МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «СИСТЕМА МОНІТОРИНГУ ТА АНАЛІЗУ АНОМАЛЬНОЇ ПОВЕДІНКИ КОРИСТУВАЧІВ У КОРПОРАТИВНИХ МЕРЕЖАХ НА ОСНОВІ SYTECA UAM»

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Діана ГАВРИШЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Виконала: здобувачка вищої освіти гр. УБД-41

Діана ГАВРИШЕНКО
(Ім'я, ПРІЗВИЩЕ)

Керівник: Віталій МАРЧЕНКО
Ph.D.., *(Ім'я, ПРІЗВИЩЕ)*
доцент

Рецензент: Галина ГАЙДУР
д.т.н.., *(Ім'я, ПРІЗВИЩЕ)*
професор

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Гавришенко Діані Сергіївній
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Системи моніторингу та аналізу аномальної поведінки користувачів у корпоративних мережах на основі Syteca UAM”,
керівник кваліфікаційної роботи Марченко В.В., Ph.D., доцент,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “12” травня 2026р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека корпоративних мереж, системи моніторингу активності користувачів, технології UAM та UEBA, методи виявлення аномальної поведінки користувачів, наукова та технічна література, міжнародні стандарти інформаційної безпеки.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити сучасні методи моніторингу та аналізу активності користувачів у корпоративних мережах.
4.2. Проаналізувати архітектуру та функціональні можливості системи Syteca UAM.
4.3. Виконати розгортання та налаштування системи моніторингу аномальної поведінки користувачів на базі Syteca UAM, а також розробити практичні рекомендації щодо її використання.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	20.02.2026	
2.	Збір та аналіз літератури.	03.03.2026	
3.	Аналіз особливостей управління інформаційною безпекою підприємства	02.04.2026	
4.	Дослідження основних характеристик технологій формування обізнаності й навчання персоналу.	11.04.2026	
5.	Вивчення інструментів та методів формування обізнаності й навчання персоналу з інформаційної безпеки	19.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	28.04.2026	
7.	Оформлення роботи.	04.05.2026	
8.	Оформлення презентації.	18.05.2026	
9.	Отримання рецензії на роботу.	01.06.2026	
10.	Захист в ДЕК.	__.06.2026	

Здобувачка вищої освіти _____ Діана ГАВРИШЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувачка Гавришенко Д.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Система моніторингу та аналізу аномальної поведінки користувачів у корпоративних мережах на основі Syteca UAM"
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка ГАВРИШЕНКО Діана у кваліфікаційній роботі дослідила особливості систем моніторингу та аналізу аномальної поведінки користувачів у корпоративних мережах, проаналізувала сучасні підходи до забезпечення інформаційної безпеки, дослідила функціональні можливості платформи Syteca UAM, а також виконала розгортання та налаштування системи моніторингу активності користувачів. У роботі розглянуто механізми виявлення аномальної поведінки, управління привілейованим доступом та проведення розслідувань інцидентів кібербезпеки. За результатами дослідження розроблено практичні рекомендації щодо використання системи Syteca UAM для підвищення рівня інформаційної безпеки організацій.

ГАВРИШЕНКО Діана показала розуміння проблематики дослідження, володіння методами наукового аналізу та вміння застосовувати теоретичні знання на практиці. Під час виконання роботи проявила себе як відповідальний, організований та самостійний виконавець.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки ГАВРИШЕНКО Діана на оцінку «**відмінно**» та присвоїти їй кваліфікацію бакалавра за спеціальністю «Кібербезпека» за освітньою програмою «Управління інформаційною та кібернетичною безпекою».

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"_____" ____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Гавришенко Д.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти ГАВРИШЕНКО Діана
на тему “ Система моніторингу та аналізу аномальної поведінки користувачів у корпоративних мережах на основі Syteca UAM ”

Актуальність. У час зростання кількості кіберзагроз забезпечення інформаційної безпеки корпоративних мереж є важливим завданням. Особливо актуальними є питання контролю дій користувачів, виявлення аномальної поведінки та оперативного реагування на інциденти кібербезпеки. Тому дослідження можливостей платформи Syteca UAM є актуальним і практично значущим..

Позитивні сторони.

1. У роботі ґрунтовно досліджено особливості систем моніторингу активності користувачів та аналізу аномальної поведінки в корпоративних мережах.
2. Кваліфікаційна робота оформлена відповідно до встановлених вимог. Матеріал викладено послідовно та логічно, наведено достатню кількість рисунків і практичних прикладів.
3. Авторкою проведено аналіз сучасних рішень у сфері моніторингу активності користувачів, досліджено архітектуру та функціональні можливості платформи Syteca UAM.
4. Практична частина роботи містить розгортання та налаштування системи Syteca UAM, а також дослідження механізмів виявлення аномалій і проведення розслідувань інцидентів кібербезпеки.
5. За результатами дослідження розроблено рекомендації щодо впровадження та використання системи Syteca UAM для підвищення рівня інформаційної безпеки організацій.

Недоліки.

Доцільно було б більш детально розглянути питання інтеграції Syteca UAM із SIEM-системами та застосування алгоритмів машинного навчання для виявлення аномальної поведінки користувачів.

Однак зазначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “**відмінно**”, а здобувачка ГАВРИШЕНКО Діана заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Галина ГАЙДУР
д.т.н., професор *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню систем моніторингу та аналізу аномальної поведінки користувачів у корпоративних мережах на основі Syteca UAM. Робота складається зі вступу, трьох розділів, що містять 41 рисунок, висновків і списку використаних джерел із 20 найменувань. Загальний обсяг роботи становить 58 аркушів, з яких 2 аркуші займають перелік умовних скорочень і список використаних джерел.

Метою роботи є дослідження особливостей застосування систем моніторингу активності користувачів у корпоративних мережах.

Об'єкт дослідження — процес забезпечення інформаційної безпеки корпоративних мереж.

Предмет дослідження — методи та засоби моніторингу активності користувачів та виявлення аномальної поведінки на основі Syteca UAM.

Методи дослідження*:* аналіз, синтез, порівняння, класифікація та системний аналіз. У роботі проаналізовано принципи забезпечення інформаційної безпеки корпоративних мереж, досліджено підходи до моніторингу користувачів та принципи роботи UAM-систем. Розглянуто архітектуру та функціональні можливості платформи Syteca UAM, механізми виявлення аномальної поведінки, управління привілейованим доступом та проведення розслідування інцидентів кібербезпеки.

Галузь застосування — впровадження систем моніторингу активності користувачів у корпоративних мережах для підвищення рівня інформаційної безпеки, контролю привілейованих облікових записів та виявлення кіберінцидентів.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, КОРПОРАТИВНІ МЕРЕЖІ, UAM, UBA, UEBA, PAM, SYTECA, МОНІТОРИНГ АКТИВНОСТІ КОРИСТУВАЧІВ, АНАЛІЗ АНОМАЛЬНОЇ ПОВЕДІНКИ, КІБЕРБЕЗПЕКА.

ABSTRACT

The qualification work is devoted to the study of user activity monitoring and anomalous behavior analysis systems in corporate networks based on Syteca UAM. The work consists of an introduction, three chapters containing 41 figures, conclusions, and a list of references including 20 sources. The total volume of the work is 58 pages, of which 2 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study the features of using user activity monitoring systems in corporate networks.

The object of the study is the process of ensuring information security in corporate networks.

The subject of the study is methods and tools for monitoring user activity and detecting anomalous behavior based on Syteca UAM.

Research methods include analysis, synthesis, comparison, classification, and systems analysis. The study examines the principles of ensuring information security in corporate networks, investigates approaches to user monitoring, and explores the principles of UAM systems. The architecture and functional capabilities of the Syteca UAM platform are considered, along with mechanisms for detecting anomalous behavior, privileged access management, and conducting cybersecurity incident investigations.

Field of application is the implementation of user activity monitoring systems in corporate networks to enhance information security, control privileged accounts, and detect cyber incidents.

Keywords: INFORMATION SECURITY, CORPORATE NETWORKS, UAM, UBA, UEBA, PAM, SYTECA, USER ACTIVITY MONITORING, ANOMALY BEHAVIOR ANALYSIS, CYBERSECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

UAM	User Activity Monitoring
UBA	User Behavior Analytics
UEBA	User and Entity Behavior Analytics
PAM	Privileged Access Management (
SIEM	Security Information and Event Management (
MFA	Multi-Factor Authentication
ОС	Операційна система
DLP	Data Leak Prevention
IIS	Internet Information Services
GDPR	General Data Protection Regulation
ISO	International Organization for Standardization
SOC	Security Operation Center
PCI DSS	Payment Card Industry Data Security Standard

ВСТУП

Актуальність теми. Стрімкий розвиткок інформаційних технологій та цифровізація діяльності підприємств, піднімає питання забезпечення інформаційної безпеки. Корпоративні мережі постійно піддаються різноманітним кіберзагрозам, серед яких несанкціонований доступ до інформації, витік конфіденційних даних, використання шкідливого програмного забезпечення та внутрішні загрози, пов'язані з діями користувачів. Значна частина інцидентів інформаційної безпеки виникає саме внаслідок помилкових або навмисних дій працівників організації.

Зважаючи на це важливого значення набуває використання систем моніторингу активності користувачів та аналізу аномальної поведінки, які дозволяють своєчасно виявляти підозрілі дії, контролювати доступ до інформаційних ресурсів та підвищувати рівень захисту корпоративної інформаційної інфраструктури. Одним із сучасних рішень у цій сфері є Syteca, що поєднує функції моніторингу дій користувачів, контролю привілейованого доступу, запису сесій та аналізу подій безпеки.

Використання систем класу UAM (User Activity Monitoring) та UEBA (User and Entity Behavior Analytics) дозволяє організаціям оперативно реагувати на потенційні загрози, здійснювати розслідування інцидентів кібербезпеки та мінімізувати ризики витоку інформації. Крім того, впровадження таких систем сприяє підвищенню рівня контролю за діяльністю користувачів і забезпечує дотримання політик інформаційної безпеки підприємства.

З огляду на зазначене дослідження систем моніторингу та аналізу аномальної поведінки користувачів у корпоративних мережах на основі Syteca UAM є актуальним науковим і практичним завданням.

Мета роботи полягає у дослідженні особливостей використання системи моніторингу та аналізу аномальної поведінки користувачів у корпоративних мережах на основі Syteca UAM.

Об'єкт дослідження – процес забезпечення інформаційної безпеки

корпоративних мереж.

Предмет дослідження – методи та засоби моніторингу активності користувачів та аналізу аномальної поведінки на основі Syteca UAM.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати особливості забезпечення інформаційної безпеки корпоративних мереж.
2. Дослідити принципи роботи систем моніторингу активності користувачів та аналізу аномальної поведінки.
3. Розглянути функціональні можливості системи Syteca UAM.
4. Виконати розгортання та налаштування системи моніторингу на базі Syteca.
5. Розробити рекомендації щодо застосування системи моніторингу та аналізу аномальної поведінки користувачів у корпоративних мережах.

Методи дослідження. Для вирішення поставлених завдань у роботі використано методи аналізу та синтезу порівняння, класифікації, системного аналізу, а також методи дослідження систем інформаційної безпеки та моніторингу активності корстувачів.

Практичне значення одержаних результатів. Поялгає у можливості використання системи Syteca UAM для підвищення рівня інформаційнох безпеки корпоративних мреж, своєчасного виявлення аномальної поведінки користувачів, контролю дійпривілейованих користувачів та покращення процесу розслідування інцидентів кібербезпеки.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

Розділ 1. ТЕОРЕТИЧНІ ОСНОВИ МОНІТОРИНГУ ПОВЕДІНКИ КОРИСТУВАЧІВ У КОРПОРАТИВНИХ МЕРЕЖАХ

1.1 Аналіз ризиків аномальної поведінки користувачів

Виклики для виявлення та аналізу аномальної поведінки користувачів у бізнес-мережах стають більш актуальними через недавню цифровізацію бізнес-операцій та появу різноманітних кіберзагроз. Традиційні рішення, такі як тестування інформаційної безпеки на основі сигнатур, не дозволяють адекватно захиститися від сучасних атак, включаючи внутрішні загрози та атаки з компрометованими обліковими записами. У цьому контексті зростає популярність поведінкових технік, зокрема аналітики поведінки користувачів та об'єктів (UEBA), де спостерігаються дії користувачів та системних об'єктів для виявлення відхилень від їх очікуваної поведінки [1].

Аномальна активність користувачів описує поведінку, яка не спостерігалася в їх звичайному профілі поведінки. Це може проявлятися у вигляді входу в систему в незвичний час, доступу до елементів, які раніше не використовувалися, зміни геолокації доступу, використання нових пристроїв або значного збільшення обсягів передачі даних [2]. Виявлення цих відхилень є важливим інструментом для раннього попередження про події інформаційної безпеки.

Проведення аналізу ризиків аномальних дій дозволяє виявити різноманітні важливі загрози. В основі цих загроз лежать внутрішні загрози, які здійснюються або не здійснюються співробітниками організації. Ці загрози можуть бути шкідливими, і користувачі вже мають легітимний доступ до інформаційних ресурсів. Другою критичною проблемою є порушення облікових записів, яке може виникнути внаслідок фішингових атак, вгадування паролів та витоку облікових даних. Тут зловмисник діє з боку легітимного користувача, що ускладнює виявлення його атаки класичними методами [3].

Ще одним значним ризиком є латеральний рух зловмисника після початкового проникнення у велику корпоративну мережу. Ця активність супроводжується спробами проникнути в нові системи та ресурси, які знаходяться поза межами звичайної активності користувача. Крім того, ескалація привілеїв, яка фактично є несанкціонованим доступом до розширеного доступу до системи, представляє велику загрозу. Виявлення цих дій є критично важливим для зупинки прогресу атаки [4].

Аналіз загрози аномальної поведінки користувачів може проходити кілька етапів. На початковому етапі дані агрегуються з таких джерел, як журнали подій ОС, мережевий трафік, системи аутентифікації та програмне забезпечення. Спочатку (і найголовніше) ми встановлюємо базовий профіль фактичної поведінки з історії користувачів на основі їхньої поведінки. На цьому етапі відхилення виявляються шляхом порівняння того, що робиться зараз, з базовим профілем [1].

Це супроводжується механізмом оцінки ризику для кожної події або групи подій (Risk Scoring). Отримане значення може бути використане системою для запуску відповідної реакції, від запобігання доступу до запиту іншого ідентифікатора до інформування служби інформаційної безпеки. Використання алгоритмів машинного навчання робить виявлення аномалій більш точним і дозволяє досягти меншої кількості хибнопозитивних результатів [3].

Ефективність аналізу аномальної поведінки користувачів дозволить виявити загрози, які не були виявлені попередніми методами, включаючи атаки нульового дня, та запобігти внутрішнім загрозам. З іншого боку, на практиці основними недоліками є залежність від якісних вхідних даних, складність у налаштуванні моделей поведінки та ризики хибнопозитивних результатів [2].

Отже, аналіз ризиків аномальної поведінки користувачів є важливим аспектом системи інформаційної безпеки корпоративних мереж, що покращить своєчасне виявлення потенційних загроз та максимальний захист інформаційних ресурсів організації.

1.2 Технології User Activity Monitoring (UAM) та User Behavior Analytics (UBA)

У сучасних корпоративних інформаційних системах важливу роль відіграють технології моніторингу та аналізу поведінки користувачів. До найбільш поширених належать User Activity Monitoring (UAM) та User Behavior Analytics (UBA) [5]. Незважаючи на певну схожість, ці технології мають різне призначення та сфери застосування.

Технологія **User Activity Monitoring (UAM)** призначена для контролю дій користувачів у межах інформаційної системи. Вона забезпечує фіксацію та аналіз активності користувачів, зокрема відвіданих вебсайтів, використаних програм, доступу до файлів, часу входу та виходу із системи. Також можуть здійснюватися запис екрана, створення скріншотів і ведення журналів подій. Основною метою UAM є забезпечення інформаційної безпеки, контроль дотримання політик доступу та виявлення інсайдерських загроз .

Застосування UAM особливо актуальне в організаціях, які працюють із конфіденційною інформацією або мають віддалених співробітників. Такі системи дозволяють своєчасно виявляти підозрілу активність, наприклад несанкціонований доступ до файлів або спроби копіювання даних, а також підвищують рівень контролю за роботою персоналу .

На відміну від UAM, технологія **User Behavior Analytics (UBA)** орієнтована не лише на фіксацію дій користувачів, а й на їх глибокий аналіз. UBA-системи збирають великі обсяги даних про взаємодію користувачів із системами та застосовують аналітичні методи і машинне навчання для виявлення закономірностей поведінки. Основна мета полягає у розумінні поведінки користувача, визначенні її причин та прогнозуванні подальших дій .

UBA дозволяє створювати поведінкові профілі користувачів і визначати відхилення від нормальної активності. Наприклад, система може виявити нетипові дії, такі як доступ до ресурсів у незвичний час або використання нетипових сервісів. Завдяки цьому забезпечується більш точне виявлення

потенційних загроз, зокрема компрометації облікових записів або інсайдерських атак .

Основна відмінність між UAM і UBA (рис.1.2) полягає у їхньому призначенні. UAM зосереджується на контролі та фіксації дій користувачів, тоді як UBA аналізує поведінку та виявляє приховані закономірності. Іншими словами, UAM відповідає на питання «що робить користувач», а UBA — «чому він це робить і чи є це нормальною поведінкою».

