеки на базі ESET Protect та розробити рекомендації щодо її реалізації.

Наукові завдання:

проаналізувати кіберзагрози та актуальні вектори атак;

проаналізовати наслідки порушення політик безпеки та існуючі інструмент захисту;

обґрунтувати необхідність впровадження автоматизованих систем управління політиками безпеки;

дослідити методи та засоби централізованого управління безпекою;

дослідити призначення та функціональні можливості платформи ESET Protect;

розкрити порядок застосування технології використання автоматизованого управління політиками безпеки на базі ESET Protect;

розробити рекомендації фахівцям з кібербезпеки щодо застосування технології використання автоматизованого управління політиками безпеки на базі ESET Protect.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології використання автоматизованого управління політиками безпеки на базі ESET Protect, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Апробація результатів. Результати кваліфікаційної роботи апробовані на Всеукраїнській науково-практичній конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМАТИКИ ТА СУЧАСНОГО СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1. Аналіз кіберзагроз та актуальних векторів атак

Згідно зі звітом IBM Security «Cost of a Data Breach Report 2024», середня вартість витоку даних у світі досягла історичного максимуму і становить 4,88 мільйона доларів США, що на 10% більше порівняно з попереднім роком [1]. Це зростання зумовлене ускладненням атак та збільшенням часу, необхідного для виявлення та локалізації інцидентів.

Людський фактор: за даними звіту Verizon DBIR (Data Breach Investigations Report) 2024, понад 68% усіх порушень включають нетехнічний людський елемент, такий як помилки конфігурації, використання слабких паролів або успішний фішинг [2]. Це прямо вказує на необхідність автоматизованого примусового дотримання політик безпеки, які б нівелювали помилки персоналу.

Час реакції: середній час життєвого циклу атаки (від проникнення до усунення) становить близько 258 днів. Використання автоматизованих систем із застосуванням штучного інтелекту (AI) та автоматизації (наприклад, ESET Protect з модулем EDR) дозволяє скоротити цей час у середньому на 98 днів [1].

Атаки на ланцюги постачання: очікується, що до 2025 року 45% організацій у всьому світі зазнають атак на ланцюги постачання програмного забезпечення, що втричі більше, ніж у 2021 році [3].

Окрему увагу варто звернути на звіт ESET Threat Report (H2 2025). Компанія ESET зафіксувала різке зростання кількості загроз, пов’язаних із використанням вразливостей у застарілому програмному забезпеченні. Це підкреслює критичну важливість автоматизованого управління оновленнями (Patch Management), що є однією з ключових функцій досліджуваної системи ESET Protect [4].

Україна залишається полігоном для випробування новітніх кіберзагроз через триваючу гібридну війну. Згідно з аналітичними даними Держспецзв'язку та

урядової команди реагування CERT-UA, кількість кібератак на українську інфраструктуру залишається стабільно високою.

Основні вектори атак в Україні (за даними CERT-UA за 2023-2024 рр.):

Кількість інцидентів: зафіксовано понад 2 500 критичних кіберінцидентів за рік. Більшість із них спрямовані на державний сектор, енергетику та логістику [5].

Типи шкідливого ПЗ: домінуючими залишаються програми-вайпери (Wipers), призначені для знищення даних, а також шпигунське ПЗ (Spyware). Зростає активність груп, що використовують «living-off-the-land» бінарні файли (LOLBins) — легітимні інструменти ОС, які важко виявити стандартними антивірусами без налаштованих політик моніторингу [5].

Фішинг: понад 60% первинних векторів проникнення в українські організації відбувається через електронну пошту. Це вимагає жорстких політик фільтрації контенту та налаштування захисту поштових клієнтів на рівні кінцевих точок [6].

У 2025 році кібербезпека вступила в нову еру, що визначається безпрецедентними економічними проблемами та невпинними обсягами атак. Глобальний огляд є однозначним: кіберзлочинність — це не просто ІТ-проблема, це макроекономічна загроза та питання національної безпеки [7].

Таблиця 1.1.

Ключові глобальні показники у 2024 році порівняно з 2025 роком

Метрика	2024 рік	2025 рік	Відмінність
Річні витрати на кіберзлочинність	~8 трильйонів доларів США, орієнтовно.	10,5 трильйонів доларів США, орієнтовно.	+31% прогнозоване зростання у річному обчисленні
Середня світова вартість одного витоку даних	Рекордно високий показник у 4,88 мільйона доларів	4,44 мільйона доларів	Незначне зниження на −9%
Порушення, пов'язані з програмами-вимагачами	~32% порушень	44% порушень	Вища зараженість
Порушення за участю третіх осіб	~15% порушень	~30% порушень	Подвійний ризик ланцюга поставок
Глобальний ринок кіберстрахування	20,8 млрд доларів США у 2024 році	24–25 млрд доларів США, оцінка 2025 року	+18% зростання ринку
Незаповнені вакансії у сфері кібербезпеки	~4,02 мільйона розривів у 2024 році	Розрив у 4,8 мільйона	+19% погіршення дефіциту талантів

Розуміння того, як зловмисники потрапляють у вектори атак, є надзвичайно важливим. Статистика кібербезпеки за 2025 рік демонструє чіткий зсув у ландшафті атак, де деякі старі тактики розвиваються, а нові з'являються.

Таблиця 1.2.

Основні вектори атак

Вектор атаки	% порушень	Середня вартість порушення
Фішингова соціальна інженерія	15,9%	~$4,8 млн у середньому по всьому світу
Третя сторона/Ланцюг поставок	15% початкового вектора / ~30% залучають треті сторони загалом	~4,91 млн доларів США
Облікові дані	10%	~$4,5 млн. орієнтовно
Експлуатація вразливостей	20% порушень	~$4,8 млн, подібно до фішингу
Шкідливе програмне забезпечення (не програмне забезпечення-вимагач)	~17% орієнтовно.	~4,5 млн доларів США
Розгортання програм-вимагачів	44% порушень містили програмне забезпечення-вимагач	~5,15 млн доларів США у разі витоку даних
Зловмисні або недбалі внутрішні загрози	Кілька відсотків, точний відсоток варіюється, IBM посилається на ~8% зловмисних інсайдерів	~$4.92 млн. вектор найвищої середньої вартості
Неправильні конфігурації Хмара/IT	~1 з 5 порушень пов'язано з неправильною конфігурацією.	~5,05 млн доларів США, якщо задіяна хмара
Розподілена відмова в обслуговуванні DDoS	<5% як основна причина	Часто змінюється непряма вартість

Фішинг залишається точкою входу №1 . Незважаючи на роки навчання з обізнаності з безпеки, фішингові електронні листи, SMS та голосові афери продовжують обманювати співробітників і є безпосередньою причиною 16% порушень , а якщо врахувати будь-який фактор людської помилки, то вони можуть стати причиною до 80–90% порушень. Новим поворотом у 2025 році стало використання генеративного штучного інтелекту для посилення фішингу. Зловмисники тепер легко генерують ідеально сформульовані, контекстно-залежні приманки місцевими мовами, без граматичних помилок, які раніше були попереджувальними знаками [7]. Deepfake аудіо також використовувався через вішингові дзвінки, де голоси генеральних директорів клонуються для авторизації

шахрайських переказів. Ці досягнення означають, що фішингові атаки зараз переконливіші, ніж будь-коли, і саме тому цей метод досі так добре працює.

Збереження популярності програм-вимагачів : стверджуючи, що програми-вимагачі присутні у 44% порушень , ми маємо на увазі, що майже в половині інцидентів на певному етапі зловмисники намагалися зашифрувати дані для отримання викупу. Однак жертви стали більш стійкими, переважна більшість, понад 60%, тепер відмовляється платити викуп, особливо з покращенням резервного копіювання та планів відновлення. Це спонукало угруповання вимагачів змінити тактику: крадіжка даних та вимагання без програмного забезпечення для витоку шифрування зросли у 2025 році, як і багатосторонні атаки, що поєднують шифрування, витоки даних і навіть DDoS-загрози, так зване потрійне вимагання. Групи вимагачів також були спрямовані на критичну інфраструктуру та виробництво, де простої є найбільш болісними, щоб збільшити свій вплив [7].

Зростання кількості експлойтів у ланцюгах поставок стало визначальною зміною 2025 року. Коли ~30% порушень стосуються третіх сторін, це означає, що зловмисники активно переслідують постачальників програмного забезпечення, підрядників та сервісні компанії як трампліни. Один скомпрометований постачальник може надати доступ до десятків або сотень клієнтських мереж, що є множником сили для зловмисників. У цьому році спостерігалося кілька таких інцидентів, як-от компрометація популярного програмного забезпечення для управління IT, яка потім дала зловмисникам доступ до десятків клієнтів, що нагадує атаку SolarWinds 2020 року. Ця тенденція підкреслює важливість перевірки постачальників, використання мінімальних привілеїв для доступу третіх сторін та моніторингу партнерів у ланцюжку поставок.

Експлойти та невиправлені системи: Ще однією помітною тенденцією є відродження прямого злому через експлойти вразливостей . Оскільки багато організацій переходять до хмарних та віддалених робочих налаштувань, VPN, хмарні додатки та пристрої Інтернету речей розширили поверхню атаки. У 2025 році зловмисники скористалися цим: експлойти нульового дня в VPN-пристроях,

невиправлені вразливості програмного забезпечення, такі як сумнозвісний Log4j у 2021 році, та подібні недоліки з того часу призвели приблизно до кожного п'ятого порушення. Особливо тривожними були атаки на пристрої на межі мережі, такі як брандмауери, VPN-концентратори, їх кількість зросла у вісім разів після виявлення кількох критичних помилок. Цей вектор повністю обходить взаємодію з користувачем, це гонка між зловмисниками та захисниками за виправлення відомих недоліків. Урок очевидний: своєчасне управління виправленнями та віртуальне встановлення виправлень є важливими, оскільки експлойти можуть швидко стати широко поширеними [7].

Інсайдери та людські помилки залишаються постійною, хоч і меншою, складовою. Чи то зловмисник, який навмисно краде дані, чи помилка співробітника, який неправильно налаштовує базу даних, втрачає пристрій, людський фактор лежить в основі більшості інцидентів. Дані IBM за 2025 рік пояснюють 68% порушень людським фактором, включаючи фішинг, помилки та неправомірне використання. Зловмисники самі спричинили меншу частку, але ці порушення в середньому коштують найбільше, ймовірно, тому, що вони часто залишаються непоміченими довше та стосуються дуже конфіденційних даних, таких як комерційні таємниці або великі набори даних.

Нові вектори: У 2025 році також обговорювалися нові вектори, такі як розгортання працівниками тіньового ШІ інструментів ШІ або підключення програм ШІ до корпоративних даних без нагляду безпеки. Хоча тіньовий ШІ не є прямим вектором атаки в традиційному сенсі, його називали фактором, що збільшує витрати на порушення, розширюючи поверхню атаки. Наприклад, якщо працівник використовує несанкціонований SaaS зі ШІ, і цей SaaS порушується, можуть витікати дані компанії. Крім того, пристрої Інтернету речей зі слабким рівнем безпеки продовжували залучатися до ботнетів, таких як BadBox 2.0, які заражають мільйони смарт-телевізорів, що в першу чергу загрожує DDoS-атакам на доступність, а не даними, але тим не менш є частиною ландшафту загроз.

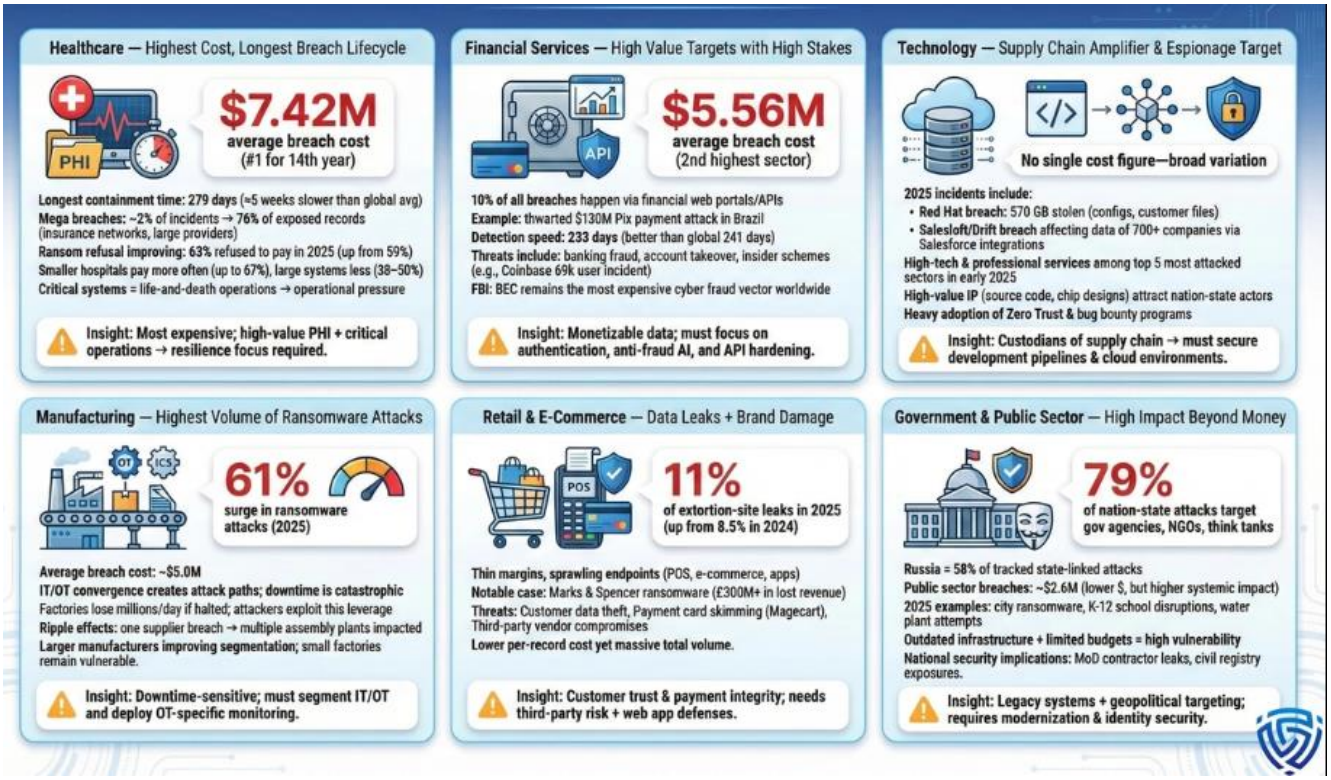

Рис. 1.1. Найбільш цільові групи векторів атак [7]

Певні галузі постійно зазнають найбільшого удару кібератак через цінність своїх даних та їхню толерантність (або відсутність) до простоїв. У 2025 році, хоча жоден сектор не залишився поза увагою, статистика показує, що деякі сектори постраждали сильніше за частотою, вартістю або і тим, і іншим.

