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 АУДИТУ В МАЛИХ ТА СЕРЕДНІХ КОМПАНІЯХ З ОБМЕЖЕНИМИ РЕСУРСАМИ ДЛЯ ВПРОВАДЖЕННЯ СИСТЕМ БЕЗПЕКИ”

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

_____ Ярослав РУДНИЦЬКИЙ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Ярослав РУДНИЦЬКИЙ
Ім’я, ПРІЗВИЩЕ

Керівник: Діана Примаченко
Ім’я, ПРІЗВИЩЕ

Рецензент: _____
Ім’я, ПРІЗВИЩЕ

Київ 2025

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
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Рудницький Ярослав Русланович
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Система аудиту в малих та середніх компаніях з обмеженими ресурсами для впровадження систем безпеки”,
Керівник кваліфікаційної роботи Діана ПРИМАЧЕНКО,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “20” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека організацій,, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити проблеми впровадження системи аудиту в малих та середніх компаніях з обмеженими ресурсами.
4.2. Проаналізувати методи та інструменти оцінки ефективності аудиту та відповідності його міжнародним стандартам.
4.3. Розробити рекомендації щодо оптимізації процесів аудиту для малих та середніх компаній з урахуванням їхніх фінансових та технічних обмежень.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури щодо аудиту в малих і середніх компаніях.	29.03.2025	
3.	Дослідження міжнародних стандартів аудиту та їхніх вимог до систем безпеки.	08.04.2025	
4.	Аналіз існуючих методів аудиту в малих і середніх компаніях.	22.04.2025	
5.	Оцінка відповідності існуючих практик аудиту міжнародним стандартам та виявлення недоліків.	08.05.2025	
6.	Формування рекомендацій щодо оптимізації процесів аудиту для компаній з обмеженими ресурсами.	20.05.2025	
7.	Оформлення роботи.	22.05.2025	
8.	Оформлення презентації.	03.06.2025	
9.	Отримання рецензії на роботу.	03.06.2025	
10.	Захист в ЕК.	__.06.2025	

Здобувач вищої освіти _____ Ярослав РУДНИЦЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
(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 здобувач Рудницький Я.Р. 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 аудиту в малих та середніх компаніях з обмеженими ресурсами для впровадження систем безпеки"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач РУДНИЦЬКИЙ Ярослав у кваліфікаційній роботі проаналізував методи аудиту інформаційної безпеки в малих та середніх компаніях з обмеженими ресурсами, дослідив особливості впровадження систем безпеки в умовах фінансових, кадрових та технічних обмежень. У роботі сформульовано практичні рекомендації щодо оптимізації процесів аудиту та підвищення рівня кібербезпеки для підприємств малого та середнього бізнесу.

РУДНИЦЬКИЙ Ярослав продемонстрував глибоке розуміння проблеми дослідження, володіння теоретичними та практичними методами її вирішення, застосував науковий підхід у своїй роботі, а також проявив себе як організований і відповідальний виконавець. Результати його дослідження були апробовані на двох конференціях.

Все це дозволяє оцінити кваліфікаційну роботу здобувача РУДНИЦЬКОГО Ярослава на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою "Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Діана Примаченко
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Рудницький Я.Р. 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

здобувача вищої освіти РУДНИЦЬКИЙ Ярослав
на тему “Система аудиту в малих та середніх компаніях з обмеженими ресурсами для впровадження систем безпеки”

Актуальність. У сучасному бізнес-середовищі малі та середні компанії дедалі активніше інтегрують інформаційні технології у свої операційні процеси, що супроводжується зростанням вимог до забезпечення інформаційної безпеки. Відсутність належного аудиту створює ризики невідповідності законодавчим вимогам, витоку конфіденційної інформації, шахрайства та кібератак.

З огляду на це, дослідження проблематики організації аудиту інформаційної безпеки в умовах обмежених ресурсів, аналіз ефективності застосування сучасних інструментів моніторингу й оцінки ризиків, а також розробка практичних рекомендацій щодо оптимізації таких процесів є актуальним і важливим науково-практичним завданням.

Позитивні сторони.

1. У роботі досліджено особливості впровадження аудиту інформаційної безпеки в малих та середніх компаніях, розглянуто ефективність різних підходів до оцінки ризиків, а також сучасних інструментів аудиту, включаючи SIEM-системи, IDS/IPS-рішення та сканери вразливостей (OpenVAS).
2. Кваліфікаційна робота оформлена відповідно до вимог. Структура роботи логічна, виклад матеріалу послідовний, із чіткими висновками та рекомендаціями.
3. За результатами дослідження запропоновано конкретні рекомендації щодо оптимізації процесів аудиту інформаційної безпеки для малих та середніх підприємств, що дозволяє адаптувати стандартизовані підходи до реальних умов компаній з обмеженими ресурсами.

Недоліки.

Доцільно було б приділити більше уваги практичній апробації запропонованих рекомендацій у вигляді пілотного впровадження або кейс-стаді на прикладі реальної компанії, що дозволило б підтвердити ефективність запропонованого підходу в умовах реальної експлуатації.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент: _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню відповідності політик і процедур інформаційної безпеки в організаціях міжнародним вимогам, аналізу можливих невідповідностей та розробці рекомендацій щодо їх вдосконалення. Робота складається зі вступу, трьох розділів, що містять 34 рисунки, висновків і списку використаних джерел із 41 найменувань. Загальний обсяг роботи становить 67 аркушів, з яких 5 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є аналіз існуючих методів аудиту інформаційної безпеки, дослідження їх ефективності у малих і середніх компаніях та розробка рекомендацій щодо оптимізації процесу аудиту із використанням сучасних підходів і технологій.

Об'єктом дослідження є методи аудиту інформаційної безпеки та їх застосування у малих і середніх компаніях з обмеженими ресурсами.

Предмет дослідження – міжнародні стандарти, технології та підходи до проведення аудиту інформаційної безпеки, оптимізація процесів аудиту в умовах

Методи дослідження. У роботі використано методи аналізу, синтезу, моделювання, порівняння та системного підходу. Проведено огляд нормативних документів і міжнародних стандартів (ISO/IEC 27001, COBIT, NIST SP 800-53) для визначення їхнього значення в аудиті інформаційної безпеки. Досліджено підходи до оцінки ризиків і управління безпекою з використанням автоматизованих засобів. Розроблено модель аудиту для компаній з обмеженими ресурсами та проаналізовано ефективність використання SIEM-систем і інструментів виявлення вразливостей, зокрема OpenVAS.

Галузь застосування. Запропоновані підходи можуть бути використані в галузі кібербезпеки під час реалізації заходів аудиту інформаційної безпеки в організаціях різного масштабу.