Рис. 1.2 Де люди плутаються між UBA та UAM [5]

Крім того, ці технології використовуються різними підрозділами організації. UAM зазвичай застосовується службами інформаційної безпеки, IT-відділами та керівництвом для контролю діяльності працівників і забезпечення відповідності нормативним вимогам. UBA, у свою чергу, може використовуватися як у сфері безпеки, так і для аналізу взаємодії користувачів із програмними продуктами з метою покращення їх функціональності .

Таким чином, технології UAM і UBA не є взаємозамінними, а скоріше доповнюють одна одну. Їх спільне використання дозволяє отримати повну

картину поведінки користувачів: від фіксації конкретних дій до глибокого аналізу та прогнозування. Це значно підвищує ефективність систем інформаційної безпеки та сприяє своєчасному виявленню потенційних загроз.

1.3 Порівняльний аналіз існуючих рішень для моніторингу активності

У сучасних умовах розвитку інформаційних технологій системи моніторингу діяльності користувачів стали важливим інструментом забезпечення інформаційної безпеки організацій. Такі системи дозволяють відстежувати, аналізувати та контролювати дії користувачів у корпоративних мережах, що дає змогу своєчасно виявляти загрози, зокрема інсайдерські атаки та несанкціонований доступ до даних.

Сучасні системи моніторингу можна умовно поділити на кілька категорій: класичні UAM-рішення (User Activity Monitoring), системи з інтегрованою аналітикою поведінки (UBA/UEBA), а також комплексні платформи, які поєднують функції моніторингу з SIEM-рішеннями.

До найбільш відомих систем класу UAM належать такі рішення, як Teramind, ActivTrak, Syteca, Hubstaff, Time Doctor та інші. Вони забезпечують збір детальної інформації про дії користувачів, включаючи використання програм, доступ до файлів, активність у мережі, а також можуть здійснювати запис екрана та ведення журналів подій. Основною їх перевагою є високий рівень деталізації даних і можливість проведення розслідувань інцидентів безпеки [6].

Наприклад, система Teramind надає широкі можливості для моніторингу та аналізу дій користувачів, включаючи запис сесій, контроль передачі даних і виявлення аномальної поведінки. Вона також підтримує функції запобігання витоку даних (DLP), що є важливим для організацій, які працюють із конфіденційною інформацією [7]. У свою чергу, Hubstaff більше орієнтований на контроль продуктивності працівників і використовується переважно для управління віддаленими командами [6].

Окрему групу становлять більш складні системи, такі як Splunk [8] або Micro Focus, які інтегрують функції моніторингу з аналітикою та управлінням подіями безпеки. Такі платформи здатні обробляти великі обсяги даних у реальному часі, виявляти аномалії та забезпечувати централізований контроль над інформаційною інфраструктурою підприємства. Зокрема, Splunk використовується як універсальна платформа для аналізу подій безпеки та моніторингу активності користувачів у складних корпоративних середовищах .

Важливою тенденцією розвитку сучасних систем моніторингу є інтеграція технологій поведінкової аналітики (UBA/UEBA) [9]. Такі системи не лише фіксують дії користувачів, але й аналізують їх з метою виявлення нетипових моделей поведінки. Це дозволяє підвищити точність виявлення загроз та зменшити кількість хибних спрацювань. Наприклад, сучасні рішення можуть визначати аномалії на основі змін у поведінці користувача, таких як нетиповий час входу або доступ до незвичних ресурсів .

Порівнюючи сучасні системи моніторингу, можна виділити їх основні відмінності:

Функціональність: UAM-системи забезпечують детальний контроль дій користувачів, тоді як UBA/UEBA-системи орієнтовані на аналіз поведінки та прогнозування загроз.

Рівень аналітики: прості системи надають лише журнали подій, тоді як сучасні платформи використовують штучний інтелект і машинне навчання для аналізу даних.

Сфера застосування: одні рішення орієнтовані на безпеку, інші — на підвищення продуктивності персоналу.

Масштабованість: корпоративні платформи (наприклад, Splunk) здатні працювати з великими обсягами даних і підтримувати складні IT-інфраструктури, тоді як прості інструменти більше підходять для малого та середнього бізнесу.

Таким чином, сучасні системи моніторингу користувачів суттєво відрізняються за своїми можливостями, призначенням і рівнем складності. Вибір

конкретного рішення залежить від потреб організації, рівня необхідної безпеки та масштабу інформаційної інфраструктури. Найбільш ефективним підходом є використання комплексних систем, які поєднують функції моніторингу та аналітики, що дозволяє забезпечити більш високий рівень захисту інформації.

Висновки до розділу 1

Останні дослідження виявили, що моніторинг і аналіз поведінки користувачів є однією з основних характеристик сучасних систем інформаційної безпеки корпоративних мереж. Зокрема, підрозділ 1.1 підтверджує, що використання поведінкового підходу до виявлення активності користувачів (User and Entity Behavior Analytics) ефективно дозволяє виявляти аномальні дії користувачів, такі як внутрішні загрози, компрометація облікових записів, латеральний рух і ескалація привілеїв. Етапи такого аналізу відомі як збір/отримання даних, профіль базової поведінки, виявлення відхилень і оцінка ризиків. Ми починаємо з встановлення особливостей і відмінностей між технологіями моніторингу активності користувачів (UAM) і аналітики поведінки користувачів (UBA) у підрозділі 1.2. Було показано, що UAM стосується захоплення і моніторингу практик користувачів, тоді як UBA передбачає глибокий аналіз поведінки з використанням аналітичних методів і методів машинного навчання: останнє допомагає надавати поведінкові інсайти. Було задокументовано, що їх повне використання сприяє більш комплексному аналізу активності користувачів і покращує ефективність виявлення загроз. Для порівняльного аналізу сучасних методів моніторингу активності користувачів проводиться розділ 1.3. Встановлено, що сучасні системи мають різні аспекти корисності, продуктивності аналітики, масштабованості та застосувань. Насправді, класичні рішення UAM призначені для детального моніторингу дій користувачів; такі як Splunk (де моніторинг поєднується з аналітикою/управлінням подіями безпеки). Також повідомляється про використання технологій поведінкового аналізу (UBA/UEBA), оскільки існує

сильна тенденція в цьому напрямку, що дозволяє покращити точність виявлення аномалій і зменшити кількість хибнопозитивних результатів. Тому результати в розділі свідчать про необхідність надання комплексних рішень на основі поєднання відстеження дій і аналітики поведінки. Це забезпечує інформаційні ресурси організації для кращого захисту на найвищому рівні і стає передумовами для впровадження виявлення та реагування на інциденти кібербезпеки, а також UAM в ефективній структурі, зосереджуючись на спеціалізованих платформах UAM, таких як Syteca, як зазначено в решті цього розділу.

Розділ 2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ МОНІТОРИНГУ АКТИВНОСТІ НА БАЗІ РІШЕННЯ SYTECA UAM

2.1 Архітектура та функціональні можливості платформи Syteca UAM

Платформа Syteca — це рішення для кібербезпеки, яке успадковує всі функціональні можливості системи Ekran, одночасно розширюючи можливості керування привілейованим доступом (PAM) і моніторингу активності користувачів (UAM) у більш орієнтований на клієнта спосіб [10]. Із Syteca ми отримуємо інструменти кібербезпеки, необхідні для ефективного управління людськими ризиками (рис.2.1):

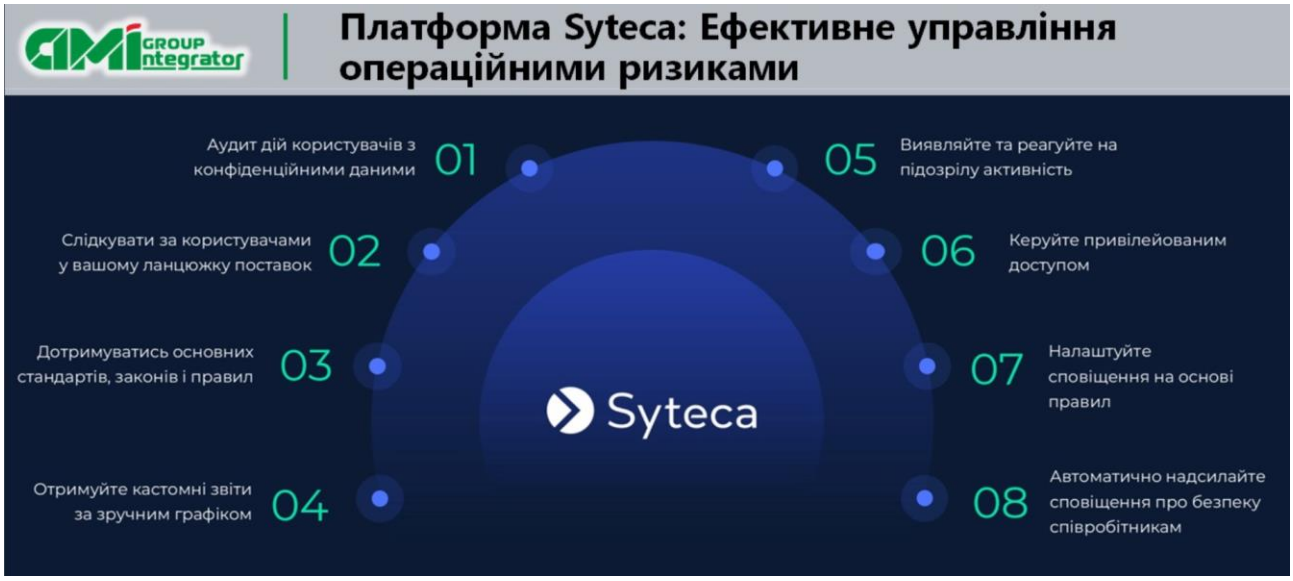

Рис. 2.1 Ефективне управління операційними ризиками [10]

Компанія змінила підхід до ліцензування. Нова платформа Syteca дозволяє використовувати лише ті функції, які відповідають поточним потребам у сфері кібербезпеки. Якщо бути зацікавленим виключно в керуванні доступом до системи, даних і кінцевих точок, ми можемо купити тільки функціонал керування привілейованим доступом (PAM). Те саме стосується, і функціоналу моніторингу активності користувачів (UAM) (рис. 2.2).

Рис. 2.2 Можливості платформи Syteca [10]

З оновленням були розширені і можливості PAM з додаванням нових функцій, а саме:

- **Виявлення облікових записів** дозволяє ідентифікувати існуючі привілейовані облікові записи у вашій IT-інфраструктурі — навіть ті, про які ви не знали.
- **Реєстрація облікових записів** дає змогу перенести ідентифіковані облікові записи в Syteca та забезпечити ефективне керування паролями.

Наразі Syteca може виявляти та підключати локальні облікові записи Active Directory та Windows. Ви можете налаштувати виявлення та адаптацію облікових записів відповідно до своїх потреб і запланувати автоматичне виявлення та адаптацію нових облікових записів у міру їх створення.

2.2 Методи виявлення аномалій та налаштування сповіщень у реальному часі

У сфері кібербезпеки важливо не просто збирати інформацію про дії користувачів, а й вчасно виявляти підозрілу або нетипову поведінку. Саме тому в системах класу UAM та UEBA, зокрема в рішеннях типу Syteca, застосовуються різні методи виявлення аномалій та механізми сповіщення у режимі реального часу.

Одним із основних підходів є використання концепції User and Entity Behavior Analytics. Її суть полягає в тому, що система спочатку "вивчає" нормальну поведінку користувача (наприклад, коли він заходить у систему, які ресурси використовує, з яких пристроїв працює), а потім порівнює з нею поточні дії. Якщо щось сильно відрізняється — це може бути ознакою загрози [3].

У практиці використовуються такі основні методи:

- **Поведінковий аналіз.** Система аналізує звичну активність користувача і визначає відхилення. Наприклад, якщо працівник завжди працює вдень, а раптом заходить уночі з іншої країни — це вже підозріло [3].
- **Правилозорієнтований підхід (rules).** Знадаються конкретні правила, наприклад: багато невдалих спроб входу; доступ до заборонених ресурсів; різке копіювання великої кількості даних. Якщо правило спрацьовує — система фіксує інцидент [11].
- **Статистичні методи.** Система аналізує середні значення та відхилення. Наприклад, якщо користувач зазвичай передає 50 МБ даних, а раптом 5 ГБ — це аномалія [12].
- **Методи машинного навчання.** Більш складний підхід, коли система сама знаходить закономірності в поведінці користувачів і з часом "вчиться" краще розпізнавати загрози. Це допомагає зменшити кількість помилкових спрацювань [13].

- **Оцінка ризику (Risk Scoring).** Кожній події присвоюється певний рівень ризику. Наприклад:

- низький — звичайна дія;

- середній — підозріла;

- високий — потенційна атака.

Це допомагає зрозуміти, на що потрібно реагувати в першу чергу [14].

Після виявлення аномалії дуже важливо швидко відреагувати. Для цього використовуються сповіщення (alerts), які генеруються системою автоматично. Основними принципами роботи зі сповіщеннями є:

- **Сповіщення в реальному часі.** Як тільки система бачить підозрілу дію — вона одразу повідомляє про це адміністратора або службу безпеки [13].

- **Кореляція подій.** Іноді одна дія нічого не означає, але кілька разом — це вже атака. Наприклад: невдалий вхід → вдалий вхід → доступ до нових ресурсів. Система об’єднує такі події та формує повнішу картину [11].

- **Пріоритезація інцидентів.** Завдяки risk scoring система показує, які сповіщення найважливіші, щоб не витрачати час на дрібниці [14].

- **Зменшення помилкових спрацювань.** За рахунок поведінкового аналізу система краще розуміє, що є нормою, а що — ні, і не “тривожить” без причини [13].

- **Автоматична реакція.** У деяких випадках система може виконувати автоматичні дії у відповідь на інцидент, зокрема блокувати користувачів, завершувати сесії або обмужувати доступ [15].

Використання різних методів виявлення аномалій дозволяє комплексно аналізувати поведінку користувачів організації і знаходити нові складні загрози в реальному часі, що дозволить оперативніше реагувати на них та запобігати розвитку інцидентів на ранніх етапах. А механізми сповіщення у реальному часі забезпечує швидке інформування відповідальних осіб про підозрілу активність, що значно зменшує можливі наслідки атак у кіберпросторі та мінімізує потенційні збитки. Поєднання таких підходів сприяє підвищенню рівня

контролю над інформаційними ресурсами, покращує ефективність роботи служб інформаційної безпеки та забезпечує більш високий рівень захищеності корпоративної інфраструктури. Таким чином, інтеграція методів аналізу аномалій і систем оперативного сповіщення є важливим та необхідним елементом сучасних систем інформаційної безпеки.

2.3 Механізм управління доступом та аудиту привілейованих користувачів

В розвитку інформаційних технологій особливу увагу приділяють захисту привілейованих облікових записів, оскільки вони мають розширені права доступу до критичних систем і даних. Саме тому все більшого поширення набуває підхід управління привілейованим доступом (Privileged Access Management, PAM), який спрямований на контроль, моніторинг і аудит облікових записів [16].

PAM є комплексом технологій і організаційних заходів, що дозволяють обмежити доступ до важливих ресурсів лише для авторизованих користувачів. До таких користувачів належать системні адміністратори, адміністратори баз даних та інші співробітники з підвищеними правами. Основною метою впровадження PAM є зменшення ризиків витоку даних, запобігання несанкціонованому доступу та підвищення загального рівня інформаційної безпеки організації [17].

Одним із ключових механізмів PAM є централізоване управління привілейованими обліковими записами, яке забезпечує контроль усіх користувачів із підвищеними правами в межах єдиної системи. Це дозволяє чітко розуміти, хто і до яких ресурсів має доступ, а також спрощує процес адміністрування [16].

Важливою складовою є також захищене зберігання облікових даних (password vault). У таких системах паролі не зберігаються у відкритому вигляді, а доступ до них здійснюється через спеціалізовані механізми. Крім того, паролі

можуть автоматично змінюватися, що значно знижує ризик їх компрометації [17].

Ще одним важливим механізмом є моніторинг і запис дій користувачів. Системи PAM дозволяють фіксувати всі дії привілейованих користувачів у вигляді журналів або записів сесій. Це дає змогу проводити аудит, аналізувати інциденти безпеки та швидко виявляти підозрілу активність [16].

Крім того, широко застосовується принцип найменших привілеїв (Least Privilege), відповідно до якого користувач отримує лише ті права доступу, які необхідні для виконання його обов'язків. Такий підхід дозволяє значно зменшити можливості для зловживань або випадкових помилок [17].

Для підвищення рівня захисту використовується багатофакторна автентифікація (MFA), яка додає додатковий рівень перевірки особи користувача. Це особливо важливо для привілейованих облікових записів, оскільки навіть у разі компрометації пароля доступ до системи залишатиметься захищеним [16].

Окремо варто виділити механізм тимчасового доступу (Just-In-Time), який передбачає надання прав доступу лише на обмежений період часу. Це дозволяє уникнути ситуацій, коли користувачі постійно мають надлишкові привілеї, що підвищує рівень безпеки [17].

Також важливим елементом PAM є аудит і звітність, які реалізуються через ведення журналів подій та формування звітів. Це дозволяє відстежувати всі дії користувачів, забезпечує прозорість роботи системи та допомагає дотримуватися вимог нормативних стандартів [16].