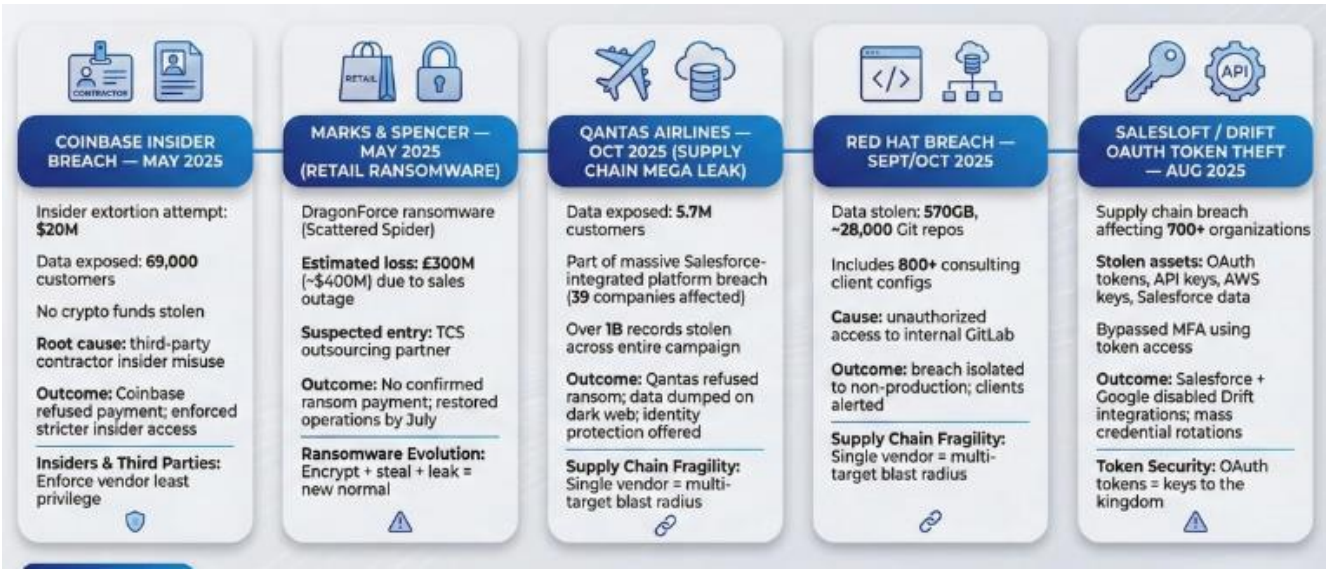

Рис. 1.2. Найбільш відомі кіберінциденти за 2025 рік [7]

Витік даних клієнтів Coinbase у травні 2025 року. Інсайдерська загроза та вимагання. Coinbase, одна з найбільших у світі криптовалютних бірж, повідомила, що між кінцем 2024 року та травнем 2025 року зловмисники-інсайдери, співробітники-підрядники стороннього постачальника підтримки, викрали дані користувачів. Витік став очевидним, коли зловмисники спробували вимагати 20 мільйонів доларів у Coinbase 11 травня 2025 року. Наслідки близько 69 000 клієнтів мали розкриті персональні дані, включаючи імена, контактну інформацію, часткові номери соціального страхування та документи, що посвідчують особу. На щастя, жодних криптовалютних активів чи закритих ключів не було викрадено. Причиною була внутрішня загроза через стороннього підрядника. Зловмисники, які видавали себе за іноземного персоналу підтримки або підкуповували його, отримали несанкціонований доступ до інформації користувачів. Це підкреслює ризик доступу персоналу ланцюга поставок/аутсорсингу до конфіденційних систем [7].

Атака програми-вимагача Marks & Spencer M&S у травні 2025 року. Програма-вимагач у роздрібній торгівлі. Marks & Spencer, велика британська мережа роздрібної торгівлі, зазнала руйнівної атаки програми-вимагача, яка вивела з ладу її платформу онлайн-покупок та деякі внутрішні системи. Атаку приписують хакерській групі Scattered Spider, яка використовує штам під назвою DragonForce . Хоча точна кількість клієнтів не підтверджена, вона, ймовірно, вплинула на сотні тисяч клієнтів. У M&S мільйони покупців. M&S довелося тимчасово призупинити онлайн-замовлення та деякі операції в ланцюжку поставок. Фінансовий вплив був величезним, за оцінками, він спричинив втрату прибутку в розмірі 300 мільйонів фунтів стерлінгів ~ 400 мільйонів доларів США через простої в продажах та витрати на усунення наслідків. Причиною була програма-вимагач через вразливість IT-аутсорсингу. Підозрюється, що порушення виникло через партнера M&S з IT-аутсорсингу Tata Consultancy Services, що означає використання сторонньої точки доступу. Зловмисники зашифрували віртуальні машини та викрали дані клієнтів, хоча жодного компрометування платіжної інформації не було підтверджено [7].

Витік даних авіакомпанії Qantas у жовтні 2025 року. Вимагання даних через порушення ланцюга поставок. Хакери викрали дані 5,7 мільйона клієнтів авіакомпанії Qantas після того, як авіакомпанія відмовилася від вимоги викупу. Це було частиною масштабного порушення сторонньої платформи обслуговування клієнтів на базі Salesforce, яка використовується Qantas та десятками інших компаній. Група зловмисників, альянс учасників Scattered Spider, ShinyHunters, Lapsus$, які називають себе Scattered Lapsus$ Hunters, заявила, що вкрала дані 39 компаній через цю атаку на ланцюг поставок, загалом понад мільярд записів у всьому світі. Для Qantas було розкрито персональні дані 5,7 мільйона пасажирів, такі як імена, контакти, дати народження, статус лояльності для подорожей тощо. Інші великі бренди, такі як Toyota, Disney, McDonald's, також були зазначені як жертви тієї ж кампанії. Це, по суті, був мега-витік через хмарного постачальника .

Витік даних Red Hat, вересень, жовтень 2025 р. Витік вихідного коду технологічної компанії. Хакерська група, яка називає себе Crimson Collective , оголосила про злам Red Hat, великого постачальника корпоративного програмного забезпечення та хмарних рішень, та викрала близько 570 ГБ даних із внутрішніх репозиторіїв. Вони опублікували списки файлів як доказ, стверджуючи, що отримали доступ до приблизно 28 000 приватних репозиторіїв Git, що належать консалтинговому бізнесу Red Hat. Витік нібито містить близько 800 звітів про взаємодію з клієнтами з детальною інформацією про IT-інфраструктуру та конфігурації для великих клієнтів Red Hat, які охоплюють фінанси, телекомунікації, уряд тощо [7].

Атака на ланцюг поставок Salesloft Drift у серпні 2025 року. Масова крадіжка токенів OAuth. Що сталося: Salesloft, платформа для взаємодії з продажами, мала інтегрований інструмент чату під назвою Drift, який був скомпрометований зловмисником UNC6395. Зловмисник викрав токени OAuth, які дозволяли отримати доступ до сотень даних клієнтів Salesforce. По суті, порушивши інтеграцію одного додатка, зловмисники проникли в CRM-системи Salesforce багатьох компаній. Через цей інцидент у ланцюжку поставок було викрито дані понад 700 організацій. Zscaler, компанія з безпеки, публічно повідомила про те, що

вона постраждала, і навіть такі великі імена, як Google та Allianz, опосередковано постраждали, оскільки до їхніх даних, підключених через Drift/Salesloft, було отримано доступ. Викрадені дані включали токени автентифікації, ключі API, ключі AWS, паролі та безліч конфіденційної інформації про клієнтів з облікових записів Salesforce, справ, користувачів тощо. Це типовий витік даних ланцюга поставок, який одночасно торкнувся кількох великих підприємств [7].

1.2. Наслідки порушення політик безпеки та аналіз існуючих інструментів захисту

Аналіз інцидентів показує, що відсутність автоматизованого контролю політик (наприклад, несвоєчасне блокування звільненого працівника або незаблоковані USB-порти) створює умови для реалізації загроз.

Ефективність системи захисту підприємства визначається не лише наявністю антивірусного програмного забезпечення, а й суворістю дотримання корпоративних політик безпеки. Порушення цих політик — чи то через зловмисні дії, чи через недбалість персоналу — призводить до критичних наслідків, які можна класифікувати за трьома основними категоріями: фінансові, операційні та репутаційні.

Фінансові та правові наслідки. Згідно з регламентом GDPR (General Data Protection Regulation), який є орієнтиром і для українського законодавства про захист персональних даних, штрафи за витік даних можуть сягати 4% від річного обороту компанії [8]. Окрім штрафів, сюди входять витрати на форензіку (розслідування), відновлення систем та компенсації клієнтам.

Операційні наслідки. Порушення політик доступності (наприклад, відсутність політики резервного копіювання або її формальне виконання) призводить до зупинки бізнес-процесів. За даними Gartner, середня вартість однієї хвилини простою IT-інфраструктури становить близько 5600 доларів США, залежно від масштабу підприємства [9].

Репутаційні ризики. Втрата довіри клієнтів є довгостроковим наслідком. Як зазначають аналітики Forrester, 38% клієнтів готові змінити постачальника послуг після того, як дізнаються про інцидент з безпекою у компанії [10].

Для забезпечення дотримання політик безпеки на ринку існує широкий спектр інструментів. Для обґрунтування вибору платформи ESET Protect необхідно провести порівняльний аналіз основних класів рішень.

EDR, EPP та AV – це інструменти захисту кінцевих точок, що охоплюють різні сфери захисту. EDR найкраще підходить для великих компаній, EPP – для середніх компаній, а антивірусне програмне забезпечення найкраще працює для окремих користувачів та невеликих команд. Великі підприємства, як правило, поєднують ці рішення, щоб отримати повністю розширені можливості захисту кінцевих точок [11].

Таблиця 1.3.

Порівняння EDR, EPP, AV

	EDR	**EPP**	**Antivirus**
Сфера захисту	Повна, покращена безпека з реагуванням на загрози в режимі реального часу.	Широкий захист з кількома розширеними можливостями, поєднує EDR та антивірус.	Базовий захист зосереджений на розпізнаних загрозах.
Основна функція	Виявляє, стримує, досліджує та усуває складні загрози.	Запобігає ризикам, виявляє їх та усуває.	Виявляє та видаляє відоме шкідливе програмне забезпечення.
Захист у режимі реального часу	Так, активно відстежує загрози та реагує на них.	Так, пропонує моніторинг у режимі реального часу та запобігання загрозам.	Так, але часто обмежується епізодичним скануванням.
Метод виявлення	Штучний інтелект, машинне навчання, поведінкова аналітика та розвідка загроз.	Виявлення на основі сигнатур, евристичний аналіз та поведінковий аналіз.	Виявлення на основі сигнатур, евристичний аналіз, перевірка цілісності.
Поведінковий аналіз	Розширений, використовує машинне навчання для виявлення нових або невідомих загроз.	Використовує поведінковий аналіз для виявлення та запобігання невідомим атакам.	Базові, часто обмежені встановленими діями.
Реагування на інциденти	Забезпечує ретельне розслідування, локалізацію та усунення наслідків.	Включає основні інструменти реагування та розслідування.	Обмежується блокуванням, карантином та видаленням виявленого шкідливого програмного забезпечення.

Виявлення та реагування на кінцеві точки (EDR) , також відоме як виявлення та реагування на загрози кінцевих точок (EDTR) – це рішення для безпеки кінцевих точок, яке постійно контролює пристрої кінцевих користувачів для виявлення та реагування на кіберзагрози, такі як програми-вимагачі та шкідливі програми [12].

Рішення безпеки EDR фіксують дії та події, що відбуваються на кінцевих точках та всіх робочих навантаженнях, забезпечуючи командам безпеки необхідну видимість для виявлення інцидентів, які в іншому випадку залишилися б непомітними. Рішення EDR повинно забезпечувати постійну та всебічну видимість того, що відбувається на кінцевих точках у режимі реального часу.

Платформи захисту кінцевих точок (EPP) розроблені для запобігання атакам як традиційних шкідливих програм, так і складних вірусів, таких як програми-вимагачі, вразливості нульового дня та атаки без використання файлів. Традиційна EPP за своєю суттю є превентивною, і більшість її підходів базуються на сигнатурах, що означає, що вони ідентифікують загрози за допомогою розроблених сигнатур файлів для нещодавно виявлених загроз [13]. До цього класу належить базовий функціонал ESET Endpoint Security. Вони об'єднують антивірус, фаєрвол, контроль пристроїв та веб-фільтрацію.

1.3. Обґрунтування необхідності впровадження автоматизованих систем управління політиками

В умовах зростання кількості кінцевих точок (робочих станцій, серверів, мобільних пристроїв) та ускладнення інфраструктури, традиційні підходи до забезпечення інформаційної безпеки (ІБ) стають критично неефективними. Впровадження автоматизованих систем управління, таких як ESET Protect, є актуальним і необхідним для забезпечення ІБ в організації.

Головною проблемою ручного адміністрування є лінійна залежність трудових витрат від кількості пристроїв. У великих інфраструктурах (понад 50–100 хостів) це призводить до ряду критичних вразливостей, а саме:

Дрейф конфігурацій (Configuration Drift). При ручному налаштуванні неминуче виникають відхилення від еталонного стану безпеки. Дослідження показують, що навіть досвідчені адміністратори припускаються помилок при повторюваних операціях. В результаті, різні сегменти мережі мають різний рівень захищеності, створюючи «сліпі зони» для атакуючих [14].

Затримка в часі реакції (Time-to-Patch). Критичні вразливості (CVE) часто експлуатуються хакерами протягом годин після їх оприлюднення. Ручне оновлення ПЗ на сотнях комп'ютерів може зайняти тижні, залишаючи компанію беззахисною перед експлойтами нульового дня. Автоматизовані системи дозволяють скоротити цей час до хвилин [15].

Відсутність спостережуваності (Observability). Без єдиної консолі управління неможливо миттєво відповісти на питання: "На скількох комп'ютерах зараз вимкнено антивірус?". У кризових ситуаціях (наприклад, атака вірусу-шифрувальника) відсутність актуальних даних унеможливлює прийняття правильних управлінських рішень.

Всі ці недоліки дозволяє вирішити рішення ESET Protect та Inspect, але в свою чергу до автоматизованого управління є свої певні вимоги, що регламентуються в стандартах та нормативних документах.

ISO/IEC 27001:2022. Стандарт вимагає впровадження технічних засобів контролю (Annex A). Зокрема, пункти A.8.9 (Configuration management) та A.8.19 (Installation of software on operational systems) неможливо ефективно реалізувати вручну у великій компанії. Автоматизація дозволяє забезпечити безперервний моніторинг та доказову базу для аудиту (Evidence collection) [16].

GDPR (General Data Protection Regulation). Регламент вимагає реалізації принципу "Privacy by Design" (Конфіденційність за дизайном). Це означає, що заходи безпеки (шифрування дисків, контроль доступу) повинні бути інтегровані в систему за замовчуванням. Крім того, стаття 33 вимагає повідомляти про витік даних протягом 72 годин, що можливо лише за наявності автоматизованих систем оповіщення про інциденти [8].

NIST SP 800-53 (Revision 5). Американський стандарт, що є еталоном для багатьох галузей, у сімействі контролів SI (System and Information Integrity) та CM (Configuration Management) прямо вказує на необхідність використання автоматизованих інструментів для виявлення несанкціонованих змін та управління оновленнями [17].

Отже, ESET PROTECT — централізована платформа управління захистом кінцевих точок, яка надає функції створення, призначення й автоматичного розповсюдження політик, керування агентами й моніторингу стану безпеки через веб-консоль. Компонентна архітектура (сервер, веб-консоль, ESET Management Agent, опційні RD Sensor/Bridge) дозволяє масштабувати систему для корпоративних середовищ і реалізувати автоматичні завдання та динамічні групи для автоматичного призначення політик. Це робить ESET PROTECT практичним вибором для реалізації вимог ISO/NIST/GDPR щодо централізації та доказовості виконання контролів.

Висновки до розділу 1

На основі проведеного аналізу обґрунтовано доцільність використання платформи ESET Protect як інструменту для автоматизації управління політиками безпеки. Впровадження цієї системи дозволить вирішити проблеми масштабованості, забезпечити централізований контроль над безліччю кінцевих точок та мінімізувати час реакції на інциденти. Це формує задачу для подальшого дослідження архітектури та функціональних можливостей ESET Protect у наступному розділі.