Ключові слова: АУДИТ, ІНФОРМАЦІЙНА БЕЗПЕКА, ISO/IEC 27001, COBIT, NIST SP 800-53, OPENVAS, SIEM, УПРАВЛІННЯ РИЗИКАМИ

ABSTRACT

This qualification paper is dedicated to the study of the compliance of information security policies and procedures in organizations with international requirements, the analysis of potential inconsistencies, and the development of recommendations for their improvement. The paper consists of an introduction, three chapters containing 34 figures, conclusions, and a list of 41 references. The total volume of the work is 67 pages, of which 5 pages are dedicated to the list of abbreviations and references.

The aim of the study is to analyze existing methods of information security auditing, to assess their effectiveness in small and medium-sized enterprises (SMEs), and to develop recommendations for optimizing the audit process using modern approaches and technologies.

The object of the research is the methods of information security auditing and their application in small and medium-sized companies with limited resources.

The subject of the research is international standards, technologies, and approaches to conducting information security audits, as well as the optimization of audit processes under constrained conditions.

Research methods: The methods of analysis, synthesis, modeling, comparison and systematic approach are used in the study. A review of regulatory documents and international standards (ISO/IEC 27001, COBIT, NIST SP 800-53) was conducted to determine their importance in information security audits. Approaches to risk assessment and security management using automated tools are investigated. An audit model for companies with limited resources is developed and the effectiveness of using SIEM systems and vulnerability detection tools, in particular OpenVAS, is analyzed.

Field of application. The proposed approaches can be used in the field of cybersecurity in the implementation of information security audit measures in organizations of various sizes.

Keywords: AUDIT, INFORMATION SECURITY, ISO/IEC 27001, COBIT, NIST SP 800-53, OPENVAS, SIEM, RISK MANAGEMENT

ЗМІСТ

ВСТУП 10

РОЗДІЛ 1 ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА АУДИТУ 12

1.1 Основні поняття інформаційної безпеки та аудит СУІБ 12

1.2 Виклики для малих та середніх компаній при впровадженні систем безпеки 14

1.3 Методи оцінки рівня безпеки та управління ризиками 16

1.4 Огляд міжнародних стандартів (ISO/IEC 27001, ISO/IEC 15408, NIST SP 800-53) 19

Висновки до розділу 1 22

РОЗДІЛ 2 МЕТОДИ, АНАЛІЗ ТА ІНСТРУМЕНТИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 23

2.1 Планування та підготовка аудиту в умовах обмежених ресурсів 23

2.2 Інструменти автоматизованої оцінки загроз (SIEM, IDS/IPS, OpenVAS) 25

2.3 Методики аутентифікації та управління доступом (MFA, IAM, PKI) 27

Висновки до розділу 2 30

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ АУДИТУ ТА ПЕРСПЕКТИВИ РОЗВИТКУ 32

3.1 Аутсорсингові моделі та MSSP як шлях оптимізації 32

3.2 Ефективне використання Open-source рішень для аудиту 37

3.3 Побудова безпечної інфраструктури на основі SIEM-моніторингу 41

3.4 Перспективи розвитку аудитів безпеки в малих і середніх компаніях 60

ВИСНОВКИ 62

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 64

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна Безпека
СУІБ	Система Управління Інформаційною Безпекою
MFA	Multi-Factor Authentication
IAM	Identity and Access Management
PKI	Public Key Infrastructure
SIEM	Security Information and Event Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
CA	Certificate Authority
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
GDPR	General Data Protection Regulation
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
EAL	Evaluation Assurance Level
OpenVAS	Open Vulnerability Assessment System

ВСТУП

Актуальність дослідження. У сучасному цифровому світі аудиторська діяльність відіграє ключову роль у забезпеченні прозорості, надійності фінансової звітності та мінімізації ризиків для бізнесу. Проте малі та середні підприємства часто стикаються з обмеженими фінансовими, технічними та людськими ресурсами, що ускладнює впровадження ефективних систем безпеки та контролю. Відсутність належного аудиту може призвести до фінансових порушень, шахрайства, витоку конфіденційних даних і недотримання регуляторних вимог, що створює додаткові ризики для діяльності компаній. Багато підприємств малого та середнього бізнесу не мають можливості наймати висококваліфікованих аудиторів або впроваджувати дорогі системи моніторингу й аналізу ризиків, що ускладнює забезпечення відповідності міжнародним стандартам.

Актуальність дослідження системи аудиту в таких компаніях зумовлена необхідністю розробки ефективних, адаптивних і економічно виправданих підходів до контролю та управління ризиками. Дослідження спрямоване на виявлення оптимальних методів аудиту, які можуть бути інтегровані в діяльність малих і середніх підприємств, забезпечуючи надійність фінансових операцій, відповідність законодавчим вимогам та підвищення рівня довіри з боку клієнтів і партнерів.

З огляду на це, дослідження проблем та перспектив розвитку системи аудиту в малих і середніх компаніях є важливим науково-практичним завданням, що сприятиме підвищенню ефективності управління та мінімізації ризиків у сучасному бізнес-середовищі. З огляду на зазначене дослідження відповідності політик і процедур інформаційної безпеки в організаціях є актуальним науковим завданням.

Мета роботи аналіз існуючих методів аудиту інформаційної безпеки, дослідження їх ефективності у малих і середніх компаніях та розробка рекомендацій щодо оптимізації процесу аудиту із використанням сучасних

підходів і технологій.

Об'єкт дослідження **–** методи аудиту інформаційної безпеки та їх застосування у малих і середніх компаніях з обмеженими ресурсами.

Предмет дослідження – міжнародні стандарти, технології та підходи до проведення аудиту інформаційної безпеки, оптимізація процесів аудиту в умовах обмежених ресурсів.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Дослідити основні вимоги міжнародних стандартів (ISO/IEC 27001, NIST, GDPR тощо) до політик і процедур інформаційної безпеки.
2. Виявити можливі невідповідності між чинними політиками та процедурами інформаційної безпеки в організаціях і міжнародними вимогами.
3. Виявити можливі невідповідності між чинними політиками та процедурами інформаційної безпеки в організаціях і міжнародними вимогами.
4. Розробити рекомендації щодо вдосконалення політик і процедур інформаційної безпеки для забезпечення їх відповідності міжнародним стандартам, оптимізувавши процеси аудиту для компаній з обмеженими ресурсами.

Методи дослідження. Для вирішення наукового завдання щодо вдосконалення системи аудиту в малих та середніх компаніях з обмеженими ресурсами для впровадження систем безпеки використано комплексний підхід, що включає різні методи дослідження.

Практичне значення одержаних результатів полягає в тому, що їх застосування дозволяє малим та середнім компаніям оптимізувати аудиторські процеси відповідно до міжнародних стандартів, навіть за умов обмежених ресурсів. Це сприяє підвищенню рівня фінансової прозорості, що, у свою чергу, зміцнює довіру клієнтів, інвесторів і партнерів.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

РОЗДІЛ 1 ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА АУДИТУ

1.1 Основні поняття інформаційної безпеки та аудит СУІБ

Інформаційна безпека (ІБ) – це стан захищеності інформації, при якому забезпечується її конфіденційність, цілісність і доступність. Ці три основні атрибути є фундаментом будь-якої системи захисту інформації.