Наслідки невикористання управління привілейованим доступом (PAM) [17]. Відмова від реалізації управління привілейованим доступом (PAM) може призвести до значних ризиків безпеки та операційних проблем для організації:

1. Підвищений ризик витоку даних. Привілейовані облікові записи мають підвищені дозволи, які можна використати для доступу до критичних систем і конфіденційних даних. Без PAM ці облікові записи більш вразливі до таких атак, як фішинг, крадіжка облікових даних і Brute force атаки. Згідно зі

звітом Verizon про розслідування порушень даних, зловживання привілеями було пов’язане з 74% порушень даних.

2. Порушення комплаєнсу. Багато норм і галузевих стандартів, такі як GDPR, ISO 27001, SOC 2 та PCI DSS, вимагають суворого контролю над привілейованим доступом. Недотримання вимог може призвести до великих штрафів, юридичних наслідків і шкоди репутації організації. У звіті IBM Cost of a Data Breach Report за 2023 рік зазначено, що середня вартість витоку даних, пов’язаного з невідповідністю, становить 5,65 мільйонів доларів.

3. Операційна неефективність. Без PAM управління привілейованими обліковими записами стає громіздким процесом. Це може призвести до неправильної конфігурації, випадкового підвищення привілеїв і адміністративних витрат. Неправильне управління привілеями може порушити бізнес-операції, спричинити простої та вплинути на продуктивність.

4. Внутрішні загрози. Співробітники або підрядники з надмірними або некерованими привілеями можуть навмисно чи ненавмисно зловживати своїм доступом. Внутрішні загрози важко виявити, і вони можуть завдати значної шкоди. Gartner повідомляє, що організації зі слабким контролем привілейованого доступу стикаються з інцидентами, пов’язаними з інсайдерськими загрозами, на 50% частіше, ніж організації з впровадженим PAM.

5. Втрата інтелектуальної власності. Привілейовані облікові записи часто мають доступ до конфіденційної інформації та інтелектуальної власності. Несанкціонований доступ до цих активів може призвести до невигідного конкурентного становища та фінансових втрат. PAM допомагає захистити цінні активи, забезпечуючи доступ до конфіденційної інформації лише авторизованим особам.

6. Збільшена поверхня атаки. Без PAM збільшується кількість користувачів із надмірними привілеями, розширюючи зону атаки для кібер-зловмисників. Це полегшує зловмисникам пошук і використання слабких місць в інфраструктурі безпеки організації.

7. Відсутність підзвітності та видимості. Без належного управління та моніторингу привілейованих облікових записів важко відстежувати та перевіряти дії користувачів. Така відсутність видимості перешкоджає здатності організації виявляти підозрілу поведінку та оперативно реагувати на неї. PAM надає детальні журнали аудиту та можливості моніторингу, покращуючи видимість і підзвітність.

Отже, механізми управління доступом та аудиту привілейованих користувачів є важливою складовою системи інформаційної безпеки. Вони дозволяють не лише контролювати доступ до критичних ресурсів, але й своєчасно виявляти потенційні загрози, що значно знижує ризики кіберінцидентів у корпоративних мережах.

Висновки до розділу 2

У другому розділі було проведено аналіз методів і засобів моніторингу активності користувачів на базі платформи Syteca UAM. У результаті дослідження встановлено, що дана платформа є сучасним комплексним рішенням у сфері інформаційної безпеки, яке поєднує функціональні можливості моніторингу активності користувачів (UAM) та управління привілейованим доступом (PAM).

У підрозділі 2.1 було розглянуто архітектуру та функціональні можливості Syteca. Визначено, що система має модульну структуру та дозволяє організації використовувати лише необхідний функціонал, що підвищує гнучкість і ефективність її впровадження. Особливу увагу приділено можливостям виявлення та керування привілейованими обліковими записами, що є критично важливим для забезпечення безпеки корпоративних мереж.

У підрозділі 2.2 досліджено методи виявлення аномальної поведінки користувачів. Встановлено, що поєднання поведінкового аналізу, правилозорієнтованих підходів, статистичних методів та алгоритмів машинного навчання дозволяє ефективно виявляти як типові, так і складні кіберзагрози.

Окремо було розглянуто механізми сповіщення у реальному часі, які забезпечують оперативне реагування на інциденти та значно зменшують їх негативні наслідки.

У підрозділі 2.3 проаналізовано механізми управління доступом та аудиту привілейованих користувачів. Визначено, що використання підходу PAM дозволяє реалізувати централізований контроль доступу, застосування принципу найменших привілеїв, багатофакторну автентифікацію, моніторинг дій користувачів та ведення аудиту. Це значно знижує ризики несанкціонованого доступу, внутрішніх загроз і витоку даних.

Отже, результати дослідження показали, що використання платформи Syteca UAM у поєднанні з сучасними методами аналізу поведінки користувачів та механізмами управління привілейованим доступом дозволяє суттєво підвищити рівень інформаційної безпеки організації. Комплексне застосування цих підходів забезпечує ефективний контроль за діями користувачів, своєчасне виявлення загроз і можливість швидкого реагування на інциденти кібербезпеки.

Розділ 3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ SYTECA UAM В ОРНАНІЗАЦІЇ

3.1 Розгортання та налаштування системи моніторингу аномальної поведінки на базі Syteca UAM

Розгортання системи моніторингу аномальної поведінки на базі платформи Syteca здійснювалось у середовищі Windows із використанням компонентів серверної частини та вебінтерфейсу адміністратора. Основною метою впровадження було забезпечення централізованого контролю дій користувачів, моніторингу привілейованих сесій та збору інформації про потенційно аномальну активність.

На початковому етапі було виконано запуск інсталяційного пакета Syteca [18]. Майстер встановлення містить покрокову процедуру налаштування компонентів системи, що дозволяє адміністратору швидко виконати базову конфігурацію середовища (рис. 3.1).

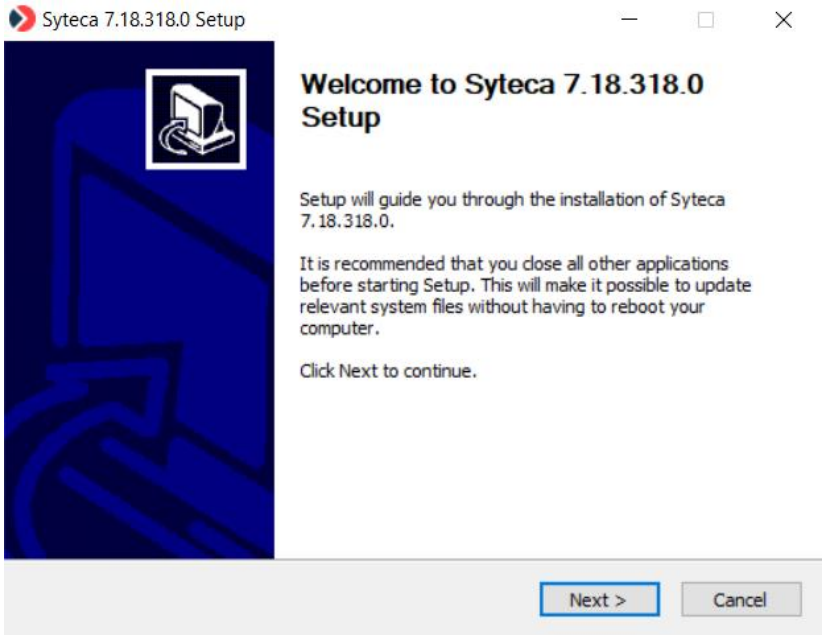

Рис. 3.1 Початкове вікно майстра встановлення Syteca

Після запуску інсталятора було обрано тип розгортання системи. На даному етапі виконується визначення ролей компонентів та параметрів встановлення серверної частини системи моніторингу (рис. 3.2).

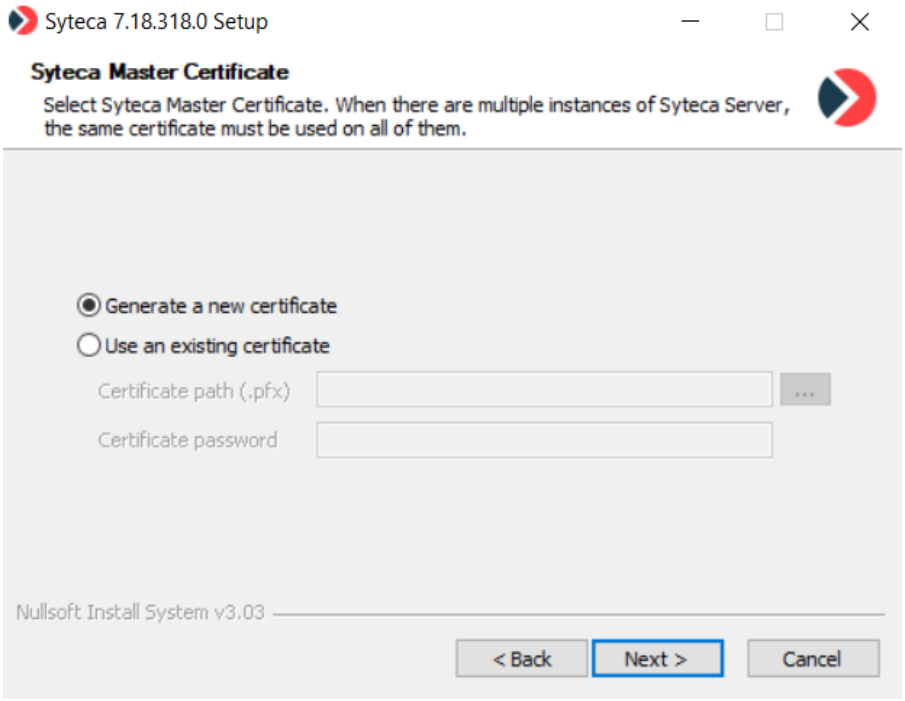

Рис. 3.2 Вибір конфігурації встановлення Syteca

Наступним кроком стало налаштування параметрів підключення до бази даних Microsoft SQL Server. У вікні конфігурації було вказано ім’я сервера бази даних, параметри автентифікації та назву бази даних для збереження журналів подій і записів активності користувачів (рис. 3.3).

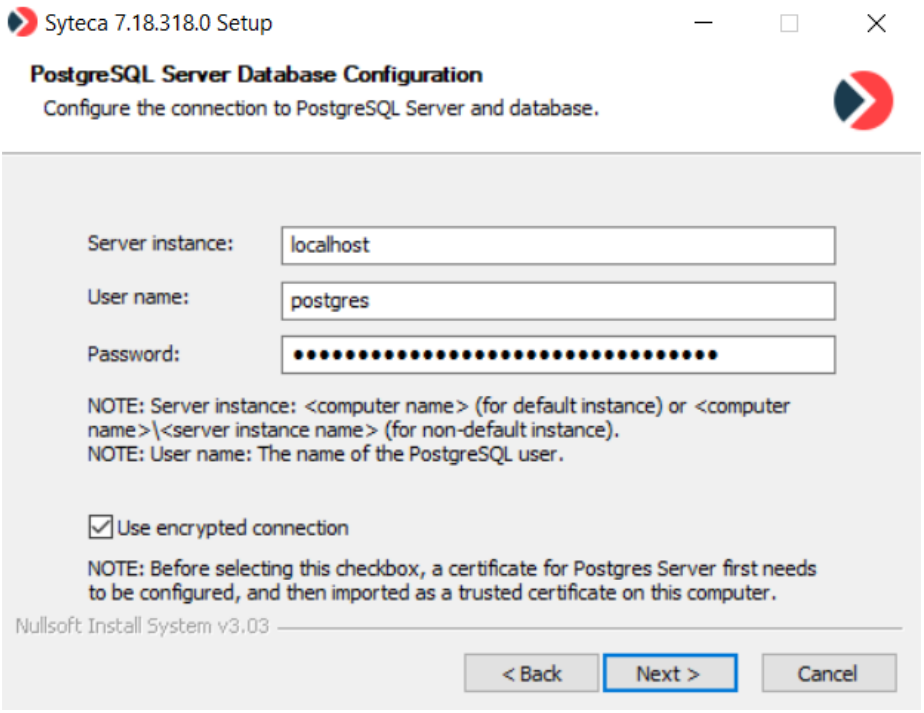

Рис. 3.3 Налаштування підключення до SQl Server

Після цього виконувалось створення облікового запису адміністратора системи Syteca. На даному етапі задавались параметри автентифікації, логін та пароль адміністратора для подальшого доступу до вебконсолі управління (рис. 3.4).

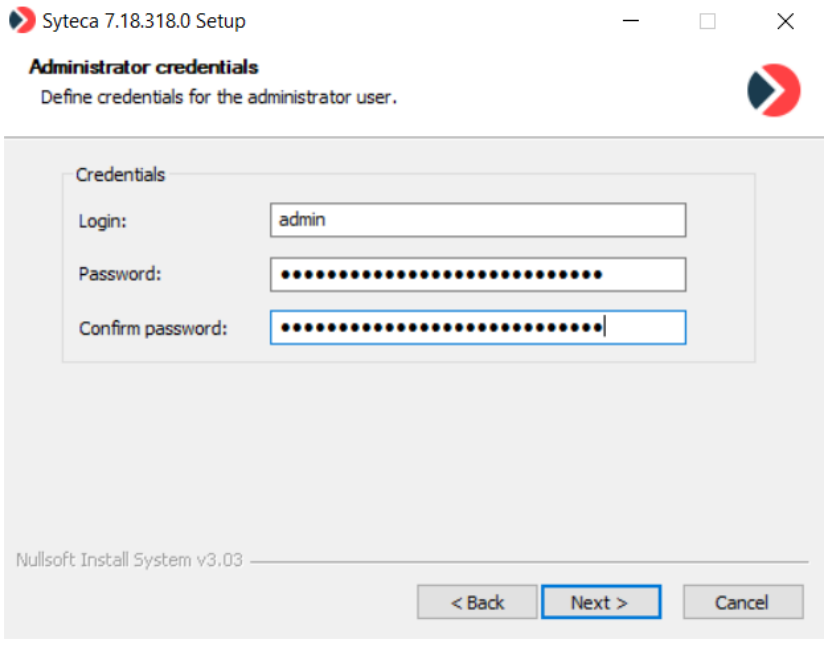

Рис. 3.4 Створення адміністративного облікового запису

Далі система перевірила наявність необхідних компонентів та залежностей для коректної роботи серверної частини. У процесі встановлення були автоматично визначені відсутні програмні компоненти та підготовлено середовище до інсталяції (рис. 3.5).

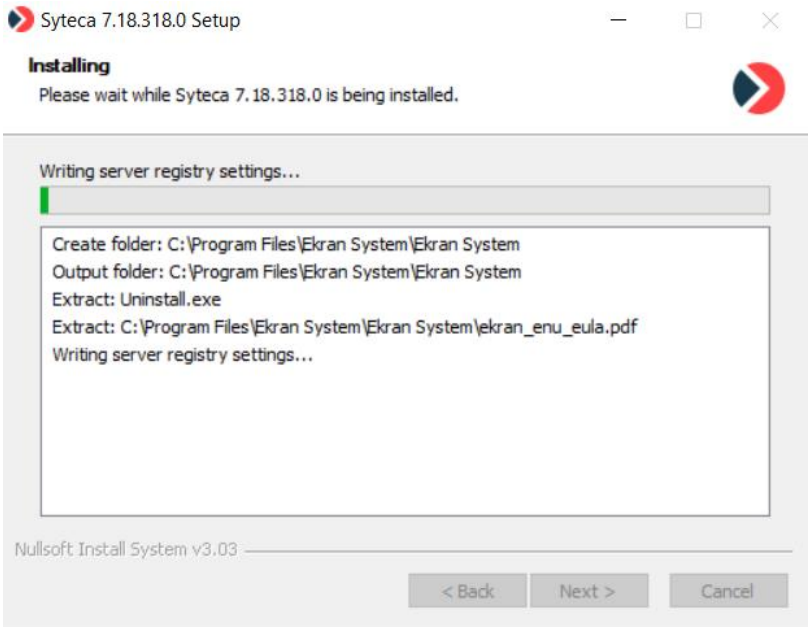

Рис. 3.5 Перевірка системних компонентів під час інсталяції

Для коректної роботи вебінтерфейсу було активовано компоненти Internet Information Services (IIS) у середовищі Windows. Зокрема, були ввімкнені служби вебсервера та сумісні компоненти, необхідні для функціонування вебконсолі Syteca (рис. 3.6).