2 МЕТОДИ ТА ЗАСОБИ АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ПОЛІТИКАМИ БЕЗПЕКИ

2.1. Дослідження методів та засобів централізованого управління безпекою

Централізоване управління безпекою (CMS) — це підхід, за якого управлінські рішення, політики, моніторинг і реагування на події здійснюються з єдиної консолі чи централізованого сервера. Такий підхід сприяє узгодженості конфігурацій, швидкому розповсюдженню змін і зниженню операційних ризиків.

Централізоване управління безпекою може бути реалізовано за допомогою різних систем та інструментів. Кожен підхід виконує дещо різні функції, але сприяє досягненню загальної мети — створення єдиної системи безпеки.

Рис. 2.1. Підходи до впровадження CMS [18]

CMS (Centralized Management System): це основа стратегії. CMS надає панель інструментів для моніторингу та управління пристроями та політиками безпеки з центрального місця. Це «мозок», який з'єднує та контролює всі інші компоненти безпеки. Потужна CMS може отримувати дані та передавати політики до широкого спектру інструментів безпеки, від захисту кінцевих точок до централізованого управління брандмауером у всіх сегментах мережі [18].

Хмарне управління безпекою (Cloud-Based Security Management): цей підхід використовує масштабовану інфраструктуру для забезпечення централізованого нагляду в розподілених середовищах. Цей підхід є особливо ефективним для організацій з віддаленими працівниками або багатохмарними розгортаннями, забезпечуючи безпечну обробку даних [18].

SOC (Security Operations Center): SOC — це спеціальна команда або установа, яка контролює та аналізує стан безпеки організації. CMS надає технологію, а SOC — людські ресурси для інтерпретації даних, реагування на інциденти та налагодження політик.

SIEM (Security Information and Event Management): рішення SIEM агрегує та аналізує дані безпеки з різних джерел, щоб забезпечити перегляд загроз у режимі реального часу. Це критично важливий компонент для виявлення аномалій та генерації сповіщень, які інформують SOC про необхідність реагування [18].

Централізоване управління безпекою базується на концепції «Single Pane of Glass» (Єдина панель управління) — архітектурному підході, що об’єднує дані з різних джерел в єдиний інтерфейс для моніторингу та прийняття рішень.

Основні принципи побудови таких систем включають:

Уніфікація конфігурацій. Система повинна забезпечувати єдиний стандарт налаштувань для всіх однотипних об'єктів. Це реалізується через шаблони конфігурацій (Configuration Templates), що усуває варіативність, спричинену людським фактором [19].

Масштабованість архітектури. Система має підтримувати ієрархічну структуру серверів (Master/Slave або Cluster), що дозволяє керувати десятками тисяч хостів без зниження продуктивності.

Відокремлення площини управління від площини даних (Management Plane vs Data Plane). Канали передачі команд управління (політики) та канали передачі даних (оновлення баз, логів) мають бути логічно або фізично розділені для забезпечення надійності [20].

Для ефективного розподілу політик у великих мережах використовується методологія ієрархічного успадкування, яка базується на трьох ключових механізмах:

Ієрархія груп (Grouping). Комп'ютери об'єднуються в логічні структури (дерева), які часто дзеркалять структуру підприємства (наприклад, «Головний офіс» → «Бухгалтерія»).

Статичні групи: Адміністратор вручну додає пристрої.

Динамічні групи: Пристрої потрапляють автоматично на основі критеріїв (наприклад, «ОС Windows 10» або «Застарілий антивірус»).

Успадкування (Inheritance). Політики, призначені для батьківської групи (Parent Group), автоматично застосовуються до всіх дочірніх груп (Child Groups) та об'єктів у них. Це дозволяє задати «Базову політику безпеки» на кореневому рівні (наприклад, пароль на налаштування), яка буде діяти для всіх [21].

Пріоритетність (Policy Merging). У складних середовищах на один комп'ютер може діяти кілька політик одночасно. Алгоритм обробки конфліктів зазвичай виглядає так:

Specificity: Політика, призначена безпосередньо клієнту, має вищий пріоритет, ніж політика групи.

Merging: Якщо політики керують різними параметрами, вони об'єднуються.

Force: У системах класу ESET Protect існує можливість встановити флаг «Force», який змушує батьківську політику перезаписувати будь-які локальні налаштування, забороняючи їх зміну на нижчих рівнях [22].

Ієрархія політик — це система, де політики розташовуються від загального (глобального) рівня до специфічного (локального/групового). Наприклад:

Глобальні політики — застосовуються до всієї організації.

Групові політики — налаштовані для певних груп пристроїв (сервери, робочі станції, віддалені офіси).

Локальні політики — особливі правила, що застосовуються до окремих вузлів або підгруп.

Це дозволяє делегувати управління при збереженні централізованих стандартів [16].

При проектуванні системи захисту критично важливим є вибір методу взаємодії сервера управління з кінцевими точками [23].

1. Безагентний підхід (Agentless). Використовує стандартні протоколи ОС (WMI, RPC, SSH) або API гіпервізора для збору даних.

2. Агентний підхід (Agent-based). Передбачає встановлення спеціалізованого сервісу (Management Agent) на кожну кінцеву точку. Саме цей підхід використовується в ESET Protect.

Аналіз методів показує, що для побудови надійної системи захисту кінцевих точок найбільш ефективним є використання агентної архітектури з ієрархічною моделлю політик. Це забезпечує безперервність захисту незалежно від підключення до мережі та дозволяє гнучко керувати налаштуваннями через механізми успадкування та примусового застосування (Forcing).

2.2. Архітектура рішення ESET Protect та взаємодія компонентів

ESET PROTECT — це система віддаленого керування нового покоління.

Для розгортання програм безпеки ESET, необхідно інсталювати такі компоненти (платформи Windows та Linux):

•Сервер ESET PROTECT

•Веб-консоль ESET PROTECT

•Агент керування ESET

Та допоміжні компоненти, які є необов'язковими, але їх встановлення забезпечує кращу продуктивність програми в мережі:

•Датчик RD

•ESET Bridge (HTTP-проксі)

Компоненти ESET PROTECT використовують сертифікати для зв’язку із сервером ESET PROTECT.

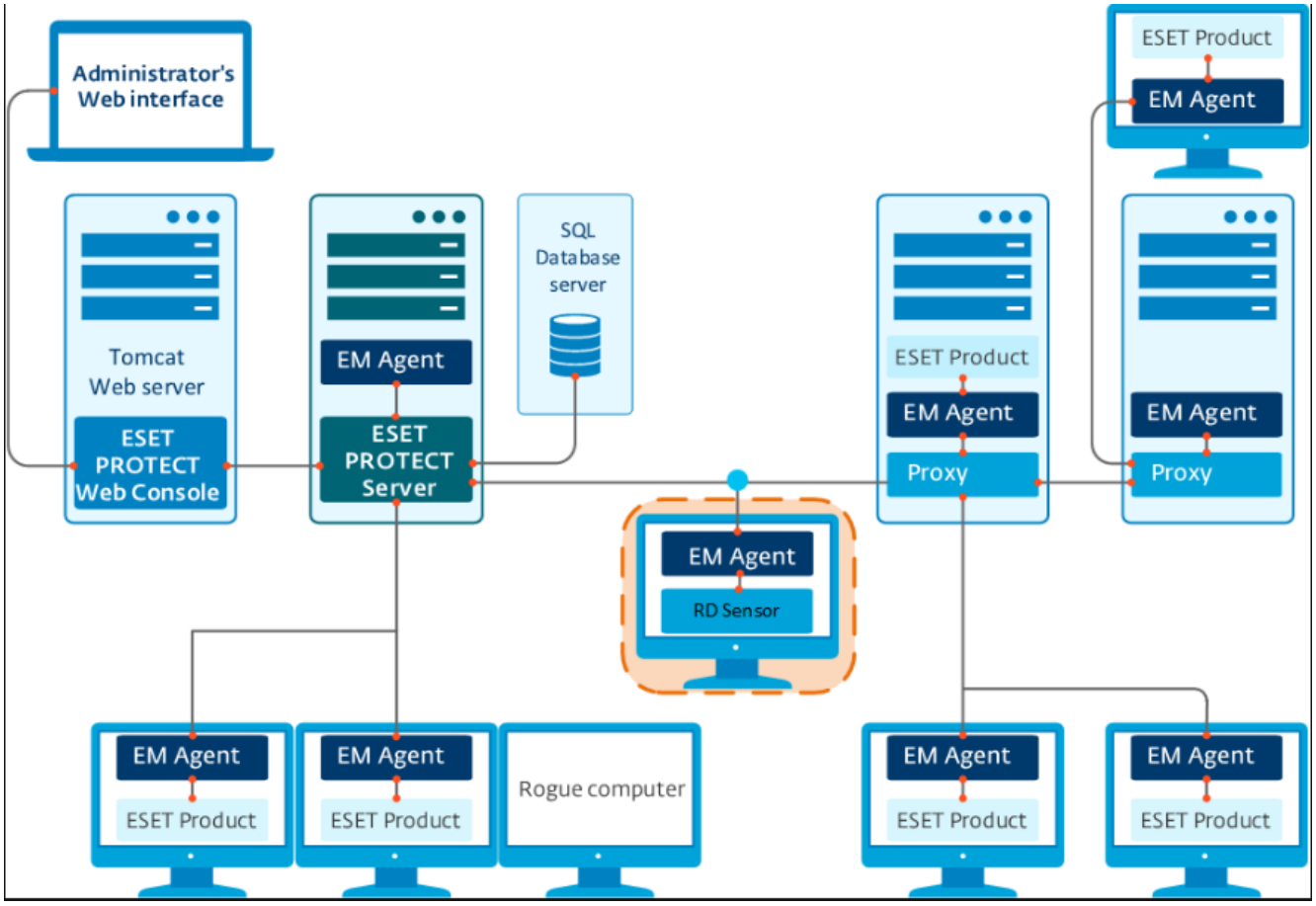

Рис. 2.2. Архітектура ESET Protect

Розглянемо детальніше компоненти архітектури ESET Protect.

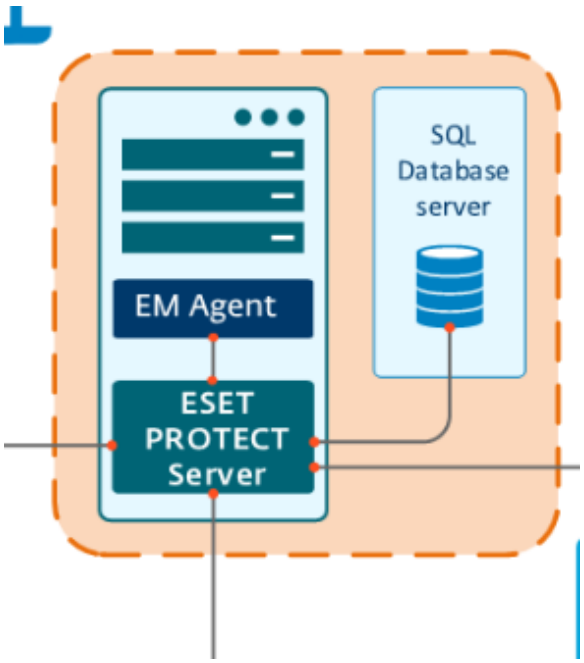

Рис. 2.3. ESET PROTECT Server [24]

ESET PROTECT Server – це виконавча програма, яка обробляє всі дані, отримані від клієнтів, що підключаються до Сервера (через агент ESET Management або HTTP-проксі). Для правильної обробки даних Серверу потрібне стабільне підключення до сервера бази даних, де зберігаються мережеві дані. Для досягнення кращої продуктивності рекомендуємо встановити сервер бази даних на іншому комп'ютері [24].

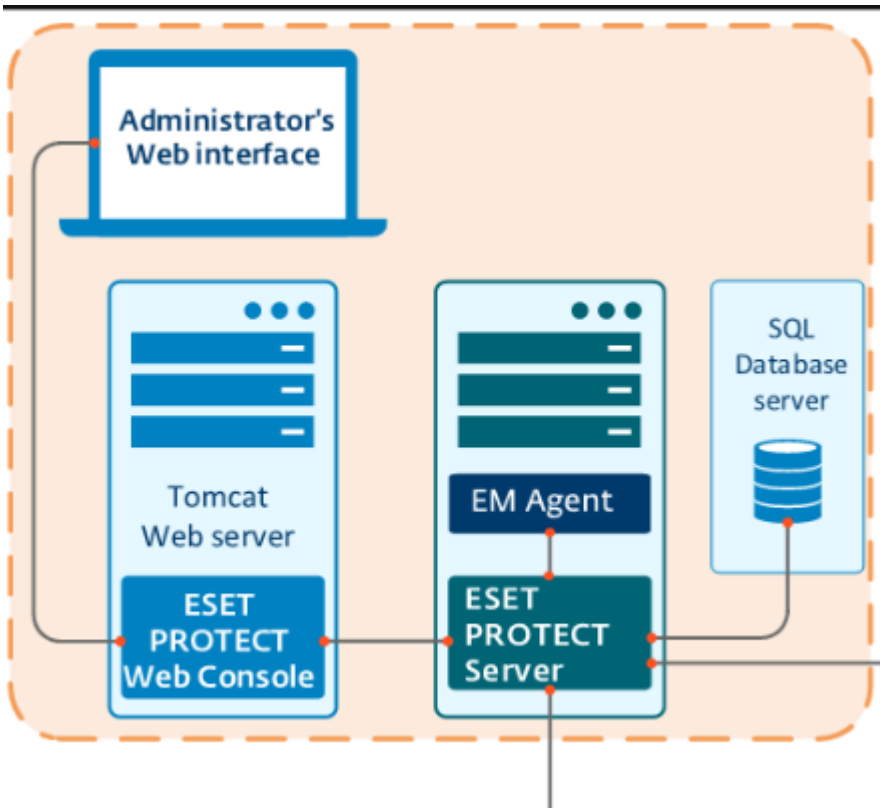

Рис. 2.4. Web Console [25]

Веб-консоль ESET PROTECT — це веб-інтерфейс користувача, який дозволяє керувати модулями безпеки ESET у вашому середовищі. Він відображає огляд стану клієнтів у вашій мережі та може використовуватися для віддаленого розгортання модулів ESET на некерованих комп'ютерах. Доступ до веб-консолі здійснюється за допомогою браузера. Якщо ви вирішите зробити веб-сервер доступним з Інтернету, ви зможете використовувати ESET PROTECT практично з будь-якого місця та пристрою.

Веб-консоль використовує Apache Tomcat як веб-сервер HTTP. Під час використання Tomcat, що входить до складу інсталятора ESET або віртуального пристрою, дозволяється підключення до веб-консолі лише через TLS 1.2 та 1.3 [25].

Агент ESET Management є важливою частиною ESET PROTECT On-Prem. Клієнти не взаємодіють із сервером ESET PROTECT безпосередньо, а агент забезпечує цей зв'язок. Агент збирає інформацію від клієнта та надсилає її на сервер ESET PROTECT. Якщо сервер ESET PROTECT надсилає завдання для клієнта, воно надсилається агенту, який потім надсилає це завдання клієнту. Агент ESET Management використовує новий, покращений протокол зв'язку [26].

Для спрощення впровадження захисту кінцевих точок до пакету ESET PROTECT On-Prem включено автономний агент ESET Management. Це простий, високомодульний та легкий сервіс, що охоплює весь зв'язок між сервером ESET PROTECT та будь-яким модулем або операційною системою ESET. Замість безпосереднього зв'язку із сервером ESET PROTECT, програми ESET взаємодіють через агента. Клієнтські комп'ютери, на яких встановлено агент ESET Management і які можуть взаємодіяти із сервером ESET PROTECT, називаються «керованими». Ви можете встановити агент на будь-який комп'ютер, незалежно від того, чи встановлено інше програмне забезпечення ESET [26].