У контексті організаційної діяльності інформаційна безпека охоплює не лише захист даних, але й відповідність законодавчим та нормативним вимогам, мінімізацію ризиків для бізнесу, захист репутації та забезпечення безперервності роботи компанії.

З метою системного підходу до управління інформаційною безпекою у компаніях впроваджуються Системи управління інформаційною безпекою (СУІБ).

СУІБ (англ. ISMS – Information Security Management System) – це сукупність політик, процедур, технічних та організаційних заходів, спрямованих на захист інформаційних активів організації. Основою для побудови СУІБ є міжнародний стандарт ISO/IEC 27001, який встановлює вимоги до створення, впровадження, підтримки та постійного покращення системи управління інформаційною безпекою [1].

СУІБ дозволяє організації:

– визначити ризики, що загрожують інформаційним активам;

– впровадити контрольні заходи для зниження цих ризиків до прийнятного рівня;

– забезпечити дотримання вимог законодавства та нормативних актів;

– зміцнити довіру клієнтів, партнерів та інвесторів.

Важливою частиною функціонування СУІБ є проведення аудиту інформаційної безпеки – процесу перевірки відповідності існуючих заходів стандартам, політикам та нормативним вимогам. Аудит дозволяє виявити

вразливі місця, оцінити ефективність поточних заходів безпеки та розробити план їх удосконалення.

Аудит інформаційної безпеки (ІБ) – це систематичний процес оцінювання, перевірки та аналізу відповідності політик, процедур, технічних рішень та організаційних заходів у сфері захисту інформації встановленим стандартам, нормативним вимогам та внутрішнім політикам організації. Його основна мета полягає у виявленні потенційних вразливостей, оцінці ризиків і ефективності впроваджених заходів безпеки, а також формуванні рекомендацій щодо їхнього вдосконалення [2].

У сучасному цифровому середовищі, де інформаційні системи є ключовим елементом функціонування бізнесу, держа́вних установ та критичної інфраструктури, аудит ІБ відіграє стратегічно важливу роль. Він дозволяє забезпечити не лише технічну захищеність ІТ-систем, а й відповідність чинним законодавчим нормам, міжнародним стандартам (зокрема ISO/IEC 27001, NIST SP 800-53, GDPR) та вимогам галузевих регуляторів.

Аудит інформаційної безпеки охоплює коло аспектів: перевірку політик доступу до інформації, управління правами користувачів, конфігурацій систем, журналів подій, процесів резервного копіювання, виявлення інцидентів безпеки та заходів реагування на них. Особлива увага приділяється процедурі управління ризиками – ідентифікації активів, загроз, вразливостей, а також оцінці потенційного впливу інцидентів і вибору відповідних заходів контролю [3].

Роль аудиту полягає не лише в діагностиці поточного стану безпеки, але й у забезпеченні безперервного покращення захисних механізмів. Завдяки результатам аудиту організація отримує об’єктивну картину сильних і слабких сторін своєї системи захисту, що дозволяє формувати довгострокову стратегію безпеки, розставляти пріоритети в інвестуванні в захист, уникати надлишкових витрат і мінімізувати ризики.

Окреме значення аудит ІБ має в контексті побудови довіри з боку партнерів, клієнтів та інвесторів. Прозорість процесів захисту інформації, документальне підтвердження відповідності стандартам та проходження

регулярних перевірок є свідченням зрілості компанії як надійного суб'єкта економічної діяльності.

Для малих і середніх підприємств, які часто мають обмежені ресурси, аудит є ще більш критично важливим інструментом. Саме через його проведення ці організації можуть виявити першочергові напрями для вдосконалення системи безпеки, обґрунтувати інвестиції в ІТ та ефективно управляти ризиками без необхідності повноцінного впровадження дорогих рішень.

1.2 Виклики для малих та середніх компаній при впровадженні систем безпеки

Малі та середні підприємства (МСП) стикаються з низкою обмежень, що суттєво впливають на можливості впровадження повноцінної та ефективної системи інформаційної безпеки. Ці обмеження можна умовно поділити на фінансові, кадрові та технічні.

Фінансові обмеження, МСП не мають достатнього бюджету для впровадження дорогих засобів захисту інформації, таких як комерційні SIEM-системи, складні засоби багатофакторної автентифікації або хмарні рішення з автоматичним виявленням загроз. Крім того, регулярний аудит, сертифікація за стандартами ISO/IEC 27001 чи NIST потребують значних витрат на консалтинг, навчання персоналу та модернізацію ІТ-інфраструктури. Часто керівництво таких компаній сприймає витрати на безпеку як другорядні в умовах конкурентної боротьби за виживання на ринку [4].

Кадрові обмеження, малі компанії рідко мають у своєму штаті кваліфікованих фахівців з інформаційної безпеки або навіть системних адміністраторів із відповідним досвідом. Без фахівців складно впроваджувати сучасні засоби захисту, аналізувати ризики, проводити аудит чи реагувати на інциденти. Внаслідок цього технічне обслуговування ІБ часто перекладається на непрофільний персонал або зовнішніх підрядників, що знижує рівень контролю та оперативності реагування.

Технічні обмеження, IT-інфраструктура в МСП часто є застарілою або хаотичною, з мінімальними засобами моніторингу, контролю доступу та резервного копіювання. У багатьох випадках використовуються безкоштовні, обмежені за функціональністю рішення, які не підтримують сучасні стандарти безпеки. Також часто бракує інструментів для збору логів, аналізу подій, виявлення аномалій та інших компонентів ефективної системи захисту.

Більшість міжнародних стандартів у сфері інформаційної безпеки (зокрема ISO/IEC 27001, NIST SP 800-53, PCI DSS) орієнтовані на великі корпорації або організації, які мають розгалужені IT-структури, відділи безпеки та достатній бюджет на підтримку ІБ. Такі стандарти передбачають велику кількість контрольних заходів, складну документацію, регулярний аудит, політики навчання персоналу та сертифікацію. Для більшості МСП це створює надмірне адміністративне та фінансове навантаження [5].

Стандартні фреймворки часто потребують великої кількості ресурсів для впровадження і супроводу, що перевищує можливості малих компаній. Наприклад, повноцінне впровадження ISO/IEC 27001 передбачає створення спеціальної політики безпеки, впровадження щонайменше десятків контрольних заходів, а також проведення регулярних внутрішніх та зовнішніх аудитів. Для більшості МСП це недосяжно без залучення зовнішніх консультантів [6].