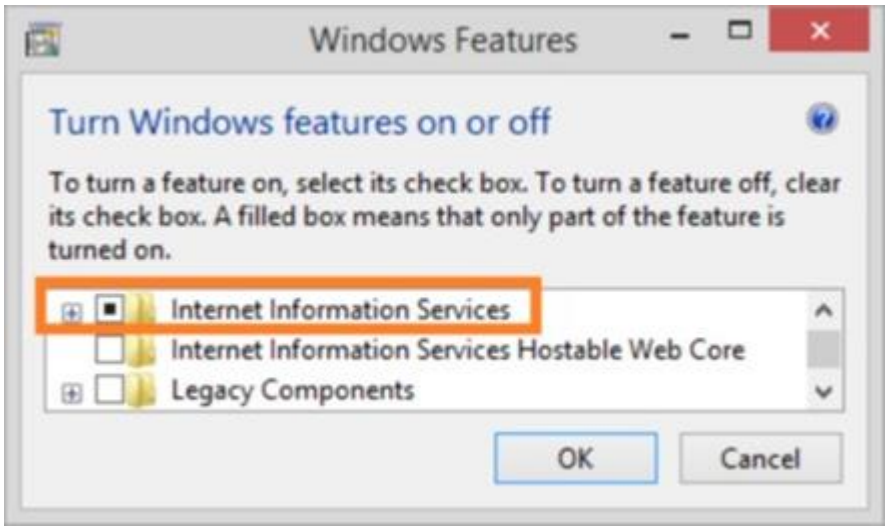

Рис. 3.6 Увімкнення компонентів IIS у Windows

Після завершення встановлення виконувалось налаштування мережевих параметрів і служб системи. Також було проведено запуск необхідних сервісів через командний рядок Windows із правами адміністратора (рис. 3.7).

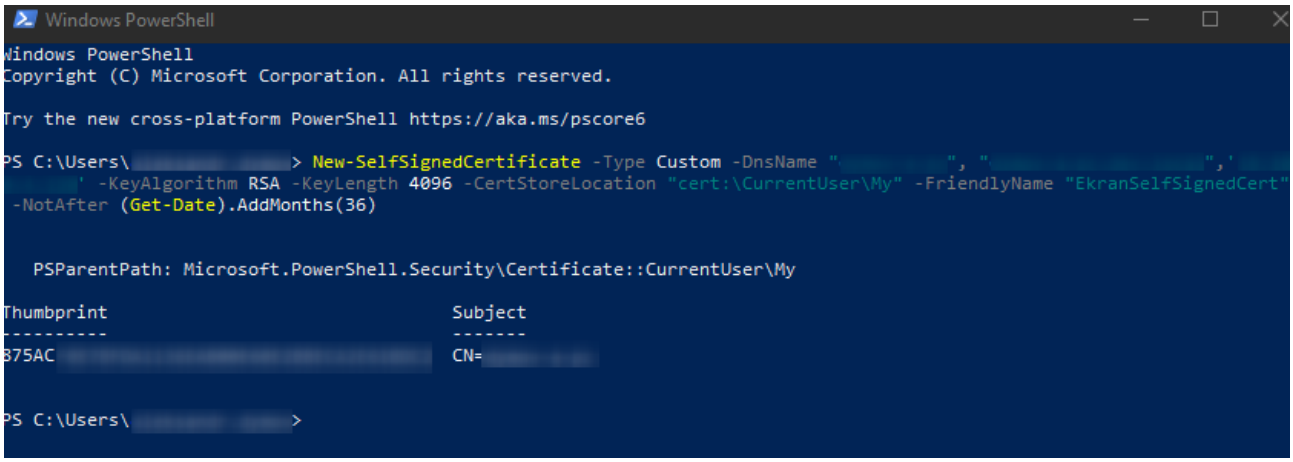

Рис. 3.7 Запуск та налаштування служб Syteca через PowerShell

На наступному етапі було налаштовано параметри мережевого підключення та адресацію серверної частини системи. У конфігурації задавались параметри сервера, мережевий порт і шляхи доступу до служб Syteca (рис. 3.8).

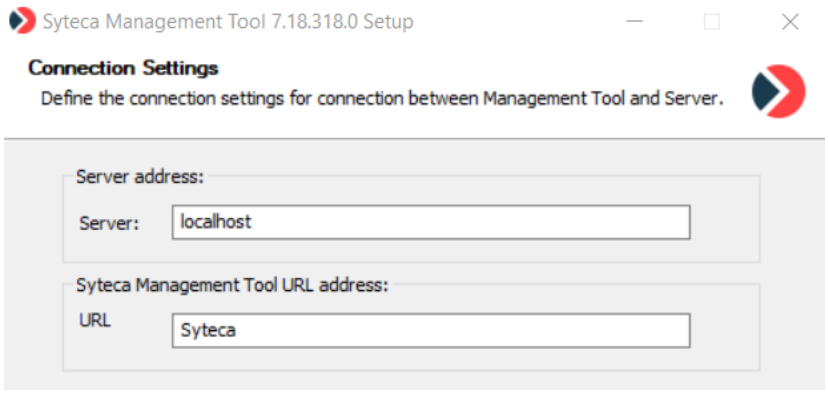

Рис. 3.8 Конфігурація мережевих параметрів системи

Після завершення встановлення та початкової конфігурації було виконано авторизацію у вебінтерфейсі адміністратора Syteca через браузер. Вебконсоль забезпечує централізоване управління політиками моніторингу, агентами та подіями безпеки (рис. 3.9).

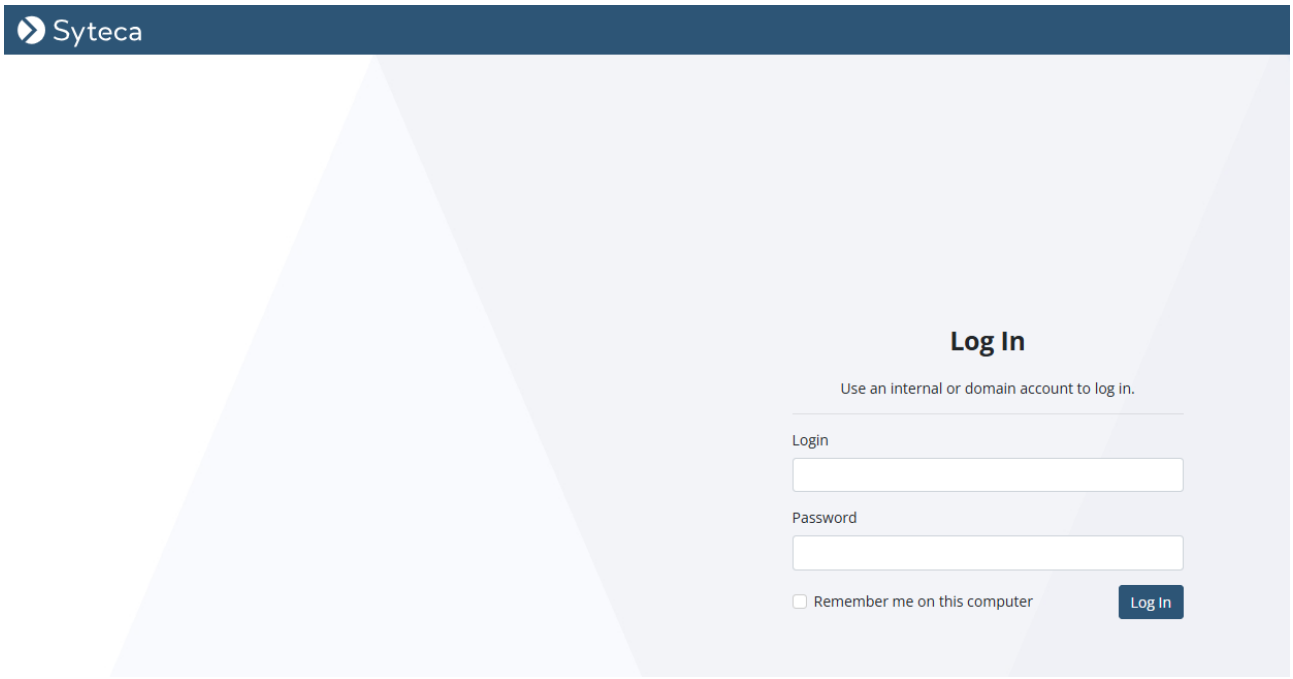

Рис. 3.9 Вебінтерфейс авторизації Syteca

Після входу до системи адміністратор отримує доступ до інформаційної панелі управління. У ній відображаються основні параметри системи, статус агентів, події безпеки та елементи керування моніторингом (рис. 3.10).

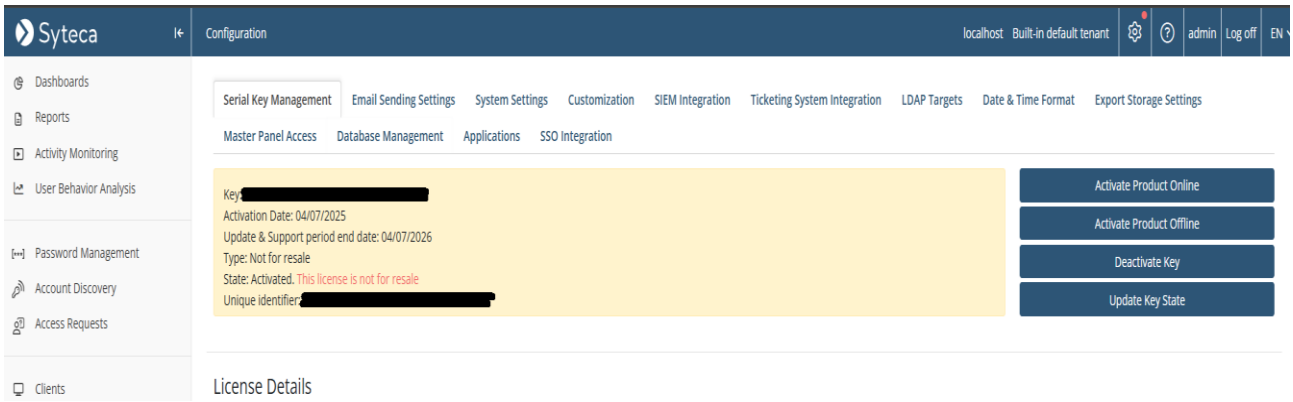

Рис. 3.10 Головна панель управління Syteca

Для виявлення робочих станцій у мережі було виконано сканування локального середовища. Під час сканування система автоматично визначає доступні вузли, домени та комп’ютери для подальшого розгортання агентів моніторингу (рис. 3.11).

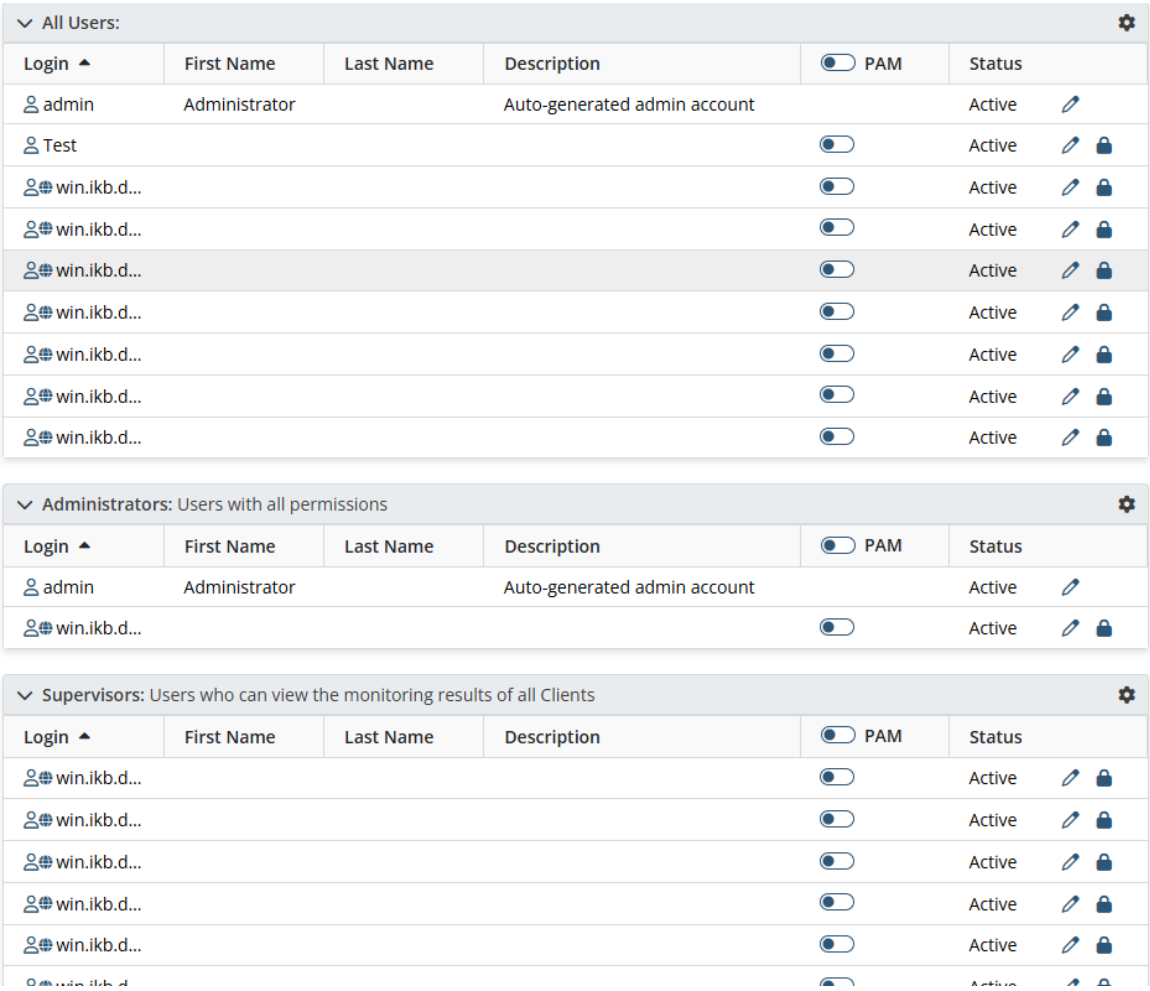

Рис. 3.11 Сканування мереж для виявлення робочих станцій

Після завершення сканування було сформовано список виявлених хостів та пристроїв. Отримана інформація використовується для централізованого розгортання агентів моніторингу на робочих станціях користувачів (рис. 3.12).

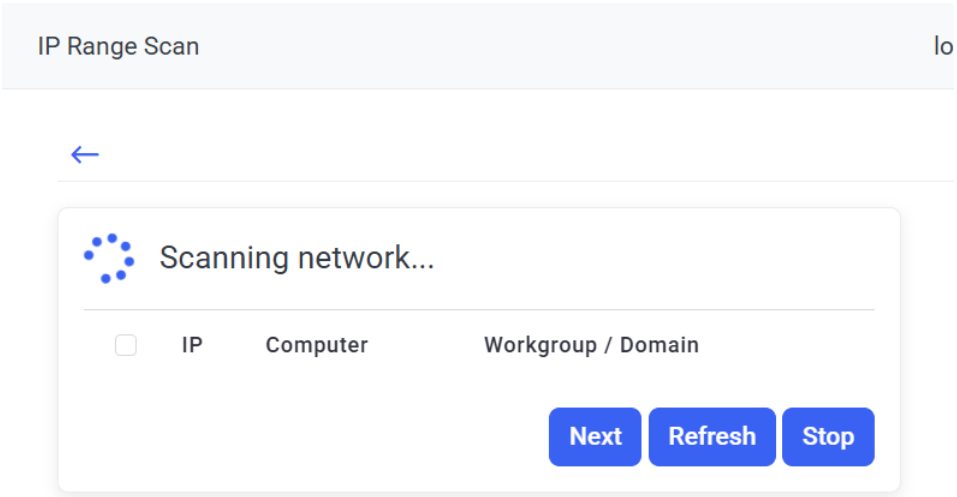

Рис. 3.12. Результати мережевого сканування

На наступному етапі здійснювалось додавання агентів до системи моніторингу. Для кожного вузла визначався статус підключення, IP-адреса, ім’я комп’ютера та поточний стан агента (рис. 3.13).

Рис. 3.13. Перелік підключених агентів Syteca

Далі було створено політики моніторингу дій користувачів. Політики дозволяють налаштувати правила запису сесій, контролю активності, моніторингу запуску процесів та фіксації підозрілих дій (рис. 3.14).

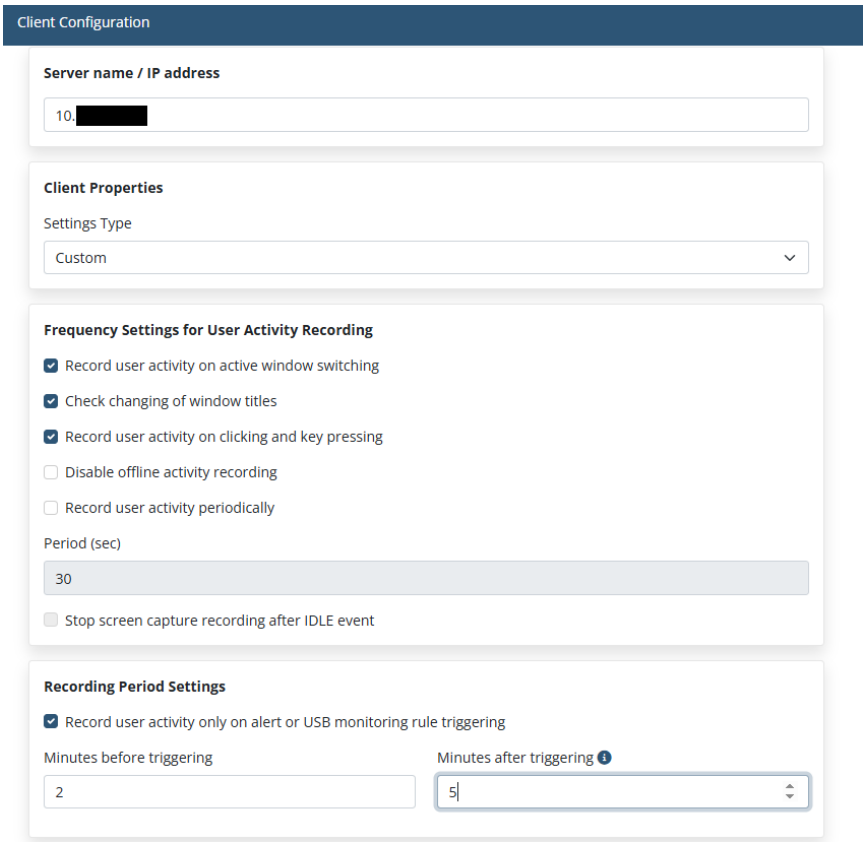

Рис. 3.14. Налаштування політик моніторингу

У системі також було налаштовано параметри сповіщень та журналювання подій. Це дозволяє автоматично реєструвати критичні дії користувачів і створювати повідомлення у випадку виявлення аномальної поведінки (рис. 3.15).