Переваги:

•просте налаштування — ви можете розгорнути Агента як частину стандартної корпоративної інсталяції.

•керування безпекою на місці — оскільки Агента можна налаштувати для зберігання кількох сценаріїв безпеки, час реакції на виявлення значно скорочується.

•керування безпекою в автономному режимі — агент може реагувати на подію, якщо він не підключений до сервера ESET PROTECT [26].

Rogue Detection Sensor (RD Sensor) – це інструмент для виявлення несанкціонованих систем, який шукає комп'ютери у вашій мережі. Sensor зручний тим, що може знаходити нові комп'ютери з ESET PROTECT On-Prem без необхідності їх пошуку та додавання вручну. Виявлені машини миттєво

визначаються місцезнаходженням та повідомляються про них у попередньо визначеному звіті, що дозволяє переміщувати їх до певних статичних груп та виконувати завдання управління [27].

ESET Bridge — це програмне забезпечення ESET, засноване на відкритому програмному забезпеченні Nginx, яке було адаптовано для потреб рішень безпеки ESET [28].

2.3. Призначення та функціональні можливості платформи ESET Protect

Платформа ESET Protect є еволюційним розвитком консолі управління ESET Remote Administrator. Це комплексне рішення класу XDR-enabler (Extended Detection and Response), призначене для централізованого управління безпекою у гетерогенних мережах, що включають робочі станції, сервери, мобільні пристрої та віртуальні машини.

Основне призначення ESET Protect полягає у забезпеченні оркестрації (узгодженого управління) засобами захисту підприємства. Система вирішує наступні завдання:

Забезпечення видимості (Visibility): надання повної картини стану інфраструктури в реальному часі. Адміністратор отримує дані про версії ОС, встановлене ПЗ, апаратну конфігурацію та статус захисту кожного хоста.

Управління життєвим циклом безпеки: автоматизація процесів розгортання агентів, активації ліцензій, оновлення сигнатурних баз та модулів продуктів без втручання користувачів.

Забезпечення відповідності (Compliance): контроль дотримання корпоративних політик безпеки та автоматичне виправлення відхилень (наприклад, примусове увімкнення фаєрволу, якщо користувач його вимкнув) [29].

Функціонал платформи можна розділити на кілька стратегічних блоків, які реалізуються через механізм політик та клієнтських завдань.

1. Управління захистом кінцевих точок (Endpoint Management). Це базовий функціонал, що дозволяє дистанційно налаштовувати параметри продуктів ESET Endpoint Security:

Сканування на віруси: запуск повного або вибіркового сканування за розкладом або за вимогою.

HIPS (Host-based Intrusion Prevention System): налаштування правил моніторингу системних процесів, реєстру та додатків для захисту від складних загроз.

Мережевий захист: керування персональним брандмауером, захистом від ботнетів та атак перебором паролів.

2. Управління вразливостями та оновленнями (Vulnerability & Patch Management). Починаючи з нових версій, ESET Protect інтегрує функціонал сканування ОС та стороннього ПЗ на наявність відомих вразливостей (CVE).

Система автоматично пріоритезує вразливості за шкалою критичності та дозволяє розгорнути патчі (оновлення) централізовано, перезавантажуючи комп'ютери [30].

3. Шифрування даних. Модуль дозволяє керувати повнодисковим шифруванням на робочих станціях Windows та macOS безпосередньо з консолі.

4. Хмарна пісочниця (ESET LiveGuard Advanced). Технологія превентивного захисту від загроз нульового дня.

Підозрілі файли, які ще не відомі антивірусним базам, автоматично відправляються в хмару ESET, де запускаються в ізольованому середовищі. Результат аналізу автоматично передається в консоль ESET Protect, і файл блокується у всій мережі [23].

Особливістю архітектури ESET Protect є наявність інструментів для автоматизації рутинних дій адміністратора.

Динамічні групи: Це механізм фільтрації клієнтів на основі логічних умов. На відміну від статичних груп, склад динамічних змінюється автоматично.

Група "Застаріла ОС". Умова: "Версія ОС < Windows 10 22H2". Як тільки ПК оновлюється, він автоматично зникає з цієї групи та переходить в групу "Актуальні ОС". Політики прив'язуються саме до цих груп, що забезпечує автоматичне застосування правил.

ESET SysInspector: інструмент для створення детальних «знімків» (snapshots) стану системи. Він збирає інформацію про запущені процеси, стан реєстру, мережеві з'єднання. Дозволяє порівняти два знімки (до інциденту і після) для виявлення змін, внесених шкідливим ПЗ.

Звітність та сповіщення: система містить понад 170 вбудованих шаблонів звітів.

Висновки до розділу 2

У другому розділі кваліфікаційної роботи проведено методологічне дослідження засобів автоматизованого управління інформаційною безпекою та детально проаналізовано архітектуру платформи ESET Protect її основні функції та можливості.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ПОЛІТИКАМИ БЕЗПЕКИ НА БАЗІ ESET PROTECT

3.1. Розроблення варіанта розгортання технології автоматизованого управління політиками безпеки на базі ESET Protect

Комплексний інсталятор дозволяє інсталювати всі компоненти ESET PROTECT за допомогою майстра локальної інсталяції ESET PROTECT.

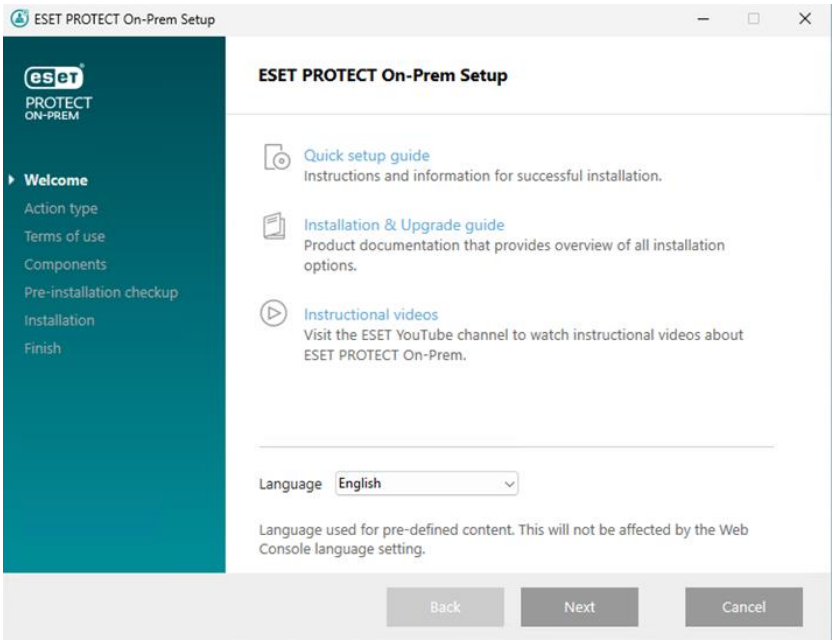

Рис. 3.1. Вибір мови інсталяції

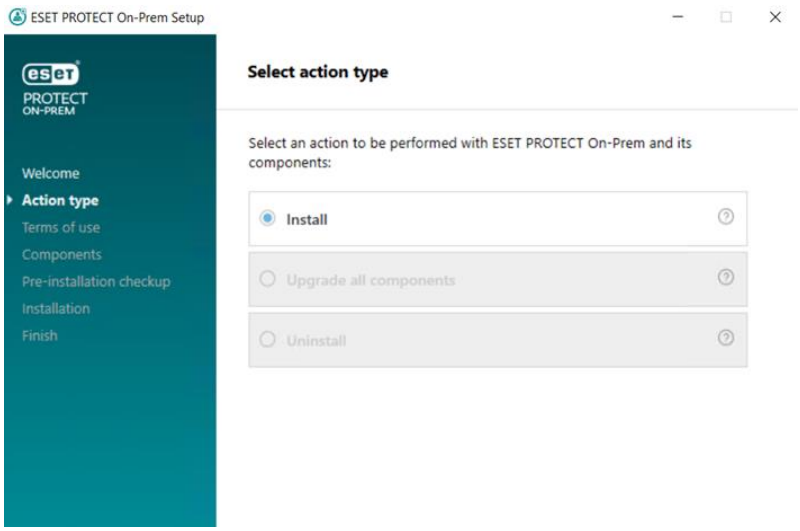

Рис. 3.2. Початок інсталяції

Установіть прапорець «Участь у програмі покращення продукту» , щоб надсилати анонімні дані телеметрії та звіт про збої до ESET (версія та тип ОС, версія програми ESET та інша інформація, що стосується програми). Виберіть « Я приймаю умови використання» та натисніть «Далі» (рис. 3.3).

Виберіть компоненти для встановлення та натисніть кнопку «Далі» .

Microsoft SQL Server Express;

Додати власний HTTPS-сертифікат для веб-консолі;

Датчик виявлення несанкціонованих дій;

Проксі-сервер ESET Bridge.

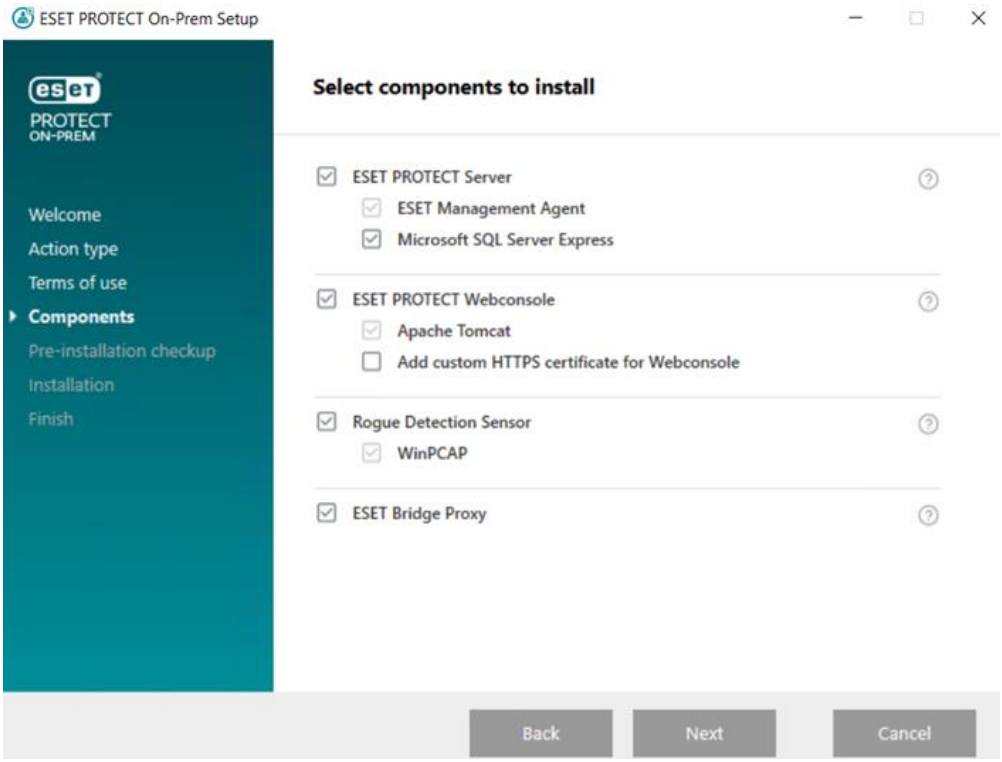

Рис. 3.3. Вибір компонент

Якщо ви вибрали опцію «Додати власний сертифікат HTTPS для веб-консолі» , натисніть «Огляд». Виберіть дійсний сертифікат (файл .pfx або .p12) і введіть його пароль. Залиште поле порожнім, якщо парольної фрази немає. Інсталятор встановить сертифікат для доступу до веб-консолі на вашому сервері Tomcat. Натисніть «Далі», щоб продовжити (рис. 3.4.).

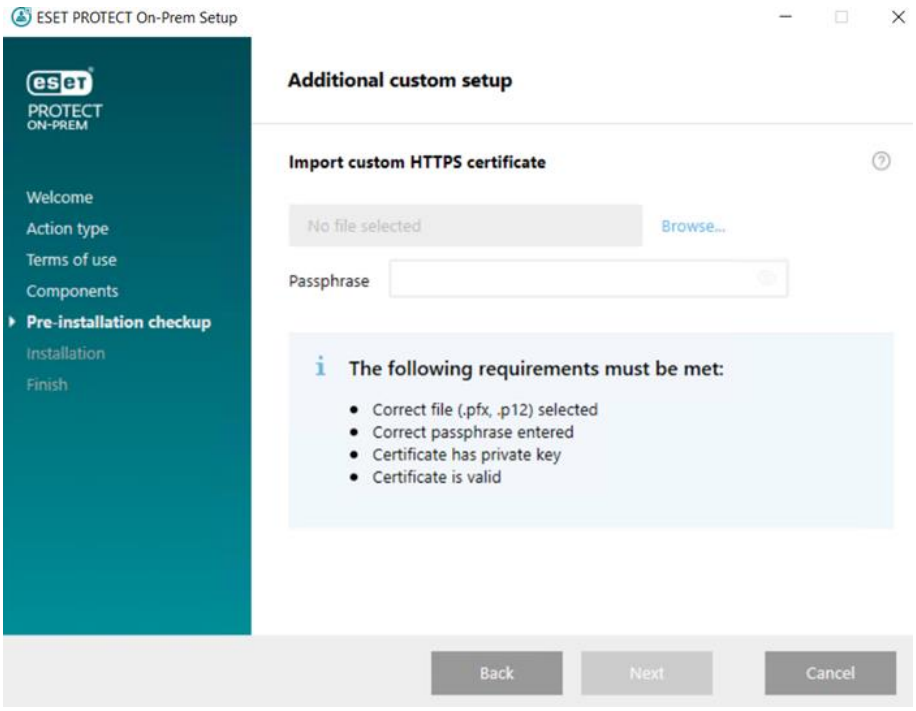

Рис. 3.4. Вибір сертифікату

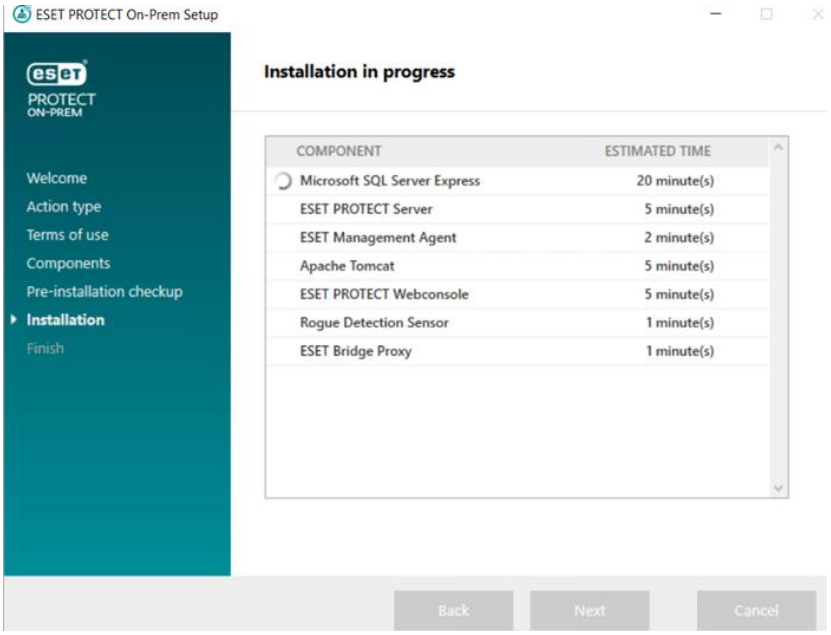

Рис. 3.5. Прогрес інсталяції

Якщо ви вирішили встановити Microsoft SQL Server Express , інсталятор виконає перевірку підключення до бази даних. Якщо у вас вже є сервер бази даних, інсталятор запропонує вам ввести дані підключення до бази даних

Інсталятор запропонує вам ввести пароль для облікового запису адміністратора веб-консолі. Цей пароль важливий — використовуйте його для входу у веб-консоль ESET PROTECT (рис. 3.6.).