Стандарти не завжди враховують специфіку малого бізнесу. Наприклад, вони можуть містити вимоги, які мають сенс у середовищі з великою кількістю працівників, кількома філіями або складними IT-системами, але втрачають свою доцільність у невеликій фірмі з кількома десятками співробітників і простими IT-ресурсами.

Складність впровадження стандартів може призвести до формального дотримання вимог без реального покращення рівня захисту. У прагненні виконати вимоги "на папері", компанії можуть нехтувати реальними ризиками, що суперечить самому змісту інформаційної безпеки.

1.3 Методи оцінки рівня безпеки та управління ризиками

Оцінка рівня інформаційної безпеки в будь-якій організації неможлива без належного аналізу ризиків. Управління ризиками є фундаментальним компонентом системи інформаційної безпеки та відіграє ключову роль у прийнятті рішень щодо пріоритетності захисних заходів, розподілу ресурсів та вибору відповідних технологічних рішень.

Ризик в контексті інформаційної безпеки визначається як імовірність реалізації загрози, що призведе до порушення конфіденційності, цілісності або доступності інформації. Відповідно, аналіз ризиків передбачає ідентифікацію активів, виявлення загроз, оцінку вразливостей, а також визначення ймовірності настання інциденту та потенційних наслідків.

Існує кілька загальноприйнятих підходів до аналізу ризиків, які можуть бути адаптовані до потреб малих і середніх компаній:

1. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Методика OCTAVE була розроблена SEI (Software Engineering Institute) і є одним з найвідоміших підходів до аналізу ризиків у сфері інформаційної безпеки. Основна ідея OCTAVE полягає в тому, що самі співробітники організації – найкращі експерти у виявленні своїх слабких місць. Тому OCTAVE орієнтована на самооцінювання за допомогою спеціально підготовлених анкет, робочих сесій та аналізу організаційного контексту [7].

Ключові характеристики OCTAVE:

– Фокус на організаційних процесах, а не лише технічних аспектах.

– Активна участь користувачів і менеджменту.

– Можливість застосування в організаціях будь-якого розміру, що робить методику зручною для МСП.

– Включає в себе три фази: ідентифікація активів та загроз, оцінка вразливостей, розробка стратегії управління ризиками.

2. ISO 31000:2018 – Управління ризиками

Міжнародний стандарт ISO 31000 пропонує універсальну рамку для управління будь-якими типами ризиків, включно з інформаційними. Він базується на принципах інтеграції, структури, адаптивності та постійного вдосконалення [7].

Стандарт ISO 31000 визначає наступні основні етапи:

– Встановлення контексту (врахування бізнес-середовища, потреб, зацікавлених сторін);

– Ідентифікація ризиків (які загрози можуть вплинути на досягнення цілей);

– Аналіз ризиків (визначення ймовірності та наслідків);

– Оцінка ризиків (порівняння з критеріями прийнятності);

– Обробка ризиків (вибір варіантів: уникнення, зменшення, передача, прийняття);

– Моніторинг і перегляд результатів;

– Інформаційна взаємодія з усіма сторонами.

Перевагою ISO 31000 є його гнучкість: він може бути масштабований та адаптований до потреб як великих, так і малих організацій.

3. FAIR (Factor Analysis of Information Risk)

FAIR – це модель кількісного аналізу ризиків, що дозволяє перетворити якісні оцінки на числові значення. Основна ідея – використовувати точні метрики для обчислення грошових втрат, що дозволяє приймати обґрунтовані управлінські рішення. Хоча методика складніша у впровадженні, її результати більш точні і бізнес-орієнтовані. Для МСП її застосування можливе в спрощеному вигляді або через адаптовані інструменти [8].

4. CRAMM (CCTA Risk Analysis and Management Method)

Методика CRAMM розроблена у Великобританії і базується на формалізованому підході до аналізу інформаційних активів, загроз і вразливостей. Вона включає в себе засоби оцінки ризиків та генерацію рекомендацій щодо відповідних контрзаходів. Хоча CRAMM традиційно

застосовується в держсекторі, її адаптовані версії можуть бути корисними і для МСП [8].

Управління ризиками є необхідною складовою системи інформаційної безпеки, і правильний вибір методики залежить від специфіки компанії, рівня ресурсного забезпечення та складності IT-інфраструктури. Для малих та середніх компаній доцільним є використання гнучких, адаптивних підходів, які не вимагають надмірних інвестицій і дозволяють отримати практичні результати – зокрема, OCTAVE та ISO 31000.

Завдяки застосуванню таких методик навіть компанії з обмеженими ресурсами можуть сформувати ефективну стратегію управління інформаційними ризиками, що підвищує їхню кіберстійкість, мінімізує потенційні збитки та сприяє довгостроковій стабільності бізнесу.

Для глибшого розуміння сутності ризику в інформаційній безпеці доцільно візуалізувати ключові компоненти, які формують цей показник. Ризик є результатом взаємодії кількох елементів: активів, що потребують захисту, потенційних загроз, які можуть реалізуватись через існуючі вразливості, а також ймовірності настання інциденту і можливих негативних наслідків. Такий підхід дозволяє не лише якісно описати ситуацію, а й кількісно оцінити ризик для прийняття обґрунтованих управлінських рішень. На рис. 1.1 представлено базову структуру компонентів ризику в контексті інформаційної безпеки.

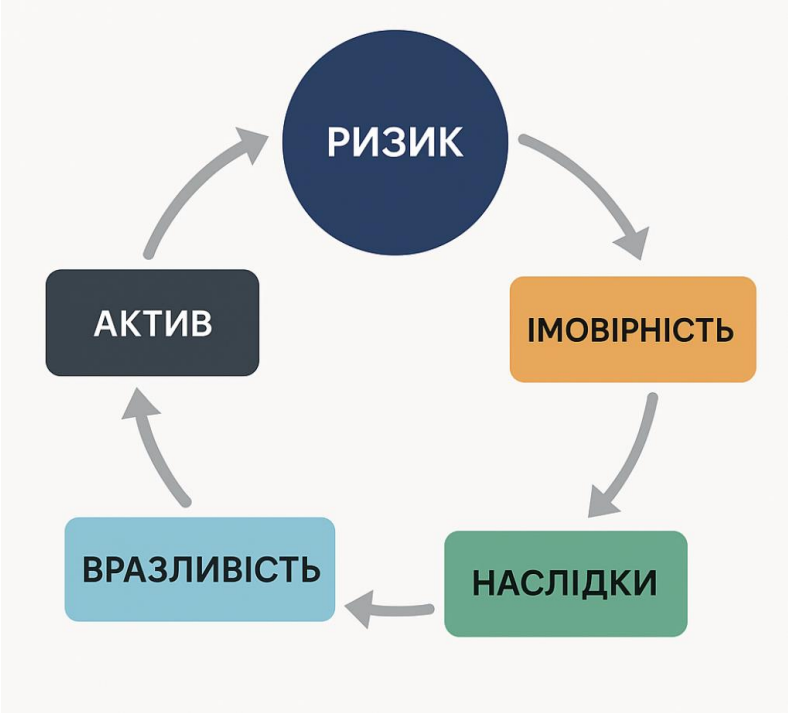

Рис. 1.1. Компоненти ризику в інформаційній безпеці

1.4 Огляд міжнародних стандартів (ISO/IEC 27001, ISO/IEC 15408, NIST SP 800-53)

Міжнародні стандарти у сфері інформаційної безпеки відіграють ключову роль у побудові надійних систем захисту в організаціях різного масштабу. Вони встановлюють вимоги до політик, процедур, технічних засобів та організаційної структури безпеки, забезпечуючи узгодженість, контроль і можливість об'єктивного аудиту. У цьому підрозділі розглянуто три найпоширеніші стандарти, які мають практичне значення для малих і середніх компаній.