Рис. 3.15. Налаштування журналювання та подій безпеки

Після налаштування політик було перевірено працездатність агентів та збір подій у режимі реального часу. У консолі адміністратора відображаються активні сесії користувачів, записи подій та стан моніторингу системи (рис. 3.16).

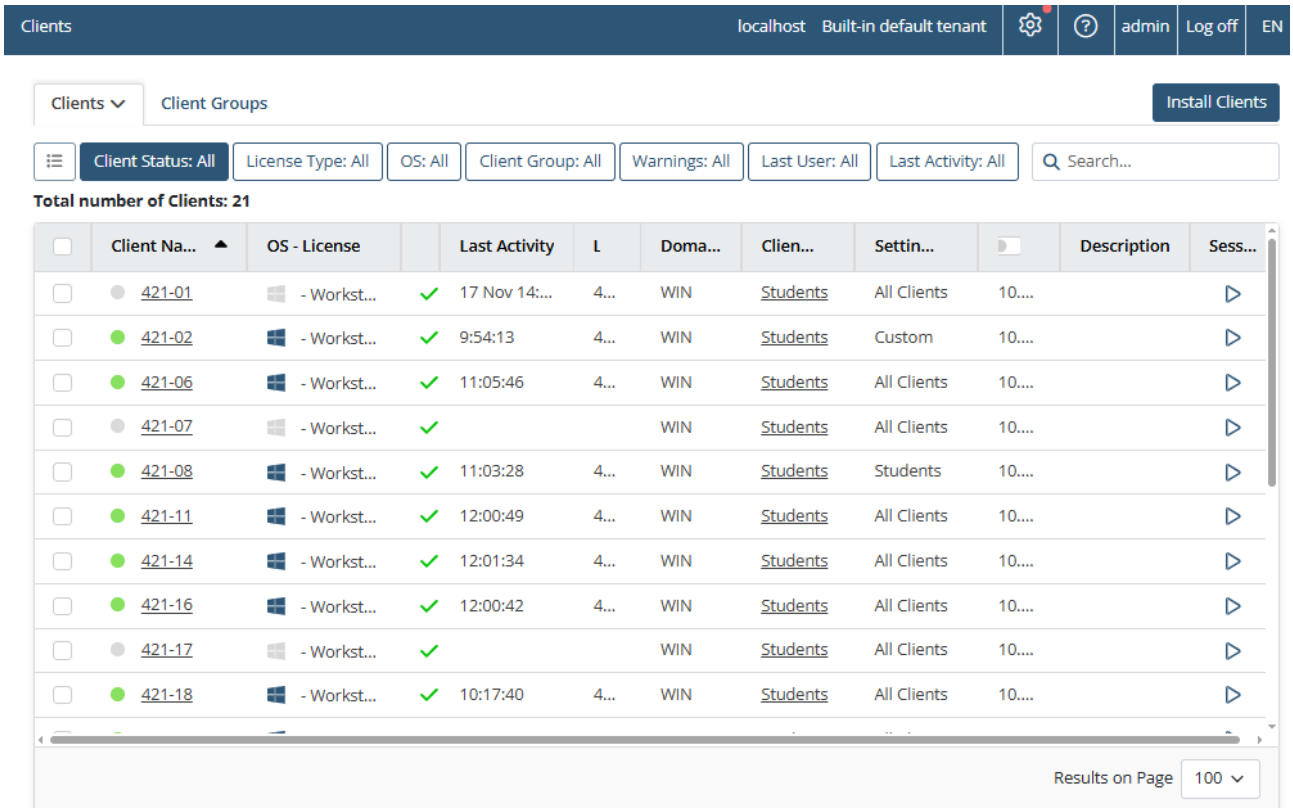

Рис. 3.16. Контроль активних сесій користувачів

Після базового налаштування було виконано конфігурацію параметрів запису сесій користувачів. У даному режимі система забезпечує фіксацію дій користувачів, запис активності на робочому столі та збереження журналів подій для подальшого аналізу інцидентів безпеки (рис. 3.17).

[Default] Running a cloud backup application	This is an alert on running a cloud backup software that can copy files/folders to a remote location.	Enabled	None
[Default] Running CD or DVD burning tools	This is an alert on running a CD/DVD burning software.	Enabled	None
[Default] Synchronizing MS-Office document with another Microsoft account	This is an alert on opening the Switch Account window in Microsoft Office applications.	Enabled	None
[Default] Running steganography tools	This is an alert on running one of the predefined stenography tools that are usually used to conceal text information within images.	Enabled	None
[Default] Password protecting Excel file	This is an alert on opening the General Options screen in Microsoft Excel to potentially set a password protection upon saving a file.	Enabled	None
[Default] Password protecting Word file	This is an alert on opening the General Options screen in Microsoft Word to potentially set a password protection upon saving a file.	Enabled	None

Рис. 3.17. Налаштування параметрів запису сесій користувачів

Також було виконано налаштування контролю доступу та привілеїв користувачів у системі. Адміністратор може визначати рівні доступу до функцій моніторингу, журналів подій та параметрів управління платформою Syteca (рис. 3.18).

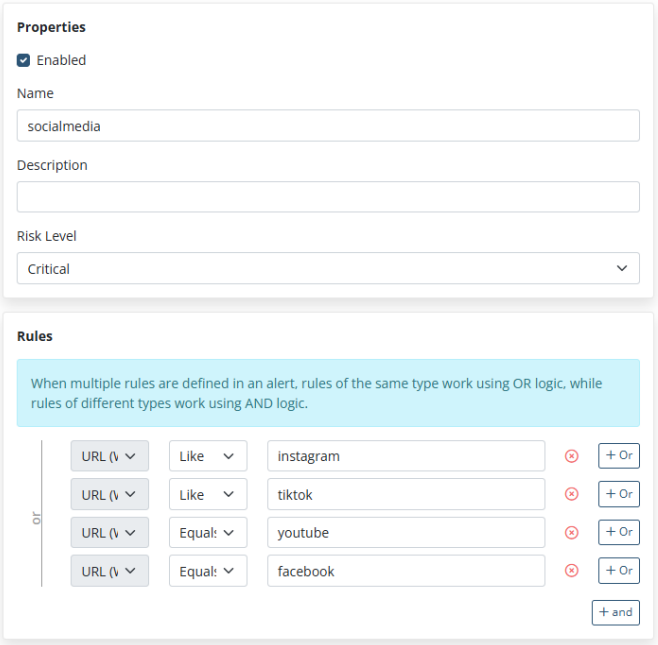

Рис. 3.18 – Налаштування прав доступу користувачів

Для аналізу подій безпеки було використано вбудовані журнали аудиту та модулі перегляду активності користувачів. Система дозволяє переглядати історію подій, фільтрувати записи та здійснювати пошук потенційно аномальної активності (рис. 3.19).

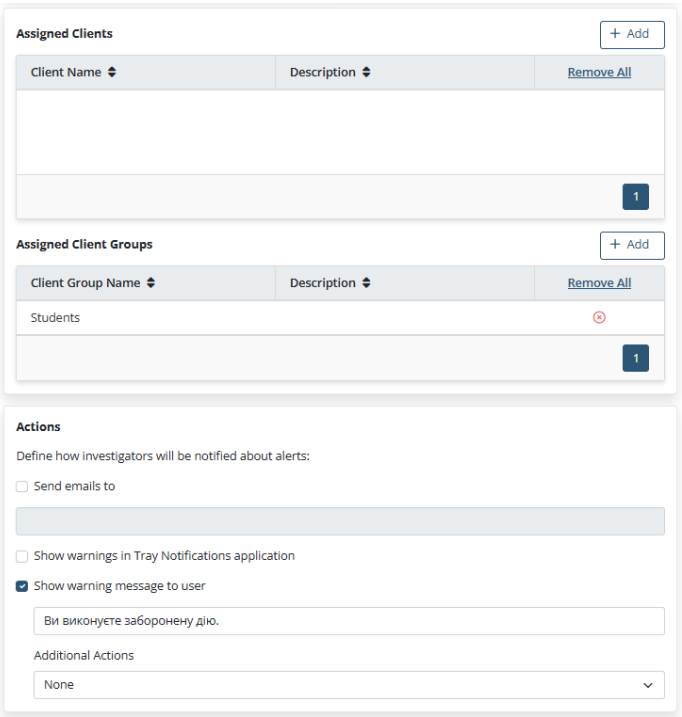

Рис. 3.19. Перегляд журналів аудиту та подій безпеки

На завершальному етапі було перевірено формування звітів та експорт зібраної інформації. Звіти можуть використовуватись для проведення аудиту інформаційної безпеки, аналізу інцидентів та контролю діяльності користувачів у корпоративному середовищі (рис. 3.20).

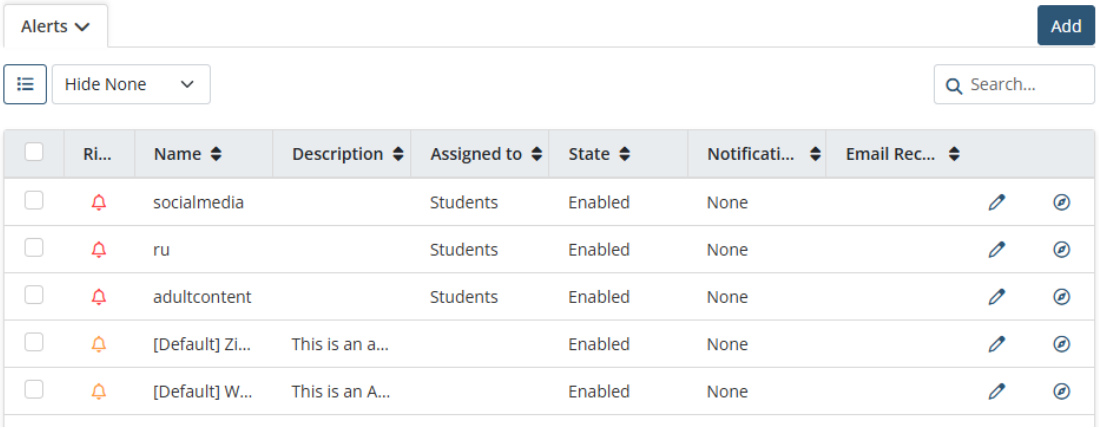

Рис. 3.20. Формування та експорт звітів у Syteca

На завершальному етапі було протестовано функціонування системи моніторингу аномальної поведінки. Перевірка показала, що платформа Syteca забезпечує централізований збір подій, контроль привілейованого доступу, аудит дій користувачів та ефективний моніторинг потенційно небезпечної активності.

Отже, розгортання та налаштування Syteca дозволило створити повноцінне середовище моніторингу аномальної поведінки користувачів із можливістю централізованого адміністрування, аналізу подій безпеки та контролю привілейованих облікових записів.

3.2 Порядок проведення розлідувань інцидентів кібербезпеки за допомогою Syteca

Розслідування інцидентів кібербезпеки в системі Syteca здійснюється шляхом централізованого моніторингу дій користувачів, аналізу активності робочих станцій та формування звітів щодо потенційно небезпечних подій. Платформа забезпечує фіксацію дій користувачів, збір журналів активності, контроль привілейованих облікових записів та можливість швидкого аналізу інцидентів інформаційної безпеки.

На початковому етапі розслідування спеціаліст з інформаційної безпеки входить до вебінтерфейсу Syteca та аналізує загальний стан системи моніторингу. На головній панелі відображаються статистичні показники, графіки активності користувачів, кількість зафіксованих подій та рівень потенційних ризиків (рис. 3.21).

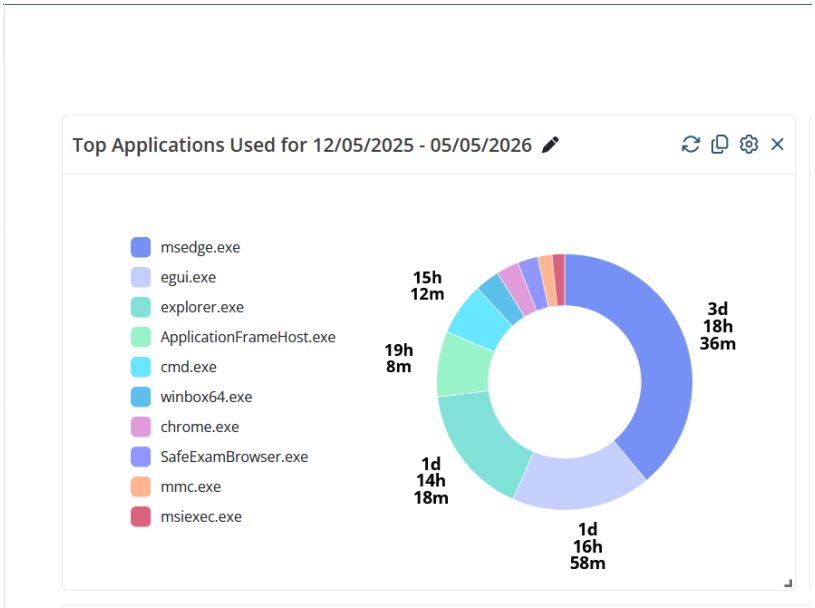

Рис. 3.21. Діаграма розподілу активності користувачів Syteca

Після отримання повідомлення про підозрілу активність адміністратор переходить до розділу детального аналізу активності користувачів. У системі формується перелік подій із зазначенням користувача, часу виконання дії, типу операції та рівня ризику. Це дозволяє оперативно визначити джерело інциденту та встановити послідовність дій користувача (рис. 3.22).

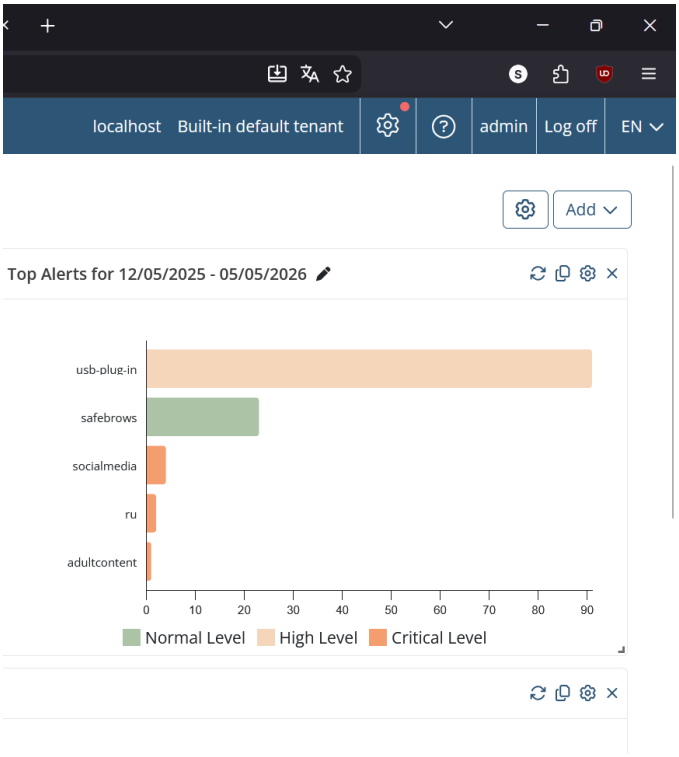

Рис. 3.22. Аналіз активності користувачів за процесами

Для більш детального дослідження інциденту використовується модуль Activity Monitoring, який відображає події, пов’язані з доступом до файлів, запуском програм, використанням зовнішніх носіїв інформації та мережевою активністю користувачів. Система дозволяє застосовувати фільтри за користувачем, IP-адресою, типом події або часовим проміжком (рис. 3.23).