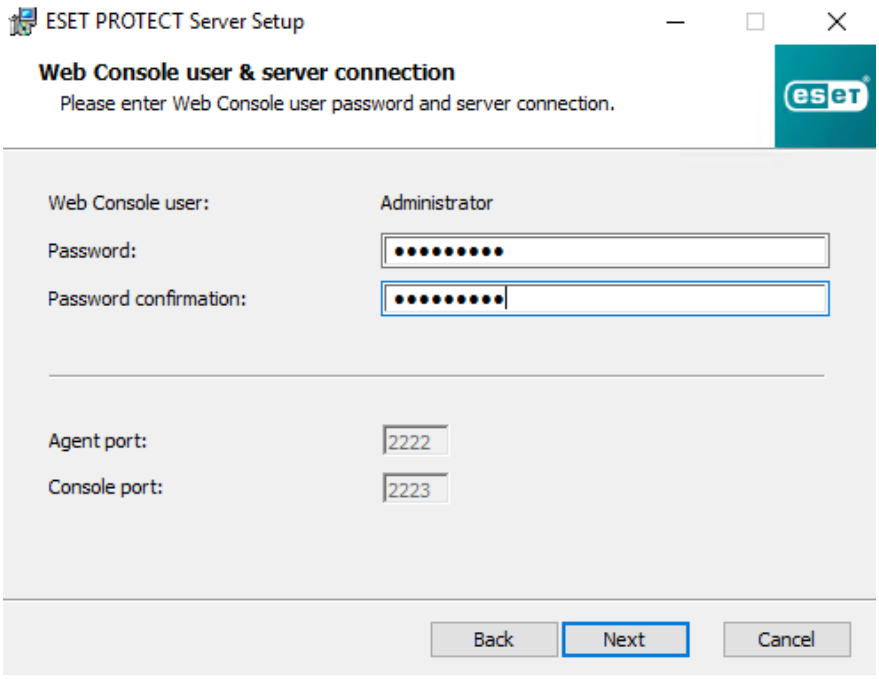

Рис. 3.6. Встановлення пароля адміністратора веб-консолі

Залиште поля без змін або введіть корпоративну інформацію, яка відображатиметься в даних агента ESET Management та сертифікатів сервера ESET PROTECT. Якщо ви вирішили ввести пароль у полі «Пароль авторизації» , обов’язково запам’ятайте його (рис. 3.7.).

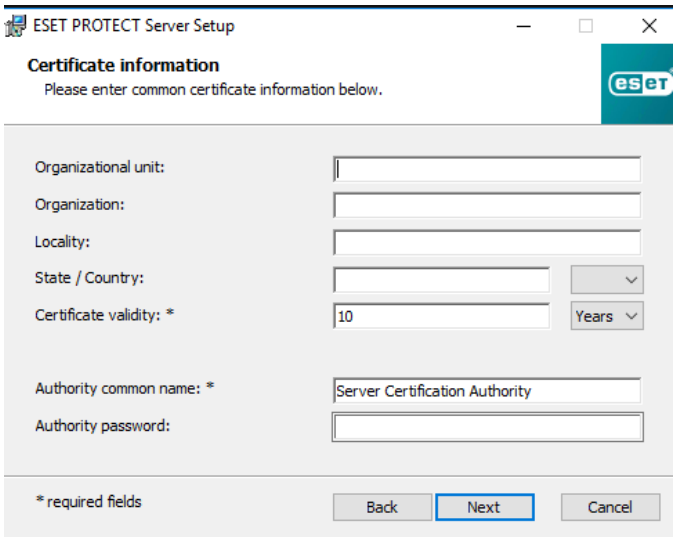

Рис. 3.7. Внесення корпоративної інформації

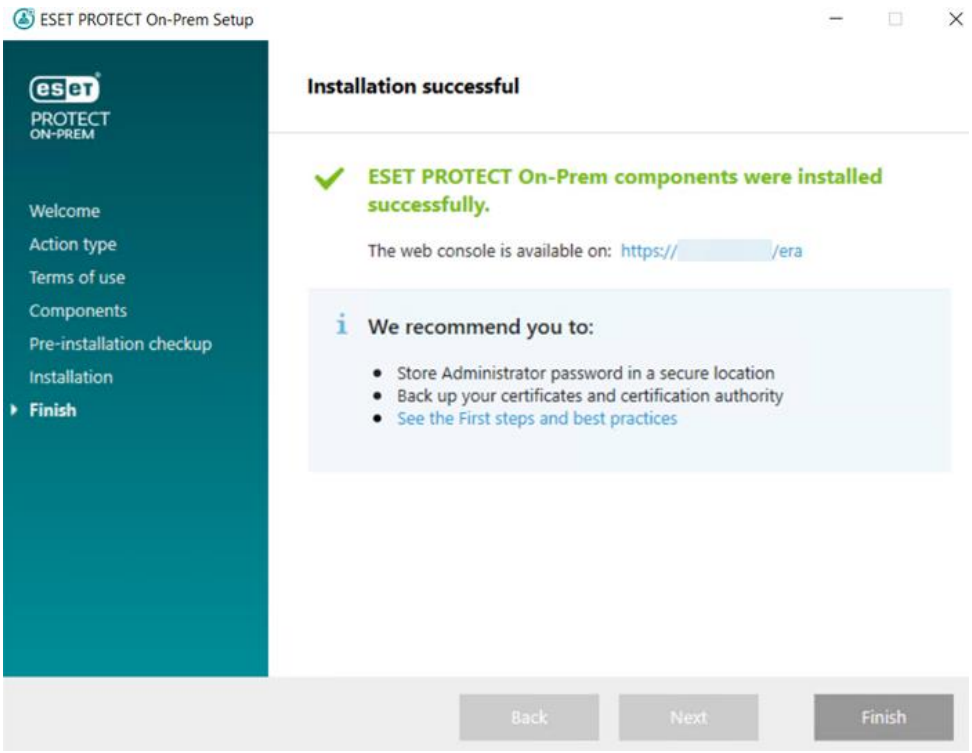

Рис. 3.8. Завершення інсталяції

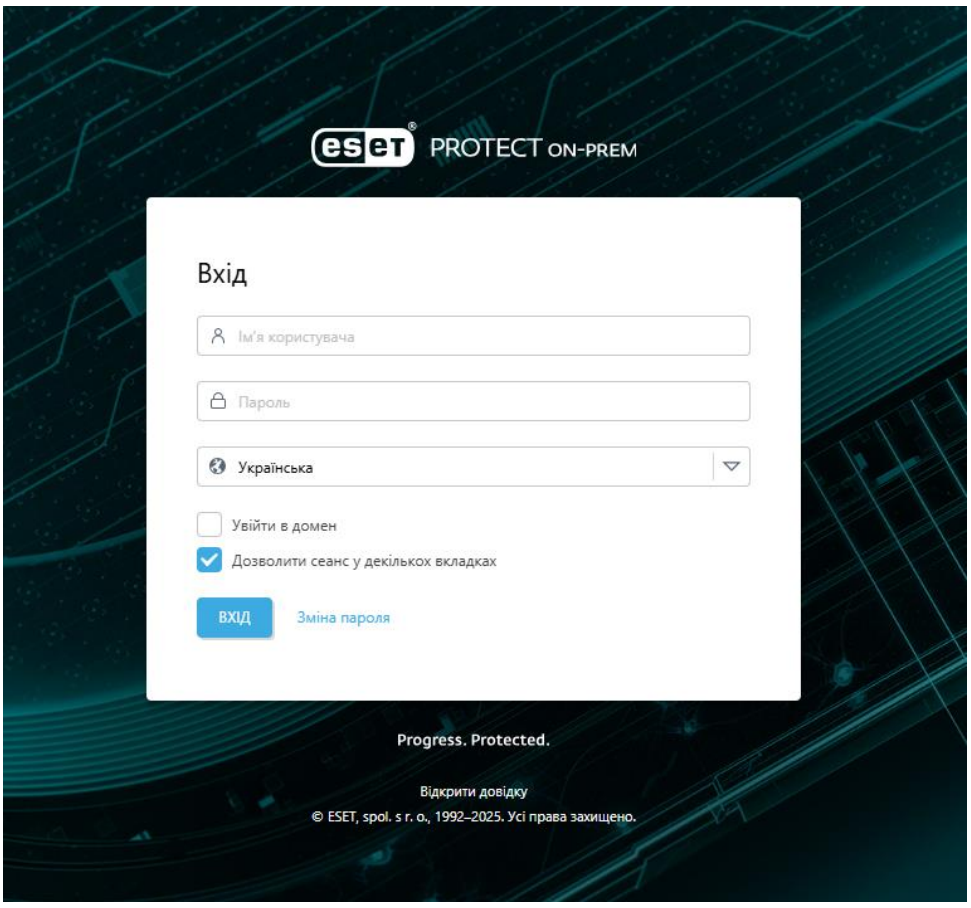

Рис. 3.9. Вхід у веб-консоль

Створюємо та впроваджуємо політику агресивного моніторингу та реагування.

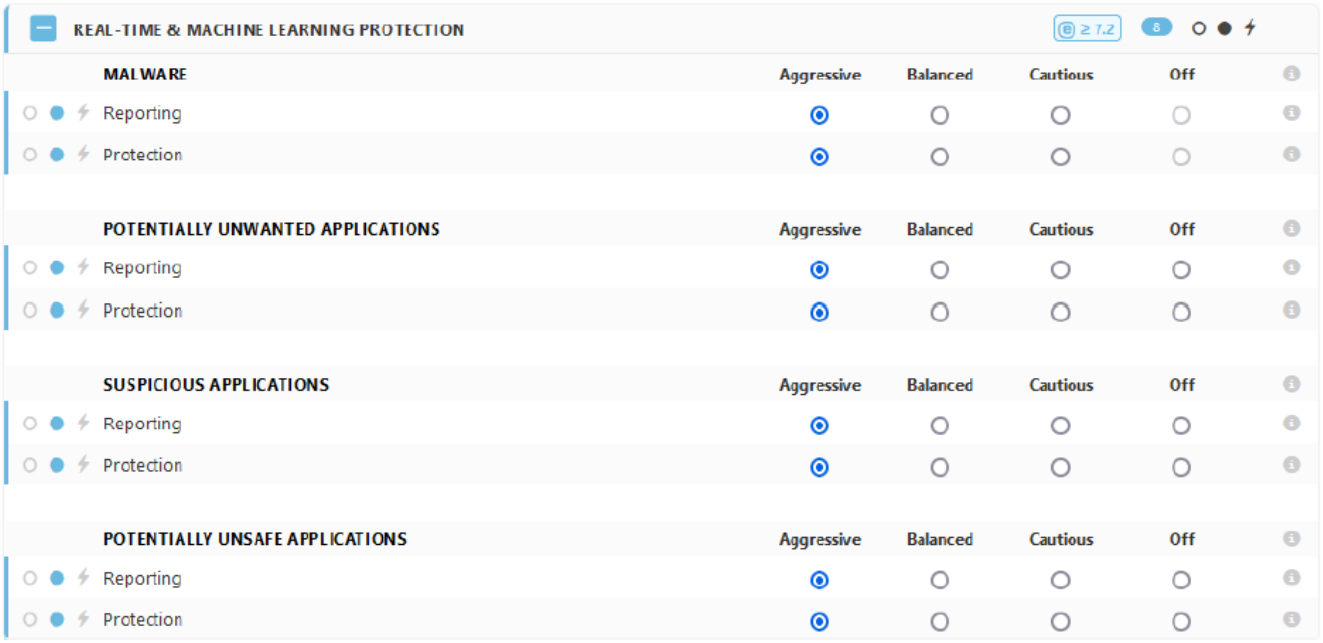

Рис. 3.10. Матриця захисту

Вимикаємо режим заміщення політик, щоб уникнути випадки зміни або відключення політик користувачами чи зловмисниками.

Вимикаємо служби ESET CMD та ESET RMM. Таким чином виключаємо ризик використання функцій для RDP або виконання зловмисних дій в інфраструктурі (рис. 3.11.).

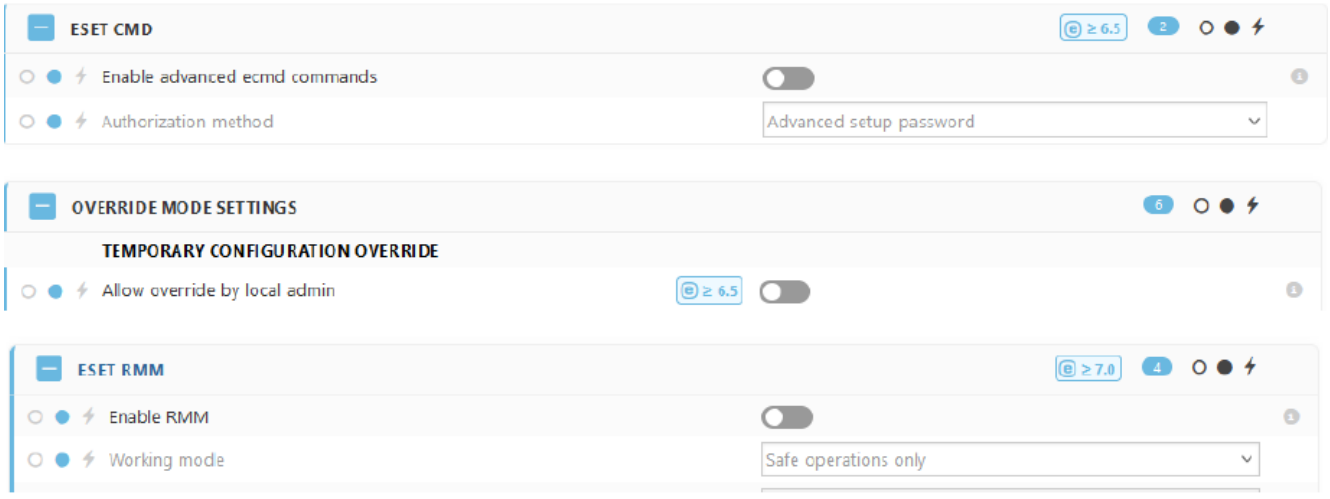

Рис. 3.11. CMD, Override, RMM

Рис. 3.12. Встановлення паролей на внесення змін політик

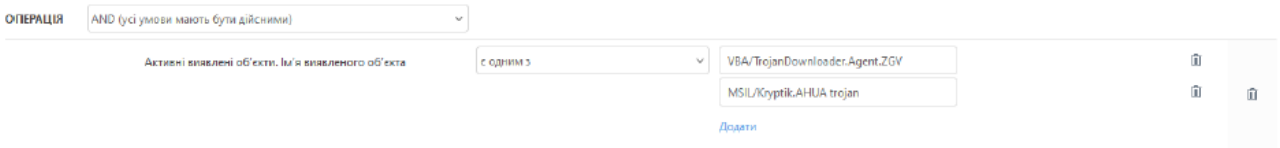

Рис. 3.13. Створення динамічних груп

Після створення динамічних груп, застосовуємо політики aggressive mode. Також налаштовуємо автоматичний збір журналів ESET Log Collector (ELC) та SysInspector для кожної кінцевої точки, яка потрапила до групи (рис. 3.14.).