ISO/IEC 27001 є найбільш визнаним і широко застосовуваним міжнародним стандартом у сфері інформаційної безпеки. Він визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Головною метою стандарту є забезпечення конфіденційності, цілісності та доступності інформації шляхом управління ризиками (рис. 1.2).

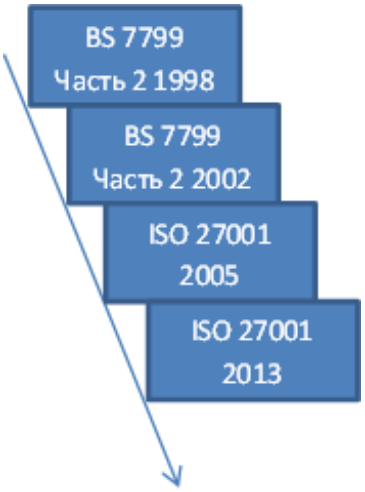

Рис. 1.2. Розвиток стандарту ISO/IEC 27001

Ключові особливості:

– впровадження політик і процедур безпеки;
– оцінка та обробка ризиків;
– регулярні внутрішні та зовнішні аудити;
– можливість сертифікації організації.

ISO/IEC 27001 особливо корисний для компаній, які прагнуть підвищити рівень довіри з боку клієнтів та партнерів, однак його повне впровадження потребує ресурсів, що може бути складно для МСП.

ISO/IEC 15408 – Common Criteria (Загальні критерії оцінки IT-продуктів) – цей стандарт зосереджений на оцінці надійності IT-продуктів і систем. ISO/IEC 15408 визначає так звані "загальні критерії", за якими здійснюється оцінка безпеки програмного забезпечення, апаратного забезпечення або IT-систем (рис. 1.3).

Рис. 1.3. Логотип стандарту ISO/IEC 15408

Основна мета стандарту – надати впевненість у тому, що продукт виконує заявлені функції безпеки та може бути довіреним у певному контексті.

Рівні оцінки (Evaluation Assurance Levels – EAL) коливаються від базового до високого ступеня впевненості (EAL1–EAL7).

Цей стандарт переважно використовується в державному секторі або серед великих підприємств, однак розуміння його принципів допомагає МСП обирати сертифіковані ІТ-рішення, що підвищують загальний рівень безпеки.

NIST SP 800-53 – контрольні заходи для систем безпеки, розроблений Національним інститутом стандартів і технологій США (NIST), містить каталог контрольних заходів інформаційної безпеки для систем, які обробляють, зберігають або передають інформацію [9]. Контроли класифікуються за функціями: захист доступу, аудиту, ідентифікації, моніторингу, криптографії (рис. 1.4).

Рис. 1.4. Етапи аналізу ризиків відповідно до підходу NIST SP 800-53

Переваги стандарту:

- універсальність і деталізація;
- можливість адаптації до будь-якої організації;
- основа для побудови політик безпеки.

Хоча NIST SP 800-53 призначений насамперед для державних структур США, він часто використовується як довідкова модель для корпоративної ІБ, зокрема для формування політик, аудитних чек-листів та планів реагування на інциденти.

Висновки до розділу 1

Розглянуто теоретичні засади інформаційної безпеки, поняття аудиту та його роль у забезпеченні належного рівня захисту інформаційних активів. Особливу увагу приділено системам управління інформаційною безпекою (СУІБ), які є основою для реалізації системного підходу до забезпечення конфіденційності, цілісності та доступності інформації в організації.

Проаналізовано специфічні виклики, з якими стикаються малі та середні компанії при впровадженні систем безпеки. До них відносяться обмежені фінансові, кадрові та технічні ресурси, які значною мірою ускладнюють реалізацію повноцінних моделей управління ризиками та відповідності міжнародним стандартам. Це обґрунтовує необхідність адаптації існуючих підходів до потреб МСП.

Вивчено ключові методи аналізу та оцінки ризиків, серед яких особливої уваги заслуговують моделі OCTAVE, ISO 31000, FAIR та CRAMM. Кожен із цих підходів має свої переваги та сфери застосування, проте саме OCTAVE та ISO 31000 найкраще відповідають можливостям і реаліям малих організацій завдяки гнучкості та адаптивності.

Розглянуто міжнародні стандарти у сфері інформаційної безпеки, такі як ISO/IEC 27001, ISO/IEC 15408 та NIST SP 800-53. Вони формують нормативну основу для побудови ефективної системи безпеки, однак потребують глибокого аналізу й адаптації перед впровадженням у малих компаніях.

РОЗДІЛ 2 МЕТОДИ, АНАЛІЗ ТА ІНСТРУМЕНТИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Планування та підготовка аудиту в умовах обмежених ресурсів

У малих та середніх компаніях проведення аудиту інформаційної безпеки стикається з низкою обмежень, серед яких найсуттєвішими є брак фінансових ресурсів, відсутність кваліфікованих спеціалістів, обмежений доступ до дорогих інструментів автоматизації, а також брак часу. Тому ефективне планування аудиту в таких умовах має базуватися на раціональному використанні наявних ресурсів, простих процедурах та пріоритетності завдань [20].

Одним із перших кроків у процесі є розробка реалістичного та адаптивного плану аудиту, що враховує обмеження організації, а також її цілі й ризики. Такий план повинен включати:

– визначення мети аудиту (наприклад, перевірка відповідності вимогам ISO/IEC 27001, оцінка вразливостей, тестування внутрішніх політик безпеки) [10];

– визначення обсягу (обмеження аудиту лише до критичних підрозділів або систем, які зберігають або обробляють чутливу інформацію);

– встановлення чітких термінів та етапів (етапи підготовки, збору даних, оцінки, звітування);

– визначення відповідальних осіб за кожен етап;

– підбір інструментів і методів, які не потребують значних фінансових витрат (наприклад, використання open-source програмного забезпечення для сканування вразливостей, журналювання або SIEM-функцій).