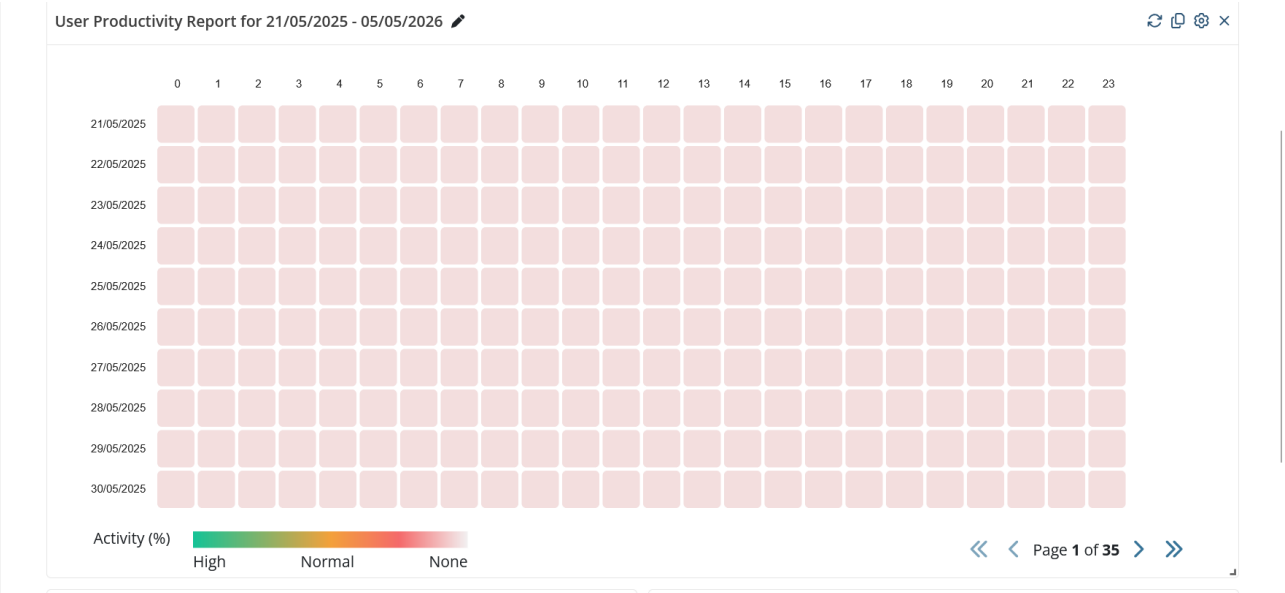

Рис. 3.23. Теплова карта активності користувачів

Однією з ключових можливостей Syteca є запис сесій користувачів. У процесі розслідування фахівець може переглянути відеозапис дій користувача на робочій станції, що дозволяє точно встановити послідовність виконаних операцій. Запис сесії містить інформацію про відкриті програми, введення команд та взаємодію користувача із системою (рис. 3.24).

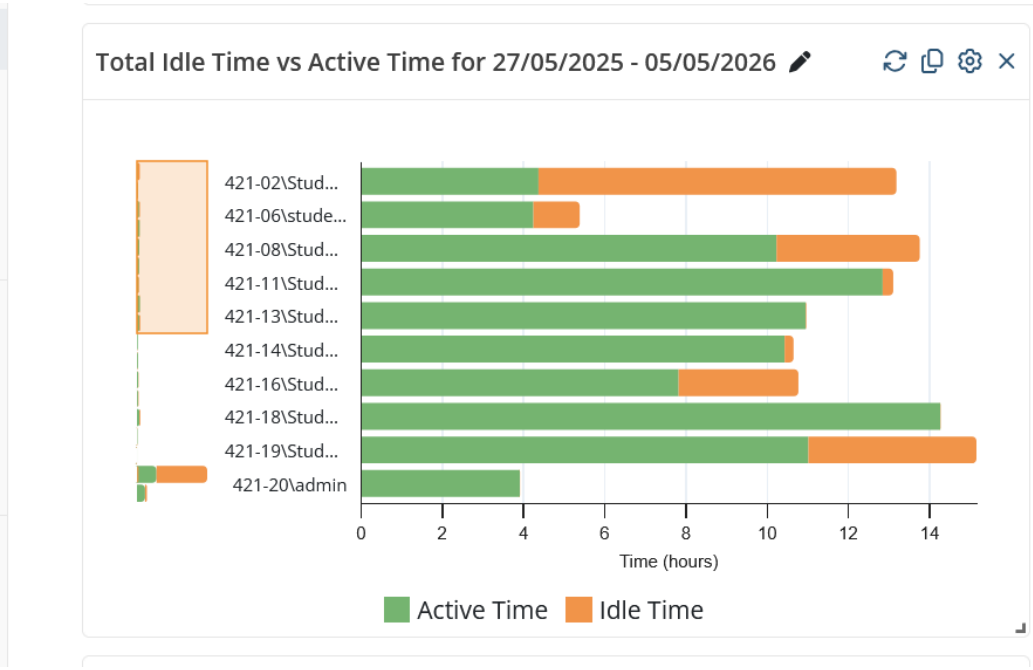

Рис. 3.24. Аналіз активності користувачів за часовими проміжками

Для аналізу інцидентів, пов’язаних із використанням привілейованих облікових записів, застосовується модуль PAM (Privileged Access Management). У цьому модулі адміністратор може контролювати доступ до критичних систем, переглядати інформацію про підключення користувачів та перевіряти історію використання привілейованих акаунтів (рис. 3.25).

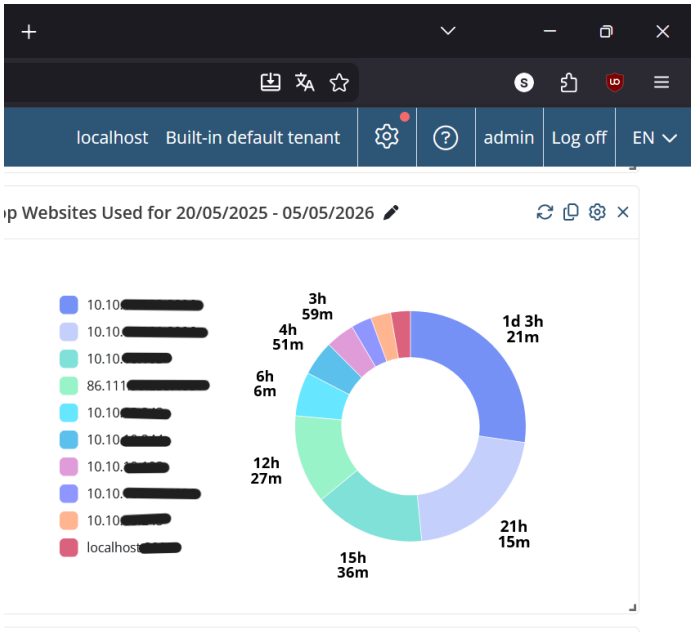

Рис. 3.25. Кругова діаграма активності користувачів

У разі виявлення підозрілих дій система дозволяє сформувати звіт щодо конкретного інциденту. Під час створення звіту обираються необхідні параметри: користувач, тип події, часовий інтервал, джерело події та рівень критичності. Після цього система автоматично генерує звіт для подальшого аналізу або передачі керівництву служби інформаційної безпеки (рис. 3.26).

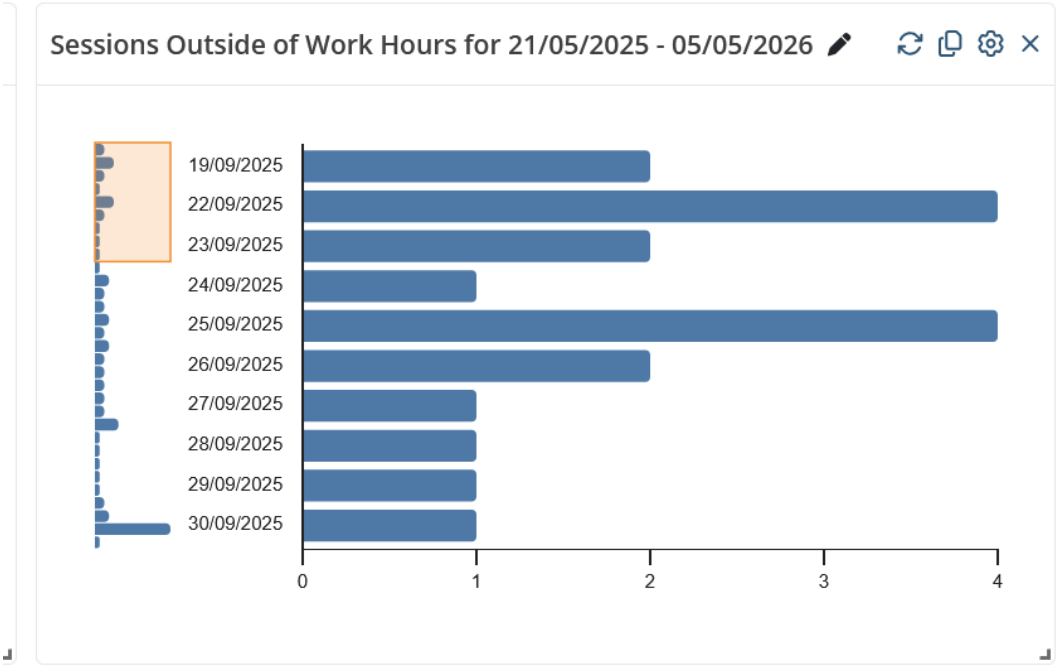

Рис. 3.26. Аналіз активності користувачів за типами подій

У Syteca також реалізовано функцію створення користувацьких звітів, що дозволяє адаптувати структуру звітності відповідно до потреб організації. Адміністратор може обирати параметри, які необхідно відобразити у звіті, а також встановлювати умови фільтрації подій (рис. 3.27).

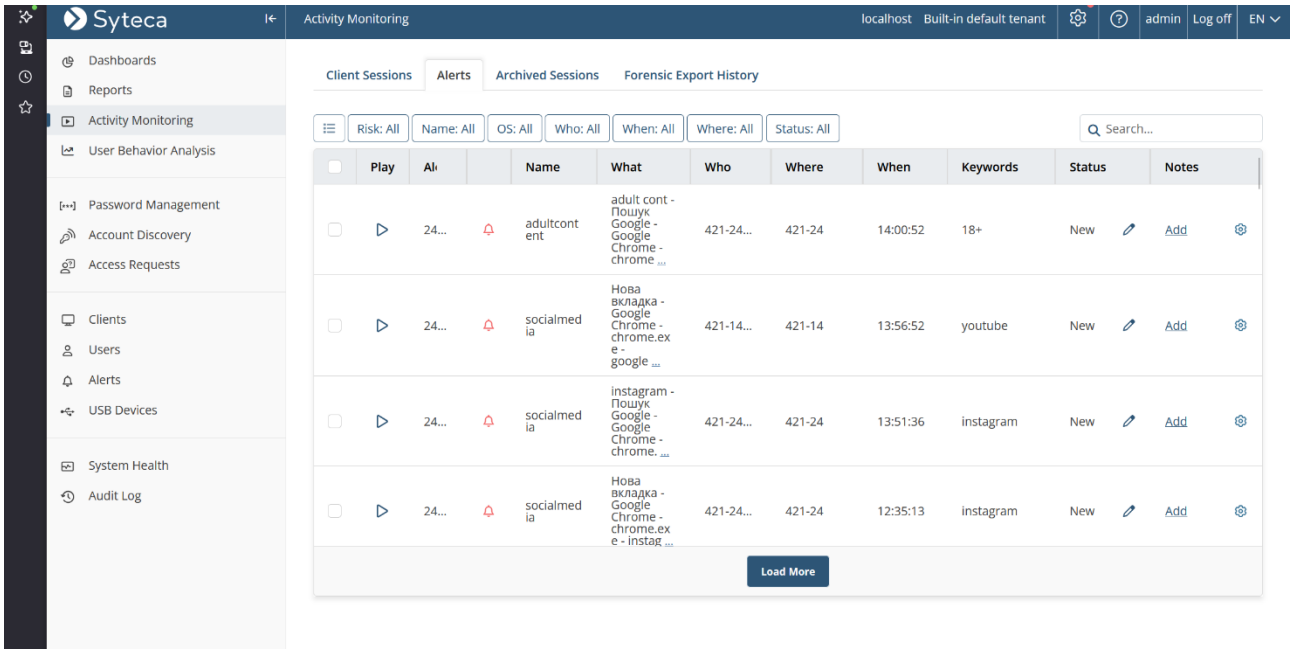

Рис. 3.27. Налаштування політик моніторингу в Syteca

На наступному етапі розслідування здійснюється аналіз журналів безпеки, які містять інформацію про всі дії користувачів у системі. Журнали подій дозволяють виявити несанкціоновані спроби доступу, запуск підозрілих процесів та зміну конфігурації системи (рис. 3.28).

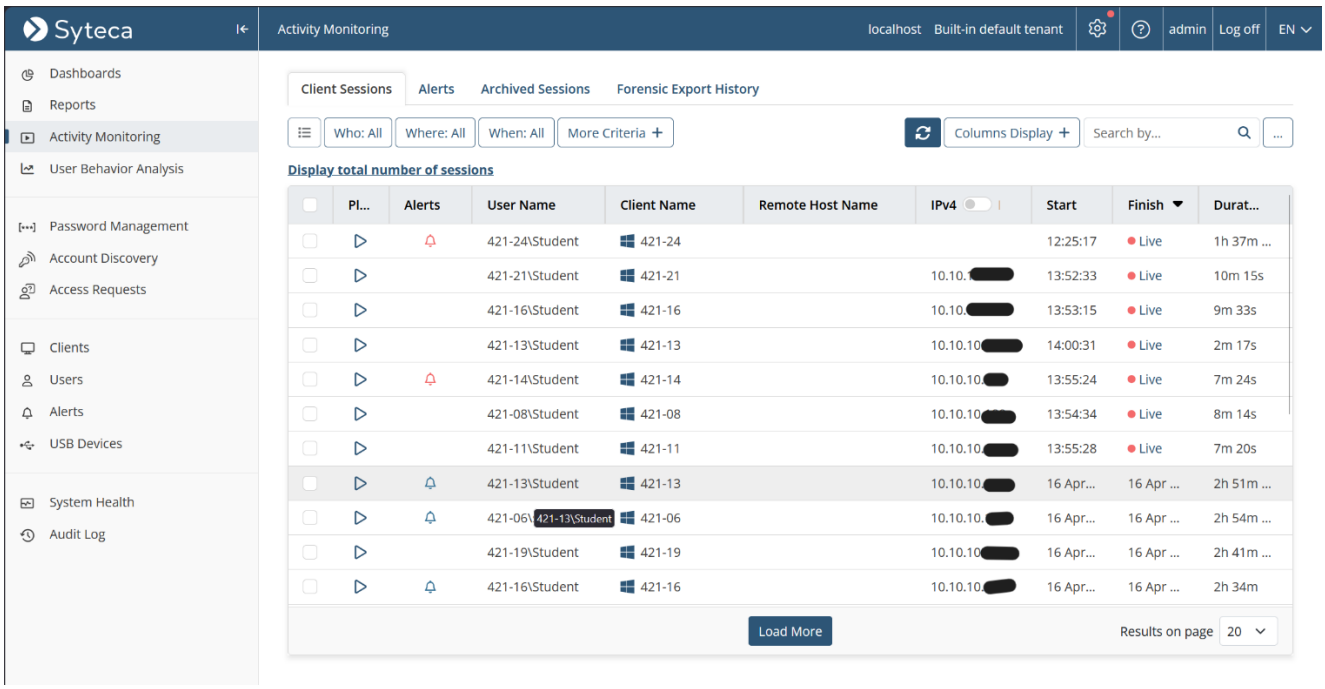

Рис. 3.28. Перегляд журналу подій користувачів

Під час розслідування інцидентів важливе значення має контроль використання зовнішніх носіїв інформації. Syteca фіксує підключення USB-пристроїв, передачу файлів та інші дії, пов’язані з копіюванням інформації (рис. 3.29).

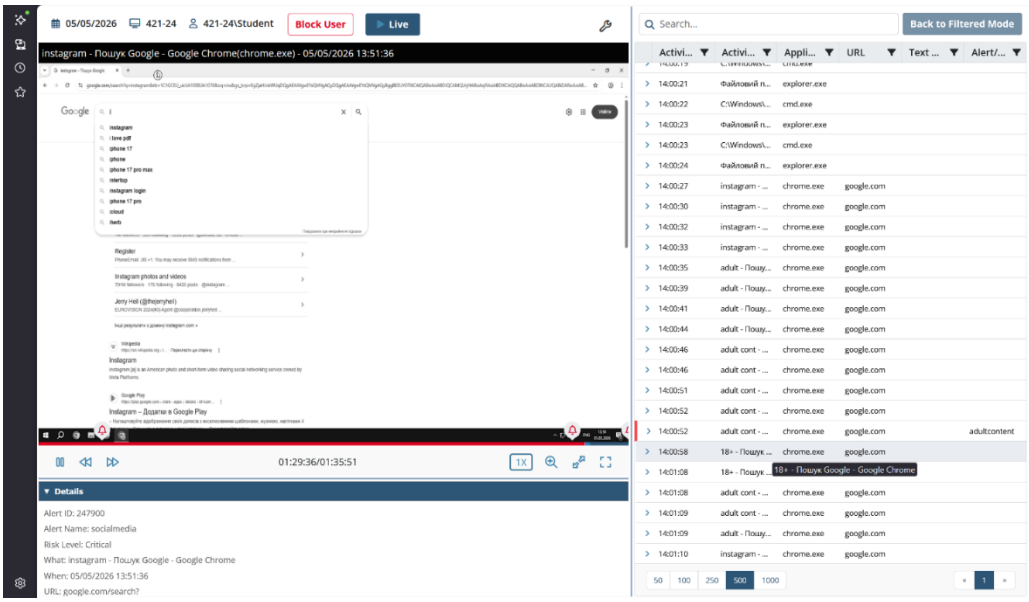

Рис. 3.29. Детальний перегляд подій у журналі Syteca

Система також забезпечує моніторинг запуску програмного забезпечення на робочих станціях користувачів. Це дозволяє виявляти запуск небажаних або потенційно небезпечних програм (рис. 3.30).