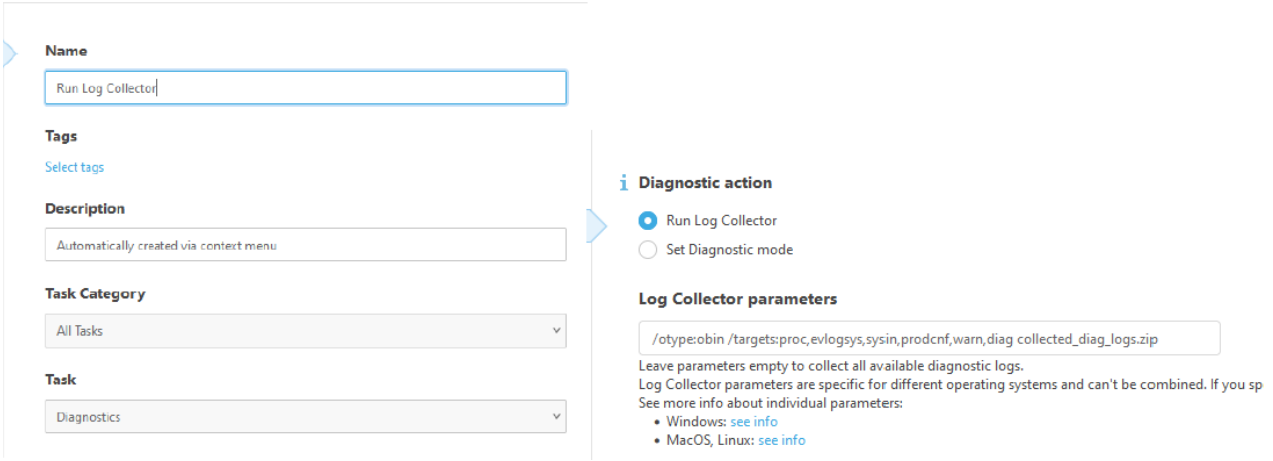

Рис. 3.14. Політика на автоматичний збір журналів

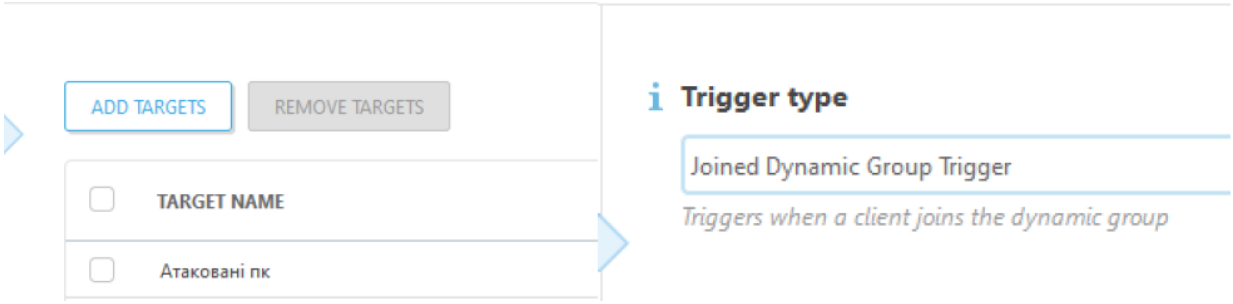

Рис. 3.15. Створення тригерів спрацювання

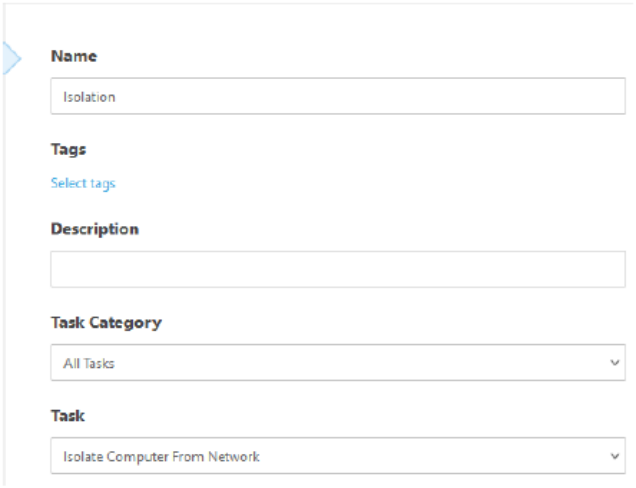

Рис. 3.16. Створення ізоляції при порушенні політик безпеки

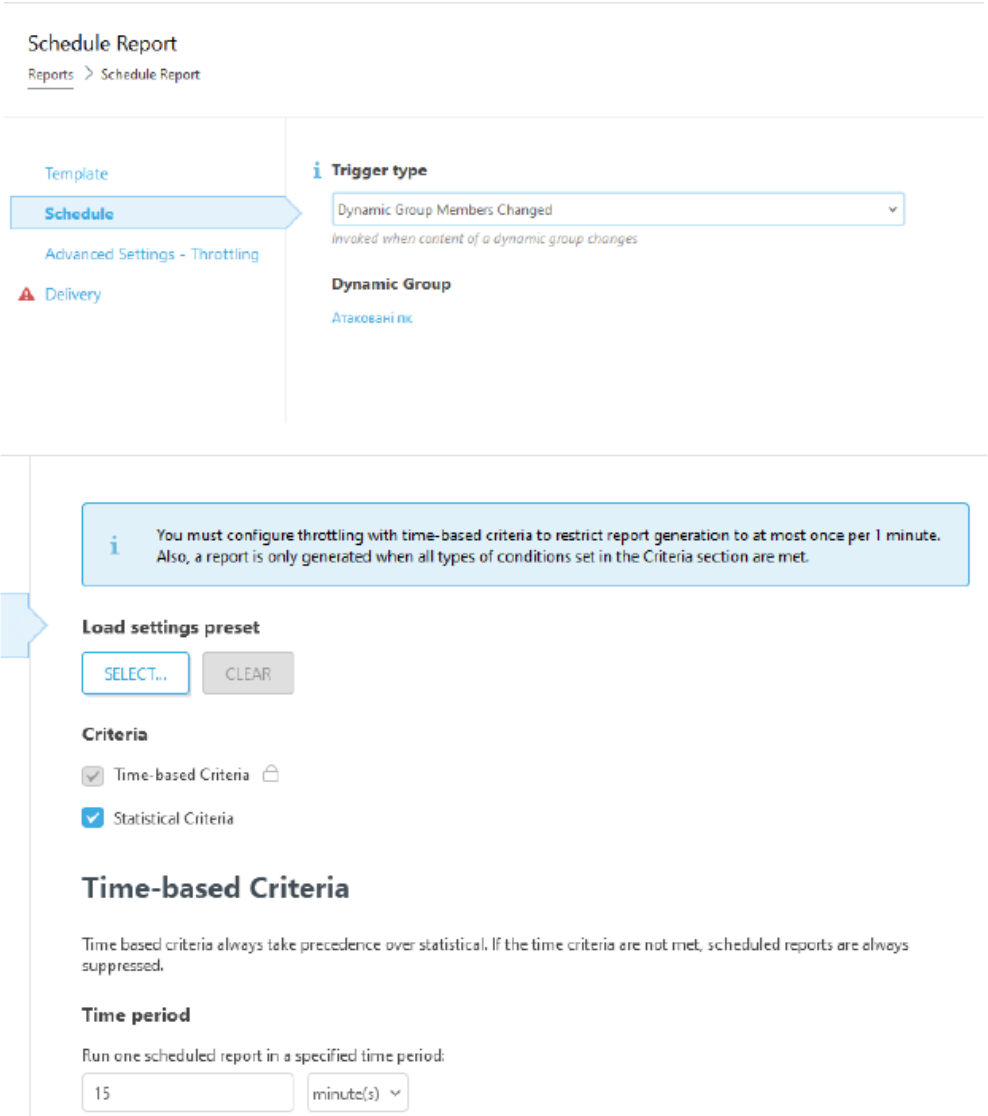

Рис. 3.17. Створення автоматичної періодичної звітності

3.2. Технологія автоматизованого управління політиками безпеки на базі ESET Protect

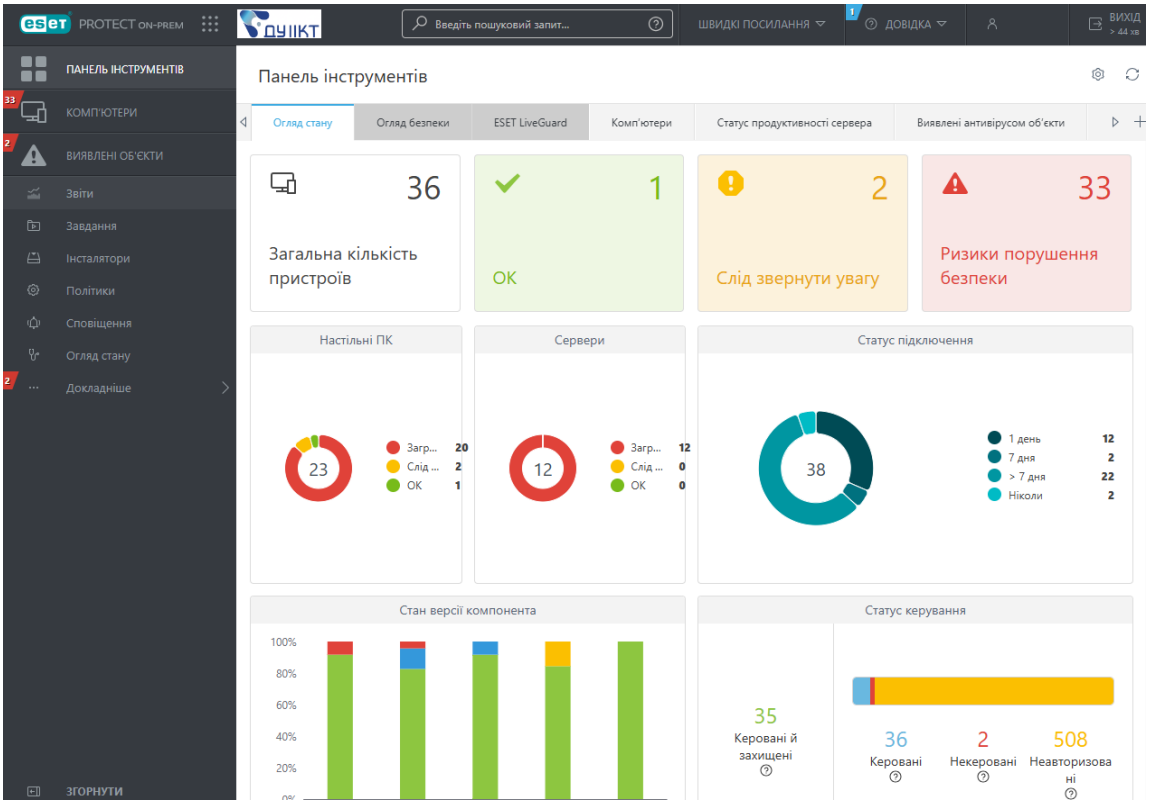

Рис. 3.17. Dashboard ESET Protect

На рис. 3.17 зображено головну панель інструментів (Dashboard) централізованої системи керування інформаційною безпекою ESET PROTECT On-Prem. Інтерфейс демонструє вкладку «Огляд стану», яка надає адміністратору зведену інформацію про поточний рівень захищеності мережевої інфраструктури, стан підключення клієнтських пристроїв та наявність активних загроз та порушень політик безпеки.

Серед кінцевих точок із 23 одиниць 20 мають критичні вразливості або активні загрози. «Статус підключення» показує високу доступність агентів: 38 клієнтів виходили на зв'язок протягом останнього тижня, що свідчить про справність каналів керування, незважаючи на проблеми з безпекою самих хостів.

«Статус керування» у нижній правій частині інтерфейсу. Система детектувала в мережевому периметрі 508 неавторизованих пристроїв (жовта

смуга), які не знаходяться під керуванням адміністратора (Rogue devices). Таке співвідношення керованих 36 до некерованих 508 хостів вказує на те, що значна частина інфраструктури (імовірно, особисті пристрої користувачів у мережі) залишається поза контуром централізованого захисту, що створює додаткові вектори для кібератак.

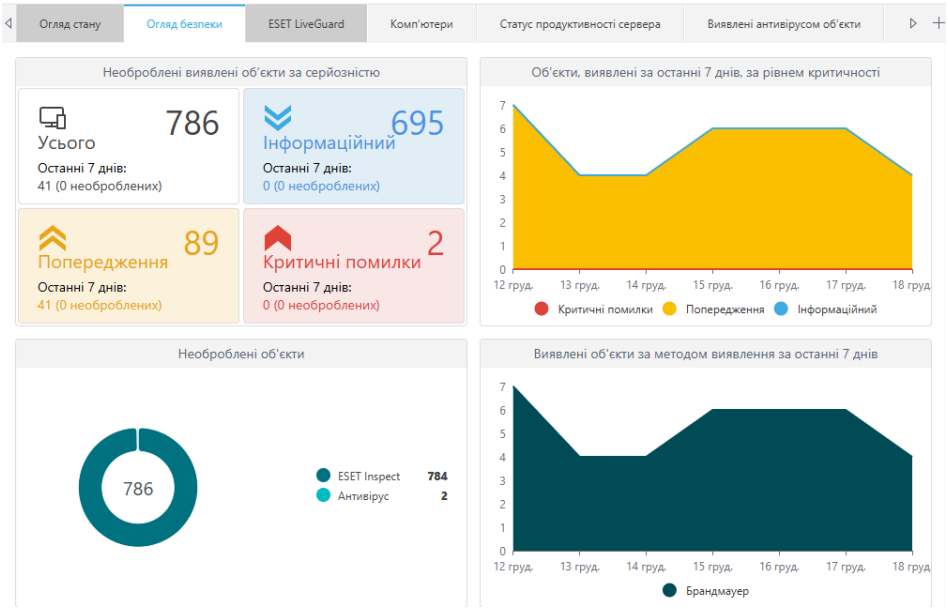

Рис. 3.18. Загальний огляд безпеки

«Огляд безпеки» (Security Overview) консолі ESET PROTECT, яка фокусується на кількісних та якісних показниках виявлених загроз. Дана панель надає деталізовану статистику щодо необроблених інцидентів, класифікуючи їх за рівнем серйозності, джерелом походження та динамікою появи в часі.