Центральним елементом планування є визначення критичних інформаційних активів, тобто тих ресурсів, втрата, модифікація або розголошення яких можуть призвести до значних бізнес-збитків. Ідентифікація активів може проводитись шляхом анкетування, інтерв’ювання співробітників, вивчення бізнес-процесів або аналізу поточної документації.

До типових критичних активів належать:

– персональні та фінансові дані клієнтів;
– ключові сервери й бази даних;
– облікові записи з підвищеними правами;
– мережеві пристрої та системи резервного копіювання;
– власницьке програмне забезпечення або інтелектуальна власність компанії.

Після визначення активів доцільно скласти чек-листи, які допоможуть стандартизувати процес аудиту й уникнути пропусків. Чек-листи можуть включати перевірку:

– наявності політик доступу;
– налаштування прав користувачів;
– протоколювання подій безпеки;
– використання оновлень і патчів;
– фізичного захисту обладнання;
– резервного копіювання та його тестування;
– наявності планів реагування на інциденти.

Чек-листи не тільки спрощують процедуру аудиту, але й дозволяють долучити до процесу непрофільних працівників, забезпечуючи контроль на базовому рівні навіть без глибоких технічних знань.

Ефективне планування аудиту в умовах обмежених ресурсів базується на чіткій пріоритезації, спрощеній процедурі аналізу ризиків та використанні структурованих шаблонів, таких як чек-листи. Це дозволяє компаніям досягати базового рівня інформаційної безпеки без значних інвестицій та з мінімальними операційними витратами.

2.2 Інструменти автоматизованої оцінки загроз (SIEM, IDS/IPS, OpenVAS)

Сучасна практика аудиту інформаційної безпеки передбачає використання спеціалізованих інструментів для виявлення загроз, аналізу подій і оцінювання вразливостей. Для малих та середніх компаній із обмеженими ресурсами важливо правильно підібрати комбінацію рішень, які забезпечують максимальну ефективність при мінімальних витратах. До ключових інструментів, що використовуються в процесі аудиту та оцінки загроз, належать SIEM-системи, IDS/IPS-рішення та сканери вразливостей, зокрема OpenVAS [11].

SIEM (Security Information and Event Management) – системи є ядром сучасної аналітики подій безпеки. Вони об'єднують функції збору, зберігання, аналізу та кореляції подій з різних джерел: серверів, мережевих пристроїв, систем безпеки, прикладного програмного забезпечення.

Основні функції SIEM:

- централізований збір логів;
- аналіз і виявлення підозрілих подій;
- сповіщення про інциденти;
- створення звітності для аудиту;
- підтримка відповідності стандартам (ISO 27001, GDPR тощо).

Приклади SIEM-рішень, придатних для МСП:

- Wazuh (з відкритим кодом);
- AlienVault OSSIM;
- Graylog [19].

SIEM-системи особливо корисні для довготривалого моніторингу та розслідування інцидентів, однак їх впровадження вимагає попередньої підготовки та базових навичок аналізу логів.

Системи виявлення вторгнень (IDS) та запобігання вторгненням (IPS) відіграють важливу роль у виявленні спроб несанкціонованого доступу або

порушень політик безпеки. IDS лише виявляє загрозу, тоді як IPS може автоматично блокувати її.

Основні функції IDS/IPS:

– аналіз трафіку на наявність сигнатур атак;
– виявлення аномалій у мережевій поведінці;
– журналювання подій і сповіщення адміністратора;
– блокування шкідливого трафіку (у випадку IPS).

Поширені безкоштовні рішення:

– Snort – IDS з відкритим кодом;
– Suricata – потужна IDS/IPS з підтримкою високошвидкісного аналізу трафіку;
– Zeek – гнучка IDS, орієнтована на поведінковий аналіз.

IDS/IPS системи ефективні при активному мережевому моніторингу та можуть бути інтегровані в SIEM-рішення для розширеного аналізу.

OpenVAS є о інструментом для автоматизованого сканування вразливостей. Це open-source рішення, що дозволяє проводити аудит безпеки систем та виявляти слабкі місця на серверах, мережах або окремих пристроях.

Основні функції OpenVAS:

– виявлення відомих вразливостей у ПЗ та ОС;
– створення детальних звітів із рекомендаціями;
– планування періодичних перевірок;
– формування рейтингу ризику для кожного об’єкта.

Перевага OpenVAS полягає у високій точності виявлення й активній підтримці спільнотою. Інструмент легко інтегрується з інтерфейсами керування, такими як Greenbone Security Assistant, що робить його зручним у використанні навіть для непрофесіоналів. В табл. 2.1 наведена порівняльна характеристика та обґрунтування вибору.

Таблиця 2.1

Порівняльна характеристика та обґрунтування вибору

Інструмент	Призначення	Тип	Основна перевага	Придатність для МСП
SIEM (Wazuh, OSSIM)	Збір і аналіз логів	Аналітика	Централізований моніторинг подій	Висока (при належній конфігурації)
IDS/IPS (Snort, Suricata)	Виявлення і запобігання вторгнень	Мережева безпека	Реагування в реальному часі	Висока (при правильному налаштуванні)
OpenVAS	Сканування вразливостей	Оцінка ризиків	Глибокий аналіз стану систем	Висока (простота інтеграції)

Для малих та середніх компаній найкращим підходом є поєднання цих трьох інструментів у єдиній системі моніторингу. Наприклад, Snort може виявляти мережеві атаки, результати яких обробляє SIEM (Wazuh), а OpenVAS періодично перевіряє системи на вразливості. Таке комплексне рішення забезпечує баланс між глибиною захисту та ресурсною економічністю [12].

2.3 Методики аутентифікації та управління доступом (MFA, IAM, PKI)

Захист доступу до інформаційних ресурсів є одним із ключових аспектів забезпечення інформаційної безпеки в будь-якій організації. Аутентифікація користувачів та управління доступом дозволяють обмежити можливість несанкціонованого доступу до критичних активів, зменшити ризики витоку даних, внутрішніх загроз та кібератак. Найбільш поширеними сучасними методиками в цій сфері є багатофакторна аутентифікація (MFA), системи управління ідентичностями (IAM) та інфраструктура відкритих ключів (PKI) [13].

MFA (Multi-Factor Authentication) – це метод перевірки особи користувача шляхом використання двох або більше незалежних факторів:

– Щось, що користувач знає (пароль або PIN);

– Щось, що користувач має (смартфон, токен, смарт-карта);

– Щось, що користувач є (біометричні дані: відбиток пальця, розпізнавання обличчя) [15].

MFA суттєво підвищує рівень безпеки, оскільки компрометація одного фактора (наприклад, пароля) не дозволяє отримати повний доступ без решти компонентів.

Впровадження в МСП:

Сучасні хмарні сервіси (Google Workspace, Microsoft 365) вже мають вбудовану підтримку MFA. Для локальних систем можна використовувати безкоштовні рішення, наприклад Authy, FreeOTP, Google Authenticator, або налаштувати двофакторну аутентифікацію через SMS чи email.