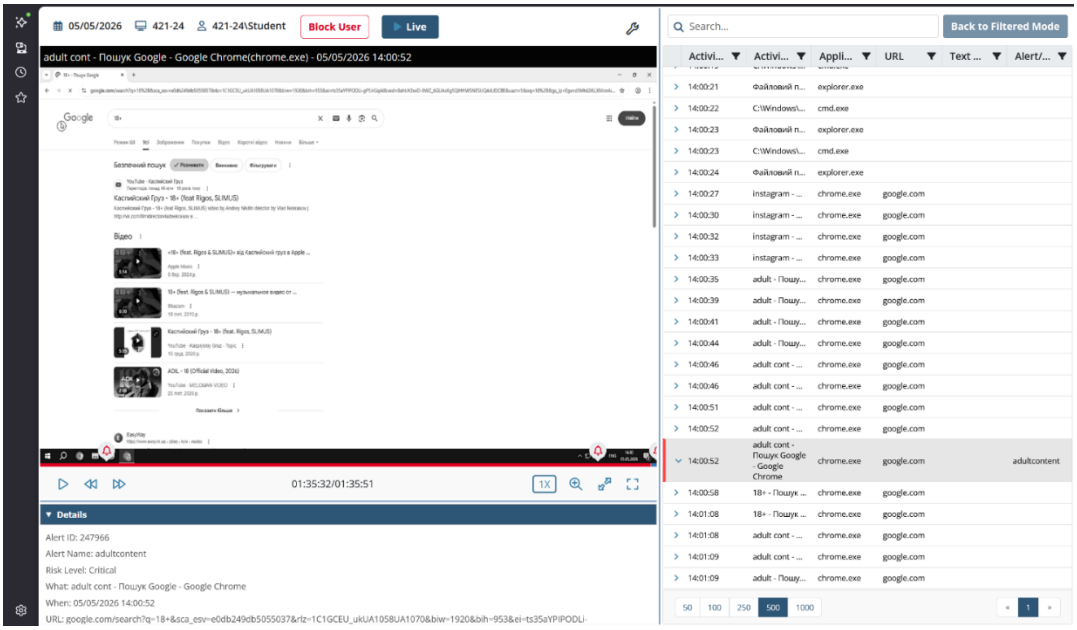

Рис. 3.30. Перегляд запису сесії користувача

Для оперативного реагування на інциденти у Syteca реалізовано систему сповіщень. У разі виявлення підозрілої активності система автоматично генерує повідомлення для адміністратора безпеки (рис. 3.31).

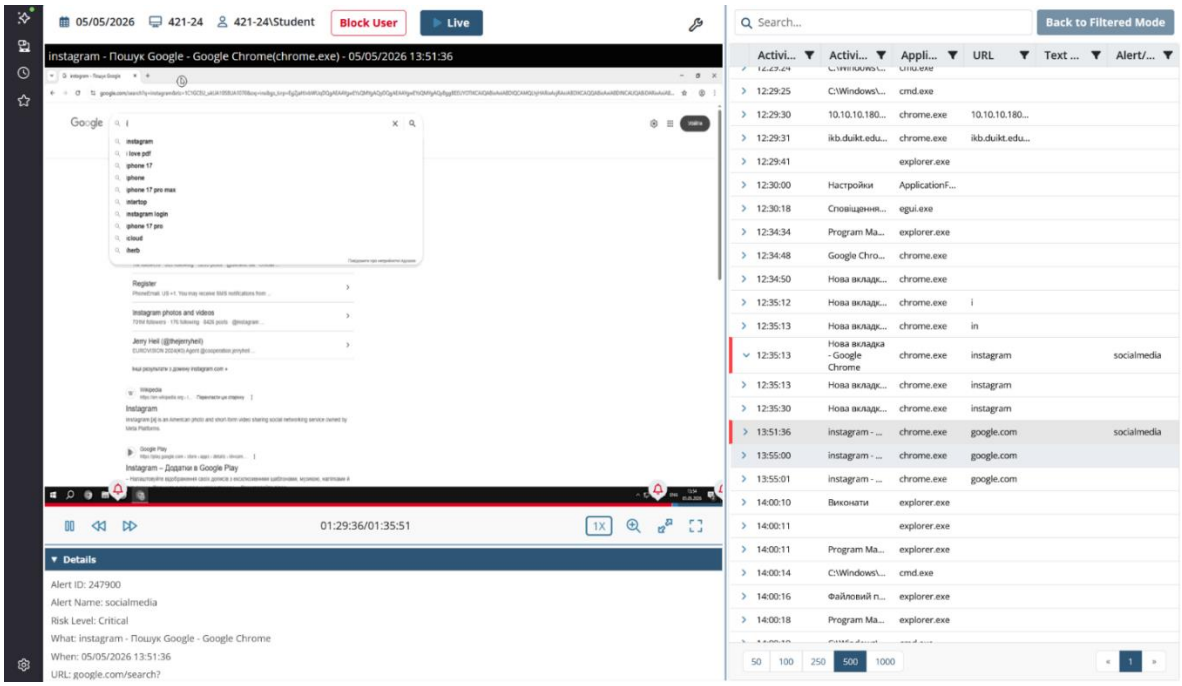

Рис. 3.31. Аналіз дій користувача під час сесії

Під час проведення розслідування адміністратор може використовувати функцію пошуку подій за різними параметрами. Це дозволяє швидко знаходити необхідну інформацію та скорочувати час аналізу інциденту (рис. 3.32).

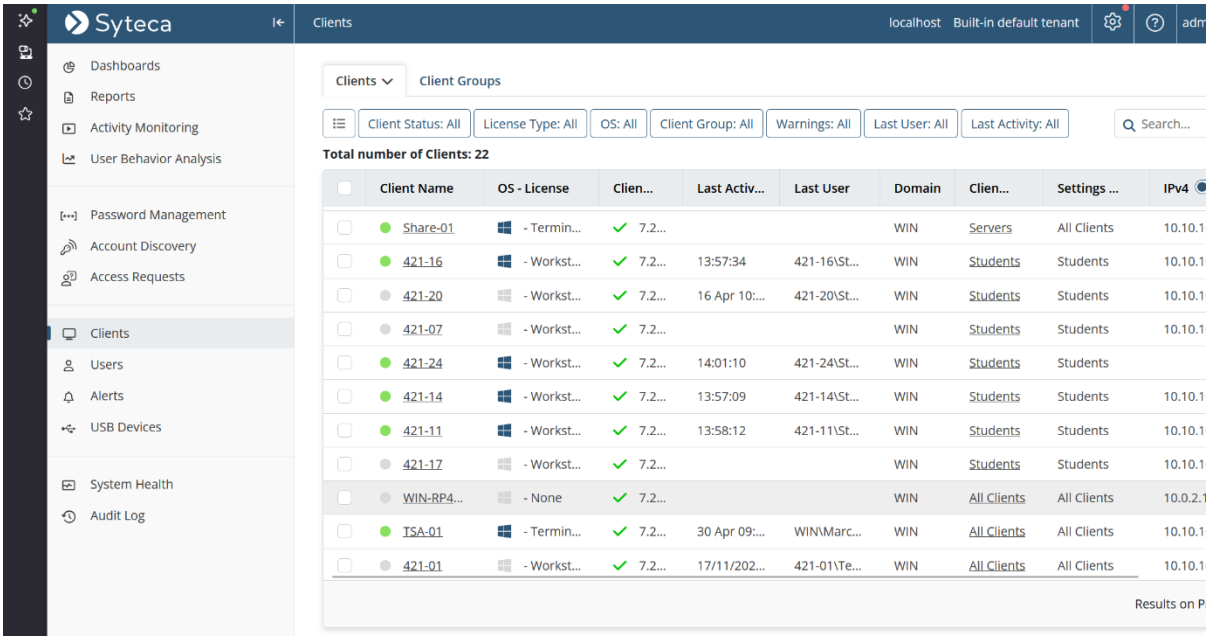

Рис. 3.32. Перегляд файлових операцій користувача

Додатково система дозволяє переглядати мережеву активність користувачів, включаючи інформацію про мережеві підключення та передачу даних між вузлами мережі (рис. 3.33).

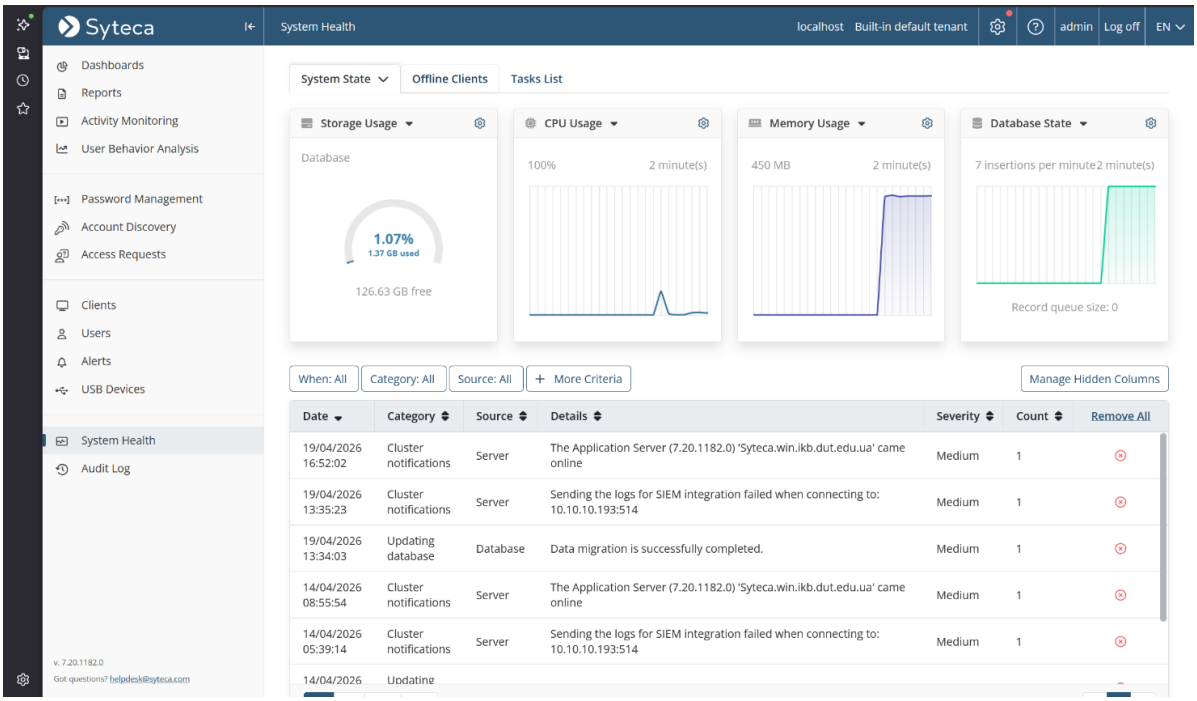

Рис. 3.33. Інформаційна панель моніторингу інцидентів

У процесі аналізу інцидентів також можуть використовуватися інструменти оцінки ризиків, які допомагають визначити критичність події та можливі наслідки для інформаційної системи організації (рис. 3.34).

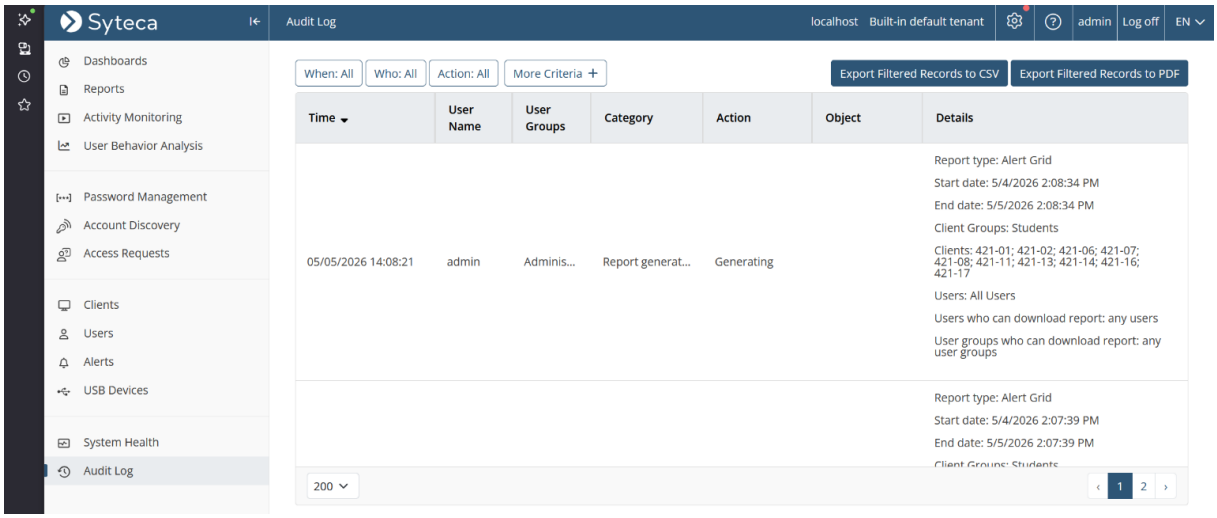

Рис. 3.34. Налаштування параметрів звітності

Для централізованого контролю дій користувачів Syteca забезпечує можливість перегляду статистики активності у вигляді графіків та діаграм. Це дозволяє швидко визначати аномальну поведінку користувачів (рис. 3.35).

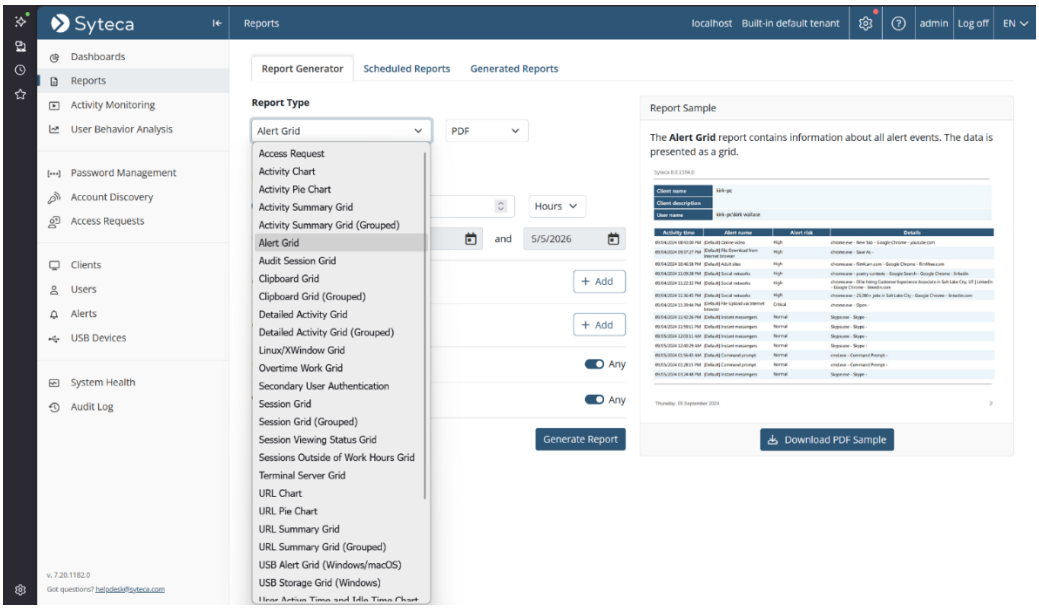

Рис. 3.35. Формування користувацького звіту в Syteca

Під час роботи із критичними системами особлива увага приділяється контролю дій адміністраторів та привілейованих користувачів. Система реєструє всі адміністративні операції та забезпечує їх подальший аналіз (рис. 3.36).