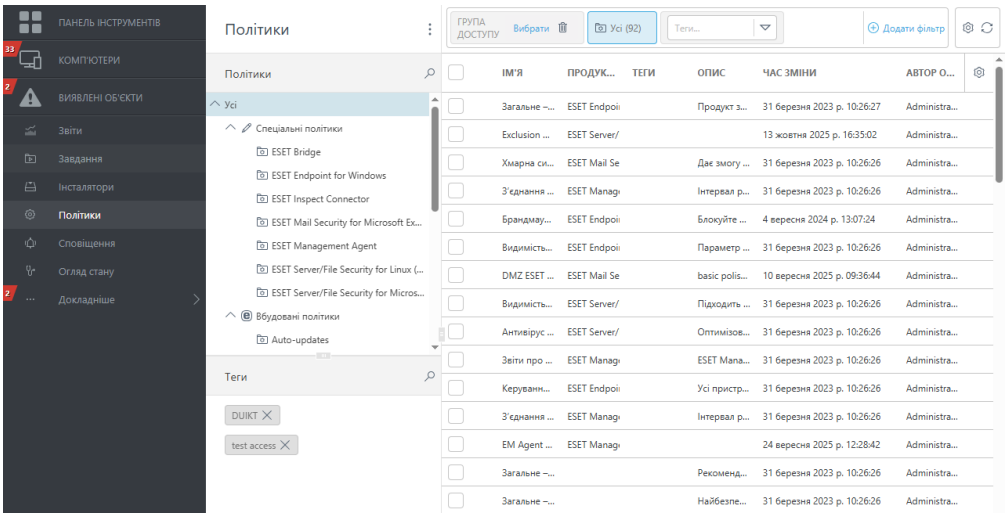

Рис. 3.19. Створені та запущені політики автоматизованого реагування

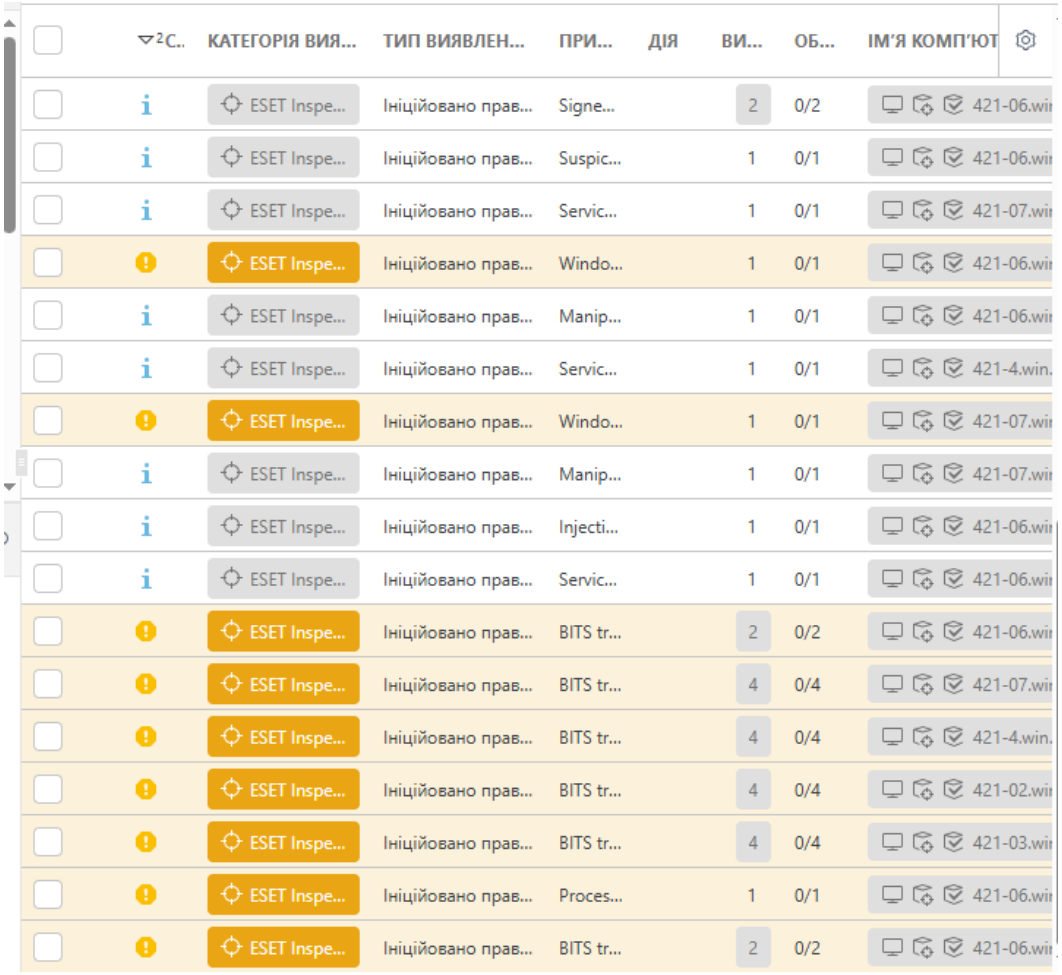

Рис. 3.20. Виявлені порушення безпеки

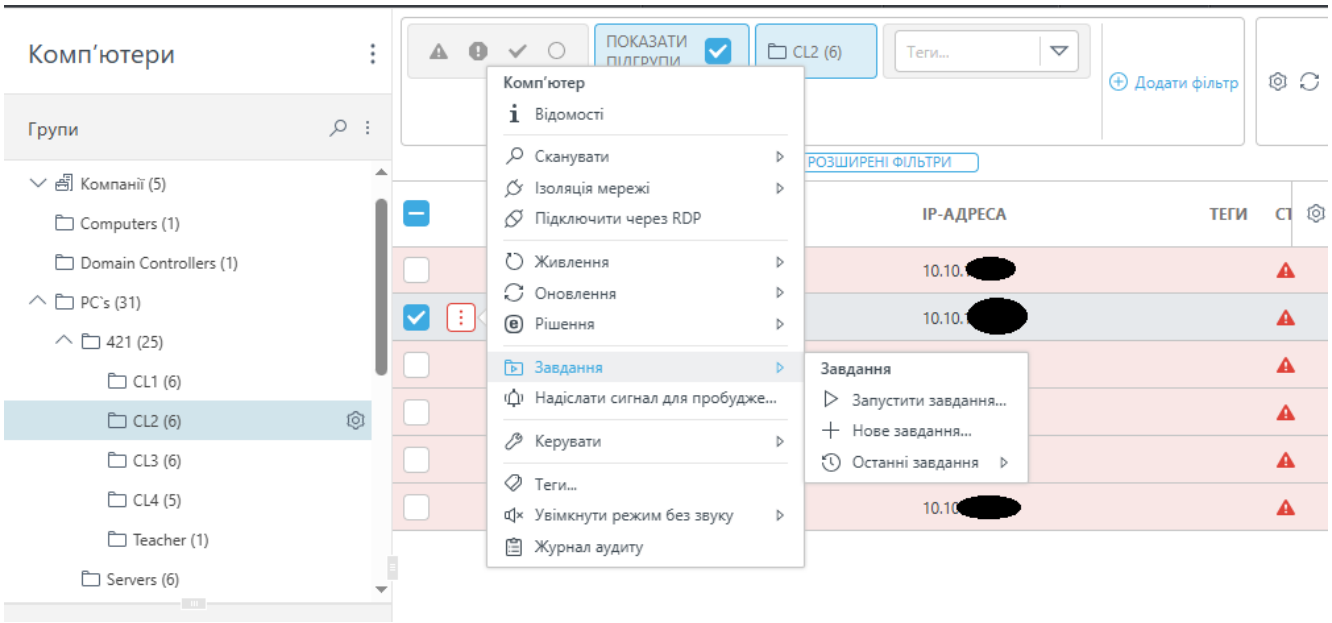

Рис. 3.21. Централізований віддалений запуск завдань на кінцеві точки

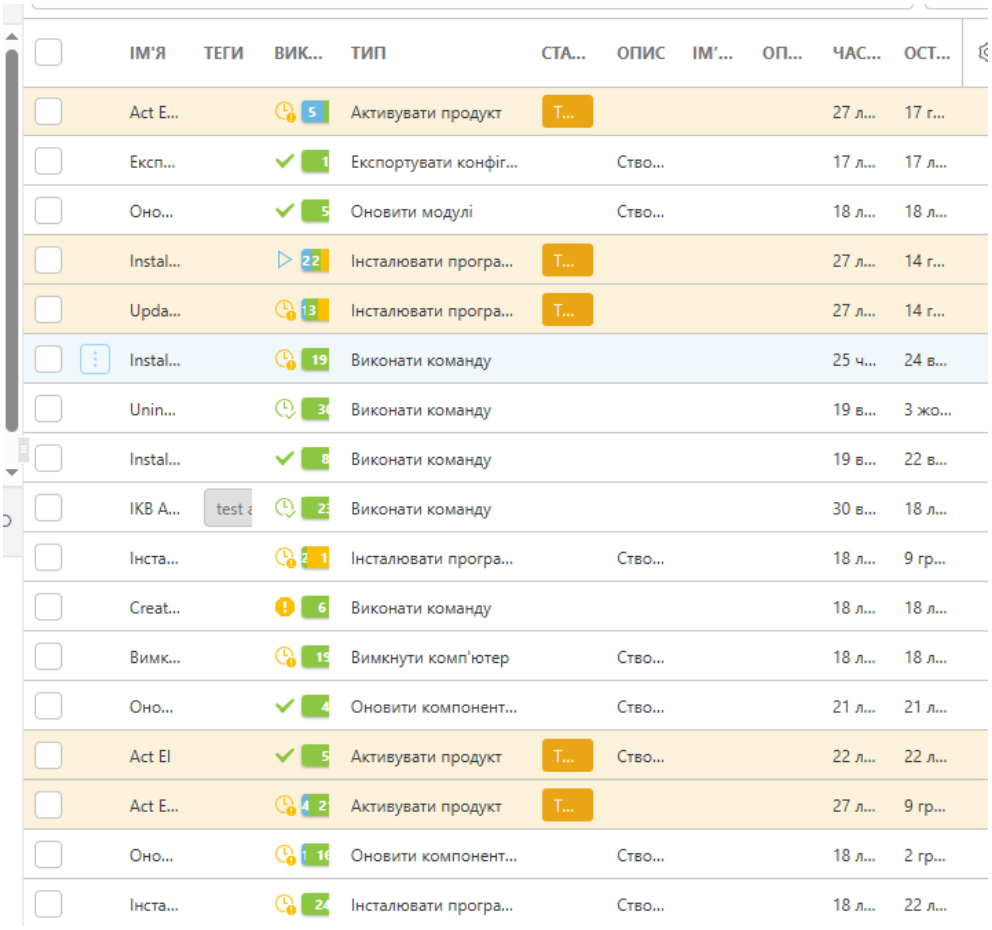

Рис. 3.22. Статус виконання запущених завдань

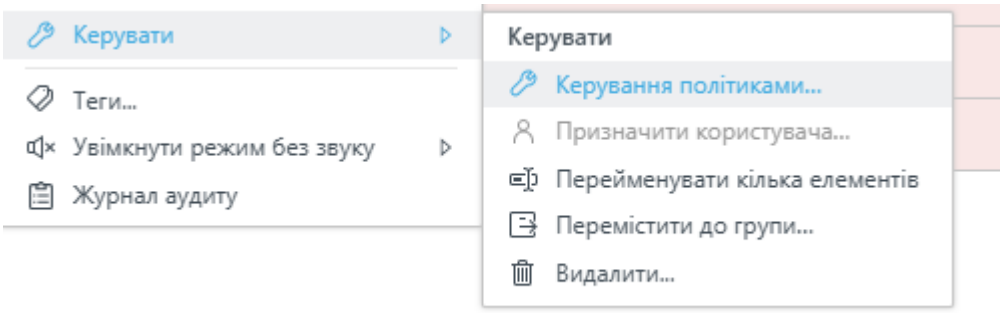

Рис. 3.23. Керування політиками для конкретної кінцевої точки

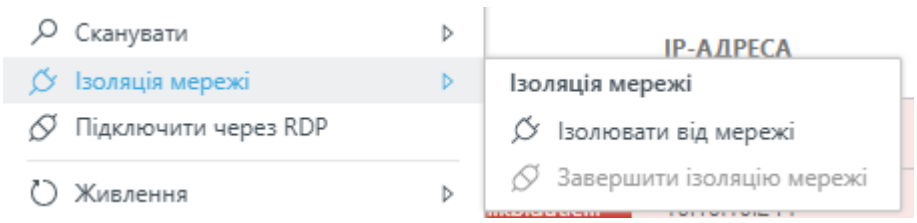

Рис. 3.24. Ізоляція небезпечних точок при порушенні правил

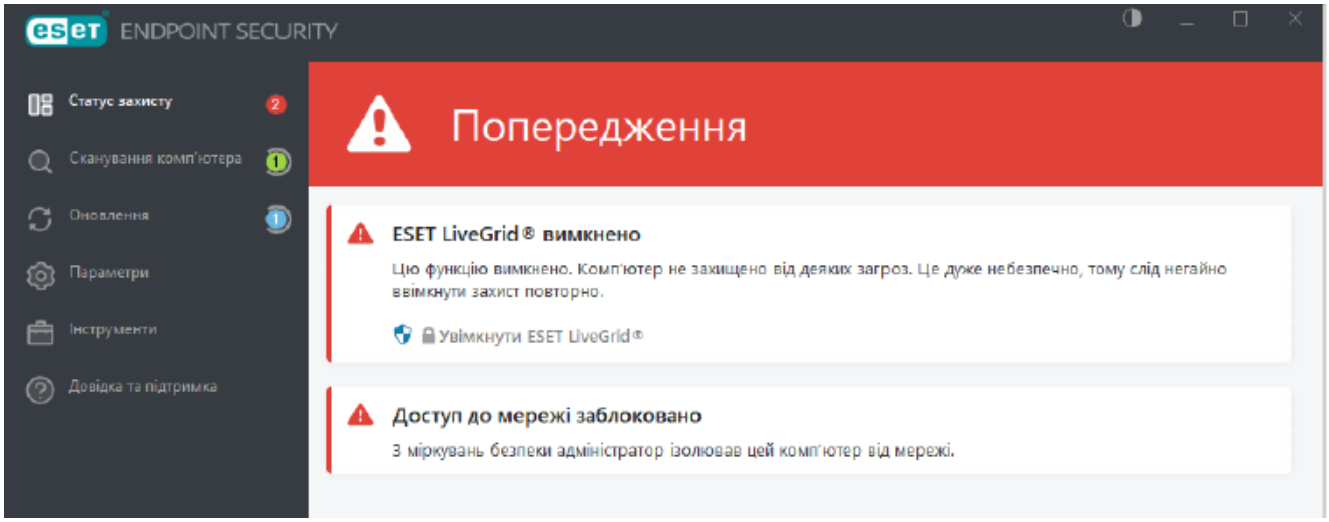

Рис. 3.25. Порушення критичної політики безпеки

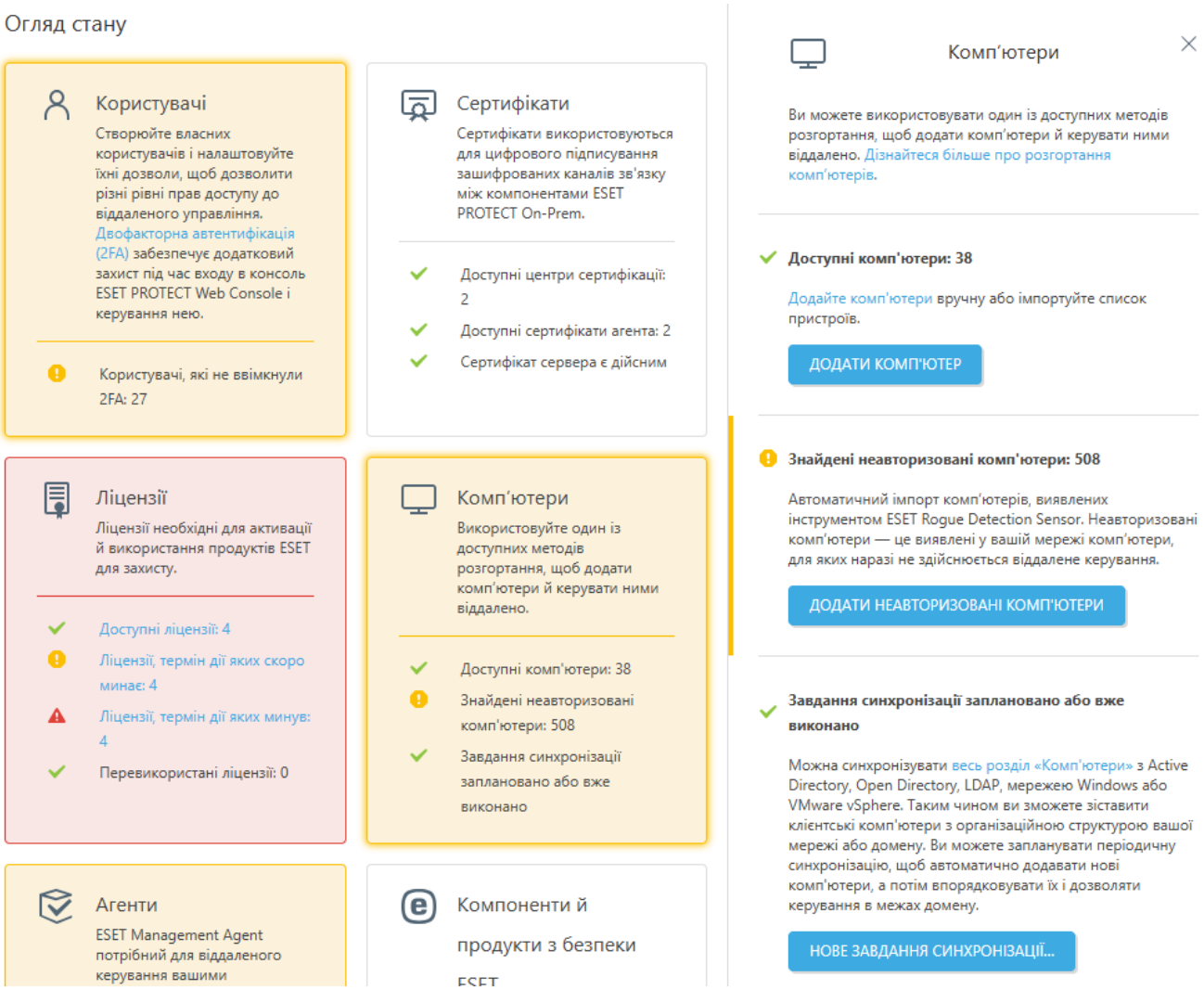

Рис. 3.26. Огляд безпеки

«Огляд безпеки» консолі ESET PROTECT, призначена для моніторингу динаміки кіберінцидентів. Панель візуалізує дані щодо необроблених загроз, порушень політик безпеки класифікуючи їх за рівнем критичності та методом виявлення. Загальна кількість необроблених об’єктів у системі становить 786 одиниць, з яких абсолютна більшість 695 має статус «Інформаційний», що вказує на події аудиту або моніторингу. Водночас, наявність 89 попереджень та 2 критичних помилок вимагає від адміністратора пріоритетного реагування для усунення потенційних вразливостей.

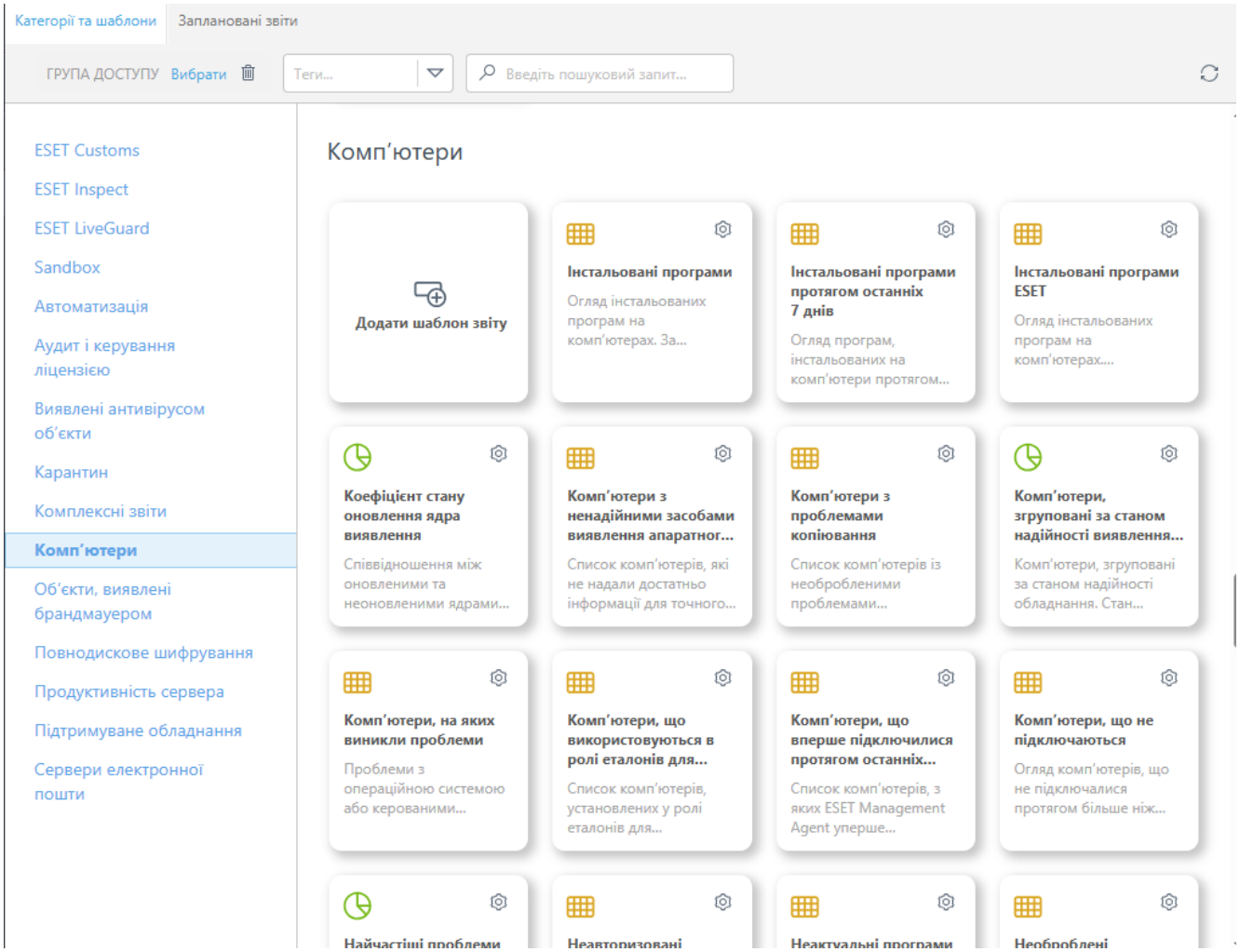

Рис. 3.27. Створення цільових звітностей

Система дозволяє налаштувати автоматичну розсилку звітів (наприклад, звіт "Комп'ютери, що не підключаються" може приходити на пошту адміністратора щоранку), що забезпечує проактивне реагування на збої в інфраструктурі.

3.3. Розроблення рекомендацій щодо використання автоматизованого управління політиками безпеки на базі ESET Protect

У ході виконання кваліфікаційної роботи було сформовано ряд рекомендацій щодо використання автоматичного управління політиками безпеки на базі ESET Protect, які розділені на певні частини починаючи від розгортання та закінчуючи моніторингом та безпекою.

I. Архітектура та розгортання

Забезпечити 100% покриття мережі агентами використовуючи компонент RD Sensor для автоматичного виявлення нових некерованих пристроїв у мережі та їх автоматичного підключення до консолі управління.

Обов’язково налаштувати двофакторну аутентифікацію (2FA) для облікових записів адміністраторів ESET Protect, щоб унеможливити перехоплення керування веб-консолі управління зловмисниками.

Сегментувати структуру груп створюючи ієрархію статичних груп, що відповідає організаційній структурі (за відділами або географічними філіями), для зручнішого делегування прав доступу локальним адміністраторам.

II. Управління політиками безпеки

У базовій політиці обов’язково встановити пароль на зміну налаштувань антивірусу на клієнтських місцях, щоб користувачі не могли самостійно вимкнути захист.

Використовувати принцип «Мінімальних прав» у політиках. Застосовувати жорсткі політики на рівні кореневої групи «Всі комп'ютери» для критичних параметрів (увімкнений захист у реальному часі), а гнучкі налаштування залишати для нижніх рівнів.

Створити окремі політики виключень для серверів баз даних або специфічного ПЗ, щоб антивірус не сповільнював їх роботу, і застосовувати їх лише до відповідних груп серверів.

Забезпечити увімкнення хмарної системи репутації ESET LiveGrid у політиках для всіх клієнтів, що значно пришвидшує виявлення нових загроз.

Реалізувати контроль пристроїв. Впровадити політику «Блокування за замовчуванням» для USB-накопичувачів, дозволяючи використання лише корпоративних носіїв за їх серійними номерами (White-listing).

III. Автоматизація та реагування.

Налаштувати динамічні групи, щоб автоматично застосовувати до них завдання оновлення або ізоляції.

Налаштувати автоматичне видалення старого ПЗ.

Автоматизувати Patch Management налаштуванням політики автоматичного сканування та встановлення критичних оновлень операційної системи Windows та популярних додатків у неробочий час.

Налаштувати автоматичне виконання завдання «Повне сканування» при спрацюванні тригера в журналі подій та автоматичну ізоляцію.

IV. Моніторинг та звітність

Налаштувати сповіщення. Регулярно генерувати звіти для керівництва.

Використовувати теги (Tagging) для швидкого пошуку та фільтрації у консолі під час порушень політик безпеки.

Моніторити статус ESET Management Agent, які не виходили на зв'язок більше 7 днів, для своєчасного виявлення проблем з мережею або кінцевою точкою.

V. Обслуговування та безпека системи

Впровадити тестову зону («Пісочницю») для оновлення версій агентів та продуктів, спочатку розгортати на тестовій групі комп'ютерів (5-10 машин), і лише після перевірки стабільності — на всю мережу.

Налаштувати автоматичне резервне копіювання бази даних ESET Protect та сертифікатів (CA), щоб мати можливість швидко відновити управління у випадку збою сервера.

Висновки до розділу 3

У третьому розділі кваліфікаційної роботи здійснено практичну реалізацію системи автоматизованого управління політиками безпеки на базі платформи ESET Protect та рекомендації щодо її застосування.

ВИСНОВКИ