IAM (Identity and Access Management) – це комплекс рішень, який дозволяє централізовано створювати, змінювати, зберігати та контролювати ідентифікатори користувачів та їхні права доступу до інформаційних систем.

Основні функції IAM:

– створення та видалення облікових записів;

– управління ролями та політиками доступу;

– аудит дій користувачів;

– контроль відповідності політик.

IAM забезпечує принцип "найменших привілеїв", згідно з яким користувач отримує лише той доступ, який необхідний для виконання його обов’язків. Це дозволяє мінімізувати ризики несанкціонованих дій, зокрема з боку внутрішніх користувачів.

Впровадження в МСП:

Для невеликих компаній варто використовувати відкриті або хмарні рішення, такі як:

– JumpCloud – керування користувачами в хмарі;

– Keycloak – open-source платформа IAM;

– Microsoft Entra ID (колишній Azure AD) – у хмарному середовищі.

PKI (Public Key Infrastructure) – це технологія, яка забезпечує шифрування, цифрові підписи та управління сертифікатами, що підтверджують справжність користувачів і пристроїв [14].

PKI базується на використанні пари ключів – відкритого (public) і закритого (private). Наприклад, користувач може зашифрувати лист відкритим ключем одержувача, а розшифрувати його зможе тільки власник закритого ключа.

PKI використовується для:

– безпечної передачі даних;
– автентифікації користувачів та пристроїв;
– цифрового підписування документів;
– забезпечення довіри в електронному середовищі.

Впровадження в МСП:

Для базових потреб можна створити власний внутрішній центр сертифікації (CA) за допомогою OpenSSL або Easy-RSA, або використовувати хмарні сервіси як-от Let's Encrypt (SSL/TLS сертифікати), AWS Certificate Manager, XCA – для генерації локальних сертифікатів [16].

У таблиці 2.2 представлено порівняльний аналіз трьох ключових методик, що використовуються для підвищення рівня захищеності доступу до інформаційних систем: багатофакторної аутентифікації (MFA), управління ідентичністю та доступом (IAM), а також інфраструктури відкритих ключів (PKI) [17]. Кожна з методик має свої сильні сторони і недоліки, що дозволяє організаціям обирати найбільш відповідні рішення відповідно до своїх ресурсів і потреб.

Таблиця 2.2

Порівняльна характеристика MFA, IAM та PKI

Методика	**Основне призначення**	**Переваги**	**Недоліки**	**Реалізація в МСП**
MFA	Підвищення безпеки за рахунок багатофакторної перевірки користувача	Захист навіть при компрометації пароля	Потреба в додатковому пристрої або програмі	Google Authenticator, FreeOTP, Microsoft Authenticator
IAM	Централізоване управління ідентичністю та правами доступу	Гнучке управління правами доступу, аудит активності	Складність налаштування в локальному середовищі	JumpCloud, Keycloak, Azure AD
PKI	Забезпечення шифрування, цифрових підписів та довіри через сертифікати	Висока довіра, підтримка шифрування та підпису	Необхідність у знаннях криптографії, керування сертифікатами	OpenSSL, Let's Encrypt, XCA

Застосування MFA, IAM і PKI дозволяє забезпечити багаторівневий захист від зовнішніх і внутрішніх загроз. Для малих і середніх підприємств критично важливо впроваджувати ці методики у спрощеній формі, орієнтуючись на хмарні сервіси, рішення з відкритим кодом і попередньо налаштовані платформи. Такий підхід забезпечує високий рівень захищеності навіть в умовах обмежених ресурсів [18].

Висновки до розділу 2

Розглянуто ключові методи та інструменти, що використовуються на практиці для реалізації ефективного аудиту інформаційної безпеки, зокрема в умовах обмежених ресурсів, характерних для малих та середніх компаній.

Проаналізовано підходи до планування аудиту, акцентуючи увагу на необхідності адаптації процесу до доступних можливостей організації. Було показано, що навіть при мінімальних витратах можна досягти базового рівня безпеки шляхом визначення критичних активів, складання чек-листів та застосування простих і структурованих процедур.

Розглянуто основні інструменти автоматизованої оцінки загроз, такі як SIEM-системи, IDS/IPS та сканери вразливостей (зокрема OpenVAS). Їх поєднане використання забезпечує комплексний підхід до моніторингу, виявлення атак та оцінювання стану безпеки, що особливо важливо для компаній, які не мають власного підрозділу кібербезпеки.

Приділено сучасним методикам аутентифікації та управління доступом: багатофакторній аутентифікації (MFA), системам IAM та інфраструктурі відкритих ключів (PKI). Зазначено, що навіть за обмежених ресурсів компанії можуть ефективно реалізувати ці механізми за допомогою відкритого ПЗ або хмарних рішень, що значно підвищує загальний рівень захищеності.

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ АУДИТУ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

3.1 Аутсорсингові моделі та MSSP як шлях оптимізації

У контексті зростаючої кількості кіберзагроз та обмежених ресурсів, характерних для більшості організацій, особливо малого та середнього бізнесу, все більше актуалізується питання ефективного управління інформаційною безпекою. Самостійне обслуговування IT-інфраструктури та кіберзахисту без належної експертизи може спричинити критичні помилки, зокрема через недостатній рівень підготовки внутрішніх фахівців або відсутність спеціалізованих підрозділів на зразок Security Operation Center (SOC) [21].

Класичні підходи до організації захисту – придбання програмного забезпечення й апаратних засобів без належної адаптації та впровадження – не гарантують належного рівня безпеки. Практика показує, що компанії часто використовують лише 50–70% можливостей наявних систем захисту, що свідчить про неефективне використання інвестицій.

Розвиток штучного інтелекту та автоматизації одночасно створює нові виклики і можливості: кіберзлочинці отримують потужні інструменти для автоматизації атак, тоді як захисні системи також можуть застосовувати AI для виявлення аномалій, аналізу загроз і реагування на інциденти.

В умовах дефіциту кваліфікованих кадрів та постійного ускладнення IT-ландшафту, підприємства дедалі частіше звертаються до керованих сервісів безпеки. Це, зокрема, Managed Security Service Providers (MSSP), Managed Service Providers (MSP) і сервіси класу MDR (Managed Detection and Response), які забезпечують не лише технічну підтримку та обслуговування, а й проактивний моніторинг, аналіз і реагування на інциденти. Такий підхід дозволяє оптимізувати витрати, знизити ризики та забезпечити постійний контроль над інформаційною безпекою без потреби формувати внутрішній підрозділ [21-22].