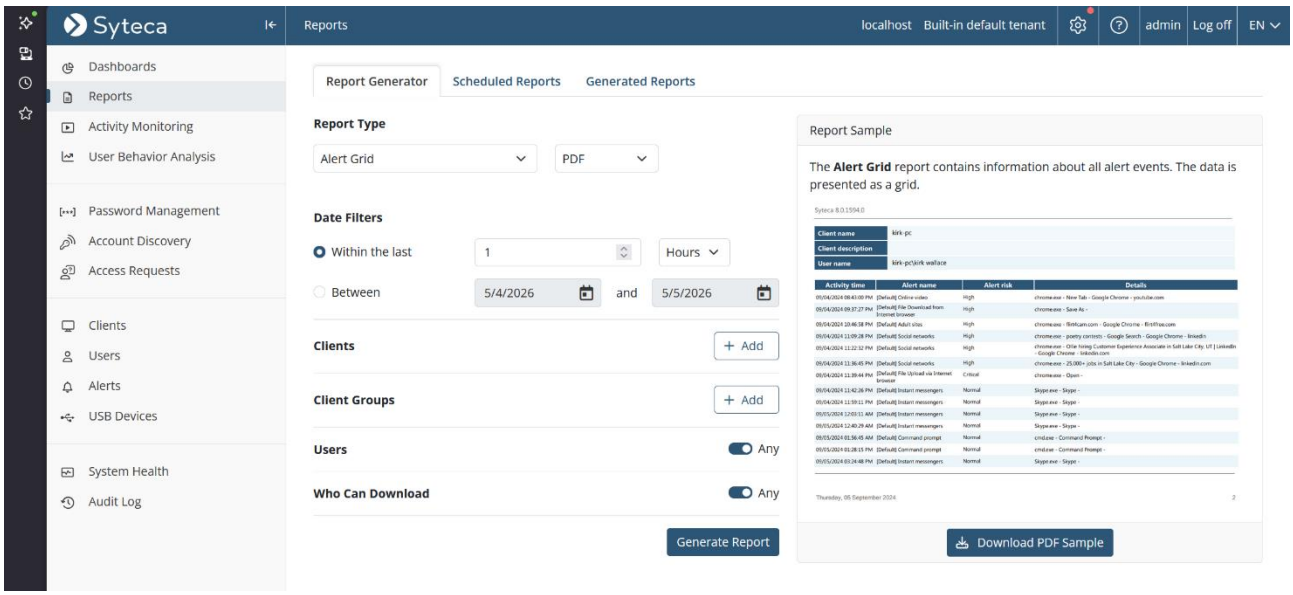

Рис. 3.36. Налаштування параметрів моніторингу користувачів

У разі необхідності результати аналізу можуть бути експортовані у зовнішні формати для подальшого використання або архівування. Це дозволяє формувати офіційну документацію щодо проведеного розслідування (рис. 3.37).

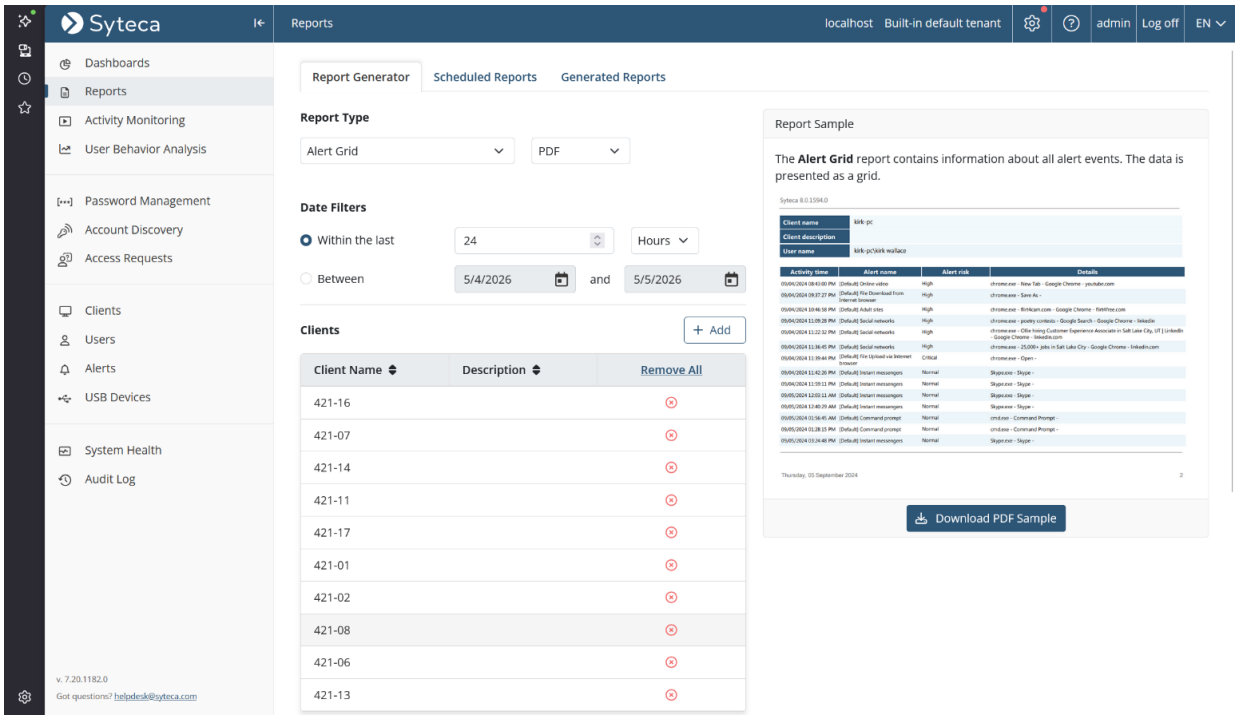

Рис. 3.37. Перегляд таблиці подій та інцидентів

Завершальним етапом є формування підсумкового звіту про інцидент кібербезпеки, у якому зазначаються причини виникнення інциденту, перелік зафіксованих подій, оцінка наслідків та рекомендації щодо підвищення рівня захисту інформаційної системи (рис. 3.38).

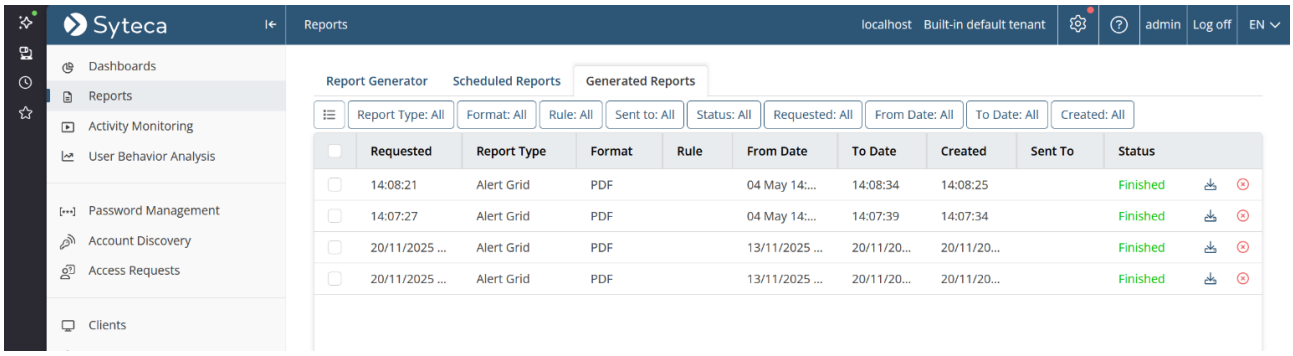

Рис. 3.38. Підсумковий журнал моніторингу подій у Syteca

Після завершення аналізу інциденту результати розслідування документуються. Отримані журнали подій, записи сесій та сформовані звіти використовуються для визначення причин інциденту, оцінки масштабу порушення та розробки заходів щодо недопущення подібних ситуацій у майбутньому.

Таким чином, використання платформи Syteca забезпечує комплексний підхід до проведення розслідувань інцидентів кібербезпеки, оскільки система поєднує функції моніторингу активності користувачів, запису сесій, контролю привілейованого доступу та автоматизованого формування звітів. Це дозволяє оперативно виявляти порушення політик безпеки, аналізувати дії користувачів та підвищувати рівень захисту інформаційної системи організації.

3.3 Рекомендації щодо застосування системи моніторингу та аналізу аномальної поведінки користувачів у корпоративних мережах на основі Syteca UAM

Важливу роль у корпоративних мережах відіграє контроль дій користувачів та своєчасне виявлення аномальної поведінки, яка може свідчити про внутрішні загрози або спроби несанкціонованого доступу до інформаційних ресурсів. Для вирішення таких завдань доцільно використовувати системи класу UAM (User Activity Monitoring), зокрема платформу Syteca, яка забезпечує моніторинг активності користувачів та аналіз подій безпеки [5].

Однією з основних рекомендацій щодо використання Syteca UAM є впровадження централізованого моніторингу всіх робочих станцій у корпоративній мережі. Це дозволяє фіксувати дії користувачів, контролювати запуск програм, доступ до файлів та використання зовнішніх носіїв інформації. Такий підхід забезпечує можливість швидкого виявлення підозрілих дій та оперативного реагування на інциденти кібербезпеки [5, 19].

Важливим елементом ефективної роботи системи є налаштування політик моніторингу відповідно до ролей користувачів та рівня їх доступу до

інформаційних ресурсів. Для працівників із привілейованими правами доступу рекомендується використовувати більш детальний контроль, включаючи запис сесій, журналювання дій та аналіз файлових операцій. Це дозволяє зменшити ризик витоку конфіденційної інформації та підвищити рівень захисту корпоративної мережі [5].

Також рекомендується використовувати механізми виявлення аномальної поведінки користувачів. Аналіз поведінкових моделей дозволяє визначати нетипові дії, наприклад вхід у систему в незвичний час, доступ до нетипових ресурсів, масове копіювання файлів або запуск невідомого програмного забезпечення. Використання таких механізмів допомагає своєчасно виявляти потенційні загрози та запобігати порушенням політик інформаційної безпеки [5, 20].

Для підвищення ефективності захисту рекомендується інтегрувати Syteca UAM із іншими засобами кібербезпеки, зокрема SIEM-системами, службами автентифікації та антивірусним програмним забезпеченням. Комплексний підхід до моніторингу та аналізу подій дозволяє підвищити ефективність розслідування інцидентів та забезпечити централізоване управління подіями безпеки [19, 20].

Крім технічних заходів, важливе значення має інформування працівників щодо правил інформаційної безпеки та політик моніторингу активності. Працівники повинні бути ознайомлені з правилами роботи з корпоративними ресурсами та відповідальністю за порушення вимог безпеки. Це сприяє зменшенню кількості внутрішніх інцидентів та підвищенню рівня захисту інформаційної системи організації [19].

Отже, використання Syteca UAM у корпоративних мережах забезпечує ефективний контроль дій користувачів, виявлення аномальної поведінки та своєчасне реагування на інциденти кібербезпеки. Реалізація наведених рекомендацій дозволяє підвищити рівень захисту інформаційних ресурсів організації та забезпечити стабільне функціонування корпоративної інформаційної інфраструктури .

Висновок до розділу 3

У третьому розділі бакалаврської роботи було розглянуто практичні аспекти розгортання, налаштування та використання системи моніторингу аномальної поведінки користувачів на базі Syteca. У процесі дослідження було проаналізовано основні етапи встановлення системи, налаштування параметрів моніторингу та організації контролю активності користувачів у корпоративній мережі.

Під час виконання роботи було встановлено, що система Syteca забезпечує ефективний моніторинг дій користувачів, контроль доступу до інформаційних ресурсів, запис сесій та аналіз подій безпеки. Використання платформи дозволяє своєчасно виявляти підозрілу активність, контролювати дії привілейованих користувачів та зменшувати ризики витоку конфіденційної інформації.

У підрозділі, присвяченому розслідуванню інцидентів кібербезпеки, було досліджено можливості Syteca щодо перегляду журналів подій, аналізу активності користувачів, запису сесій та формування звітів. Проведений аналіз показав, що використання системи дозволяє оперативно визначати причини інцидентів, відстежувати послідовність дій користувачів та підвищувати ефективність реагування на загрози інформаційній безпеці.

Також у роботі були розроблені рекомендації щодо застосування системи моніторингу та аналізу аномальної поведінки користувачів у корпоративних мережах. Було визначено, що ефективне використання Syteca потребує комплексного підходу, який включає налаштування політик моніторингу, контроль привілейованого доступу, використання механізмів виявлення аномальної поведінки та регулярний аналіз журналів подій.

Отже, результати проведеного дослідження підтверджують доцільність використання Syteca UAM для забезпечення інформаційної безпеки корпоративних мереж. Використання системи сприяє підвищенню рівня контролю за діями користувачів, своєчасному виявленню потенційних загроз та покращенню процесу розслідування інцидентів кібербезпеки.

ВИСНОВКИ

У кваліфікаційній роботі було досліджено особливості використання систем моніторингу та аналізу аномальної поведінки користувачів у корпоративних мережах на основі платформи Syteca UAM. У результаті проведеного дослідження досягнуто поставленої мети та виконано основні завдання роботи.

У першому розділі було проаналізовано теоретичні основи моніторингу поведінки користувачів у корпоративних мережах. Досліджено основні ризики аномальної поведінки користувачів, зокрема внутрішні загрози, компрометацію облікових записів, ескалацію привілеїв та латеральний рух у мережі. Визначено, що використання технологій UAM, UBA та UEBA дозволяє своєчасно виявляти підозрілу активність та підвищувати ефективність систем інформаційної безпеки. Також було проведено порівняльний аналіз сучасних систем моніторингу активності користувачів та встановлено їх основні переваги й недоліки.

У другому розділі досліджено архітектуру та функціональні можливості платформи Syteca UAM. Встановлено, що дана система забезпечує централізований моніторинг активності користувачів, контроль привілейованого доступу, аудит дій користувачів та можливість проведення розслідувань інцидентів кібербезпеки. Розглянуто основні методи виявлення аномалій, серед яких поведінковий аналіз, статистичні методи, правилозорієнтовані підходи та алгоритми машинного навчання. Також проаналізовано механізми управління привілейованим доступом (PAM), які дозволяють підвищити рівень захисту корпоративної інфраструктури та зменшити ризики несанкціонованого доступу.

У третьому розділі виконано практичне розгортання та налаштування системи Syteca UAM у тестовому середовищі. Було здійснено налаштування серверної частини, бази даних, вебінтерфейсу адміністратора, агентів моніторингу та політик контролю активності користувачів. Досліджено порядок проведення розслідувань інцидентів кібербезпеки за допомогою Syteca та

розроблено рекомендації щодо впровадження й використання системи в організаціях.

У результаті дослідження встановлено, що використання систем моніторингу активності користувачів та аналізу аномальної поведінки є важливим елементом сучасної системи інформаційної безпеки. Платформа Syteca UAM дозволяє ефективно контролювати дії користувачів, своєчасно виявляти потенційні загрози, проводити аудит привілейованих облікових записів та забезпечувати оперативне реагування на інциденти кібербезпеки.

Практичне значення отриманих результатів полягає у можливості використання розроблених рекомендацій для впровадження систем моніторингу активності користувачів у корпоративних мережах підприємств та організацій з метою підвищення рівня інформаційної безпеки й мінімізації ризиків кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. IBM. What is User and Entity Behavior Analytics (UEBA)? URL: https://www.ibm.com/think/topics/ueba (дата звернення: 04.05.2026).

2. Huawei. What is UEBA? URL: https://info.support.huawei.com/info-finder/encyclopedia/en/UEBA.html (дата звернення: 04.05.2026).

3. Microsoft. What is User and Entity Behavior Analytics? URL: https://www.microsoft.com/security/business/security-101/what-is-user-entity-behavior-analytics-ueba (дата звернення: 04.05.2026).

4. TechTarget. User Behavior Analytics (UBA). URL: https://www.techtarget.com/searchsecurity/definition/user-behavior-analytics-UBA (дата звернення: 04.05.2026).

5. EmpMonitor. UBA vs UAM: key differences and benefits. URL: https://empmonitor.com/blog/uba-vs-uam/ (дата звернення: 04.05.2026).

6. Teramind. Top user activity monitoring tools. URL: https://www.teramind.co/blog/top-user-activity-monitoring-tools/?utm_source (дата звернення: 04.05.2026).

7. Candoriq. Best user activity monitoring software tools. URL:https://www.candoriq.com/blog/best-user-activity-monitoring-software-tools?utm_source (дата звернення: 04.05.2026).

8. Splunk. Official website. URL: https://www.splunk.com/ (дата звернення: 04.05.2026 та 10.05.2026).

9. NordLayer. User activity monitoring explained. URL: https://nordlayer.com/learn/threat-management/user-activity-monitoring/?utm_source (дата звернення: 04.05.2026).

10. AM Integrator. Ekran System тепер називається Syteca. URL: https://amintegrator.com/ekransystem-teper-nazyvayetsya-syteca/ (дата звернення: 04.05.2026).

11. Kaspersky. UEBA rules in SIEM. URL: https://www.kaspersky.com/blog/ueba-rules-in-kaspersky-siem/54060/ (дата звернення: 04.05.2026).

12. Radware. UEBA Overview. URL: https://www.radware.com/cyberpedia/cloud-security/ueba/ (дата звернення: 04.05.2026).

13. Graylog. Anomaly Detection. URL: https://graylog.org/feature/anomaly-detection/ (дата звернення: 04.05.2026).

14. Microsoft Learn. Identify threats with UEBA in Microsoft Sentinel. URL: https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics (дата звернення: 04.05.2026).

15. OpenUBA. Platform Overview. URL: https://openuba.org/ (дата звернення: 04.05.2026).

16. IITD. Управління привілейованим доступом (PAM). URL: https://iitd.ua/pam-privileged-access-management/ (дата звернення: 06.05.2026).

17. Delo.ua. Що таке управління привілейованим доступом (PAM). URL: https://delo.ua/news-companies/shho-take-upravlinnya-privileiovanim-dostupom-privileged-access-management-pam-433405/ (дата звернення: 06.05.2026).

18. Quick Start Deployment Guide. Syteca Knowledge Base of End-User Documentation. URL: https://docs.syteca.com/view/quick-start-deployment-guide (дата звернення: 08.05.2026)

19. TimeCamp. What is User Activity Monitoring (UAM). URL: https://www.timecamp.com/blog/what-is-user-activity-monitoring-uam/?utm_source (дата звернення: 10.05.2026)

20. Lepide. What is User Activity Monitorin. URL: https://www.lepide.com/cyber-learning/what-is-user-activity-monitoring-uam/?utm_source (дата звернення: 10.05.2026)