На основі проведеного аналізу у розділі 1 обґрунтовано доцільність використання платформи ESET Protect як інструменту для автоматизації управління політиками безпеки. Впровадження цієї системи дозволить вирішити проблеми масштабованості, забезпечити централізований контроль над безліччю кінцевих точок та мінімізувати час реакції на інциденти. Це формує задачу для подальшого дослідження архітектури та функціональних можливостей ESET Protect у наступному розділі.

У другому розділі кваліфікаційної роботи проведено дослідження засобів автоматизованого управління інформаційною безпекою та детально проаналізовано архітектуру платформи ESET Protect її основні функції та можливості.

У третьому розділі кваліфікаційної роботи здійснено практичну реалізацію системи автоматизованого управління політиками безпеки на базі платформи ESET Protect та рекомендації щодо її застосування.

ПЕРЕЛІК ПОСИЛАНЬ

1. IBM Security. Cost of a Data Breach Report 2024. URL: https://www.ibm.com/reports/data-breach (дата звернення 10.10.2025).

2. Verizon. 2024 Data Breach Investigations Report (DBIR). URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення 10.10.2025).

3. Gartner. Top Trends in Cybersecurity 2024. URL: https://www.gartner.com/en/information-technology/insights/cybersecurity (дата звернення 12.10.2025).

4. ESET. ESET Threat Report H2 2025. URL: https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h22025.pdf (дата звернення 12.10.2025).

5. Держспецзв'язку. Аналітичні звіти про кіберагресію росії. URL: https://cip.gov.ua/ua/news/ (дата звернення 12.10.2025).

6. CERT-UA. Статистика кіберінцидентів. URL: https://cert.gov.ua/ (дата звернення 12.10.2025).

7. Cybersecurity Statistics 2025: Essential Trends & Attack Data. DeepStrike. URL: https://deepstrike.io/blog/cybersecurity-statistics-2025-threats-trends-challenges (дата звернення: 12.10.2025).

8. GDPR.eu. *Fines and Penalties*. General Data Protection Regulation Official Portal. URL: https://gdpr.eu/fines/ (дата звернення 12.10.2025).

9. Gartner. *The Cost of Downtime*. Gartner Research Reports. URL: https://www.gartner.com/ (дата звернення 13.10.2025).

10. Forrester. *The State of Data Security and Privacy*. Forrester Research. URL: https://www.forrester.com/ (дата звернення 13.10.2025).

11. Basan M., Norton K., Lafferty M. EDR vs EPP vs Antivirus: Comparing Endpoint Protection Solutions. eSecurityPlanet. URL: https://www.esecurityplanet.com/endpoint/antivirus-vs-epp-vs-edr/ (дата звернення: 13.10.2025).

12. What is EDR? Endpoint Detection & Response Defined | CrowdStrike. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ (дата звернення: 13.10.2025).

13. GeeksforGeeks. EDR vs EPP: What's the Difference? - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/computer-networks/edr-vs-epp-whats-the-difference/ (дата звернення: 13.10.2025).

14. Gartner Cyber Security Trends 2025: Key Insights. TechResearchs The future of marketing technology research. -. URL: https://techresearchs.com/cybersecurity/gartner-cyber-security-trends-2025-what-businesses-need-to-know/ (дата звернення: 14.10.2025).

15. Ponemon Institute. The State of Vulnerability Management in the Cloud and On-Premises. URL: http://cyberresources.solutions/blogs/The%20State%20of%20Vulnerability%20Management%20In%20the%20Cloud%20and%20On-Premises.pdf (дата звернення: 14.10.2025).

16. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

17. NIST. SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology.

18. OPSWAT. Centralized Security Management: Best Practices & Platform Must-Haves. OPSWAT. URL: https://www.opswat.com/blog/centralized-security-management (date of access: 16.10.2025).

19. Barman, S. Writing Information Security Policies. New Riders, 2021. 240 p.

20. NIST SP 800-128. Guide for Security-Focused Configuration Management of Information Systems. National Institute of Standards and Technology, 2011 (Updated 2020).

21. Stallings, W., Brown, L. Computer Security: Principles and Practice. Pearson, 4th Edition, 2018.

22. ESET. ESET Protect Policy Merging Logic. ESET Knowledgebase. URL: https://help.eset.com/

23. Gartner. Endpoint Protection Platforms: Agent vs. Agentless Architecture. Gartner Research, 2023.

24. Server | ESET PROTECT On-Prem 13.0. ESET Online Help. URL: https://help.eset.com/protect_install/13.0/en-US/arch_server.html?arch_server.html (дата звернення: 16.11.2025).

25. Web Console| ESET PROTECT On-Prem 13.0. ESET Online Help. URL: https://help.eset.com/protect_install/13.0/en-US/arch_server.html?arch_webconsole.html (дата звернення: 16.11.2025).

26. Agent | ESET PROTECT On-Prem 13.0. ESET Online Help. URL: https://help.eset.com/protect_install/13.0/en-US/arch_server.html?arch_agent.html (дата звернення: 20.11.2025).

27. RD Sensors | ESET PROTECT On-Prem 13.0. ESET Online Help. URL: https://help.eset.com/protect_install/13.0/en-US/arch_server.html?arch_rd_sensor.html (дата звернення: 20.11.2025).

28. HTTPS Proxy | ESET PROTECT On-Prem 13.0. ESET Online Help. URL: https://help.eset.com/protect_install/13.0/en-US/arch_server.html?arch_proxy.html (дата звернення: 20.11.2025).

29. ESET. ESET Protect Administrator Guide. ESET, Bratislava, 2024. URL: https://help.eset.com/protect_admin/

30. IDC. Worldwide Modern Endpoint Security Market Shares. IDC Research Report, 2023.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)