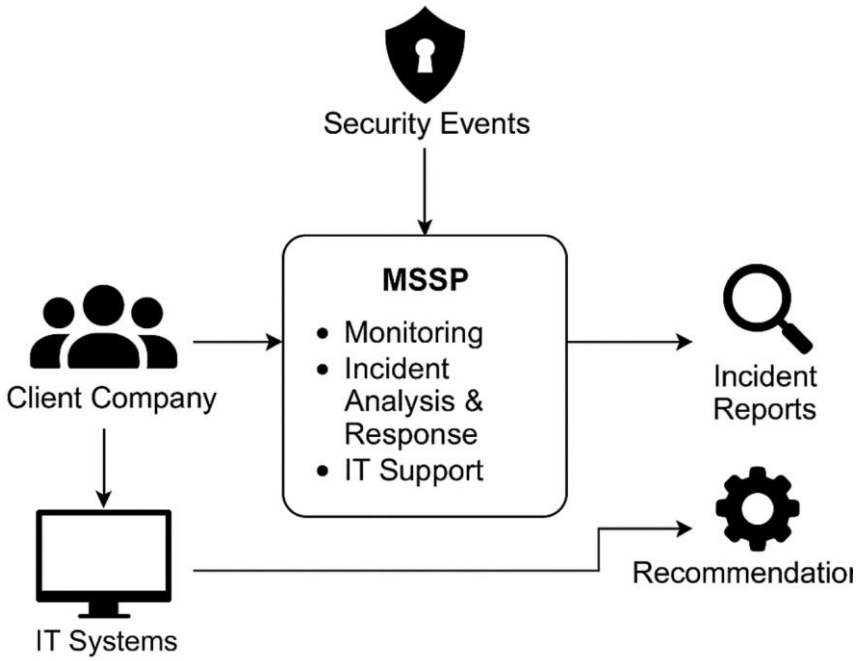

Рис. 3.1. Архітектура взаємодії клієнта з MSSP-провайдером

Managed Services – це модель аутсорсингу, за якої спеціалізований провайдер бере на себе комплексне управління та технічну підтримку IT-інфраструктури замовника. Такий підхід передбачає не лише передавання окремих задач, а й повноцінну інтеграцію експертних рішень: від налаштування та обслуговування інформаційних систем до їх захисту, постійного моніторингу, оновлення, усунення несправностей і реагування на інциденти [22].

```
{
  "module": "firewall",
  "log_source": "/var/log/firewall.log",
  "mssp_forwarding": true,
  "destination": "https://mssp-gateway.example.com",
  "token": "secure-api-token"
}
```

Рис. 3.2. Приклад конфігурації логування для MSSP-інтеграції

Порівняння MSSP і класичного аутсорсингу. Різниця між MSP, MSSP та MDR

У практиці управління інформаційною безпекою поняття аутсорсингу

набуло різних форм, однак принципова відмінність керованих послуг (Managed Services) полягає не лише у делегуванні окремих завдань, а у постійному супроводі, інтеграції в бізнес-процеси замовника та проактивному моніторингу IT-інфраструктури. На відміну від традиційного IT-аутсорсингу, що зазвичай обмежується підтримкою окремих сервісів або наданням IT-спеціалістів «в оренду», MSSP гарантують цілісну систему кіберзахисту, орієнтовану на виявлення, попередження та реагування на загрози в режимі 24/7. Це дозволяє істотно знизити ризики кібератак і підвищити надійність IT-середовища компанії. У таблиці 3.1 представлено узагальнену характеристику зазначених моделей, що дозволяє оцінити їх відмінності за ключовими параметрами [23].

Таблиця 3.1

Порівняльна характеристика MSP, MSSP та MDR

Критерій	**MSP (Managed Service Provider)**	**MSSP (Managed Security Service Provider)**	**MDR (Managed Detection & Response)**
Фокус	Загальне управління IT-інфраструктурою	Повноцінна підтримка систем кібербезпеки	Операційне реагування на інциденти
Основні функції	Мережеве адміністрування, резервне копіювання, оновлення ПЗ	Налаштування і супровід систем захисту (SIEM, FW, AV)	Виявлення, аналіз і реагування на загрози (SOC, EDR, XDR)
Технології	Базові IT-сервіси	SIEM, IDS/IPS, VPN, DLP	EDR, XDR, NDR, Cyber Deception
Проактивний моніторинг	Обмежений або відсутній	Постійний (24/7)	Постійний з глибоким аналізом

Продовження таблиці 3.1

Рівень автоматизації	Низький	Середній	Високий (включно з AI/ML-рішеннями)
Рекомендований тип бізнесу	Малі та середні компанії без складних вимог	Бізнес із середніми та високими вимогами до безпеки	Критично важливі сфери (фінанси, медицина, державний сектор)
Вартість	Низька	Середня	Висока

Незважаючи на об’єктивні переваги, рішення про співпрацю з зовнішніми провайдерами часто уповільнюється через недовіру до постачальників та побоювання втрати контролю над критичними системами. У практиці багатьох компаній, особливо у сфері SMB, CIO/CISO не готові передавати ключові елементи безпеки на аутсорсинг [24].

Тим не менш, ігнорування дефіциту кваліфікованого персоналу, спроби утримувати безпеку внутрішніми силами без належної компетенції та ресурсів – призводять до затримок в реакції, неправильної конфігурації систем і, як наслідок, ризику фінансових втрат, штрафів, або компрометації даних.

В умовах обмежених ресурсів, високої динаміки загроз та нестачі кваліфікованих кадрів, керовані сервіси (MSP, MSSP, MDR) стають актуальним інструментом забезпечення стабільної та ефективної роботи IT-інфраструктури малого та середнього бізнесу (МСБ) в Україні.

Серед ключових переваг впровадження таких послуг можна виокремити наступне:

– Оперативне впровадження. Компанії можуть почати використовувати сервіс практично відразу, без необхідності розгортання власної технічної інфраструктури.

– Усунення кадрового дефіциту. Провайдери послуг надають доступ до фахівців високої кваліфікації, що дозволяє уникнути витрат на пошук, навчання та утримання внутрішньої команди.

– Безперервний моніторинг. Сервіси MSSP/MDR забезпечують цілодобовий контроль за подіями безпеки з негайною реакцією на інциденти, що важливо для зменшення часу виявлення та реагування (MTTD/MTTR).

– Масштабованість. Послуги адаптуються до поточних і перспективних потреб бізнесу, що особливо важливо для компаній, які знаходяться у фазі росту або цифрової трансформації [24-25, 27].

– Доступ до сучасних технологій. У розпорядженні замовника – найновіші рішення в сфері безпеки (SIEM, XDR, EDR, NDR, SOAR), які інтегруються та підтримуються без потреби у великих початкових інвестиціях.

– Оптимізація витрат. Використання MSSP знижує сукупну вартість володіння (TCO), оскільки витрати на створення та утримання власного підрозділу значно вищі, ніж вартість зовнішніх послуг.

– Зовнішній аудит. Провайдер надає об’єктивну оцінку стану IT-інфраструктури та безпеки, виявляючи помилки або прогалини, які могли бути непомітними зсередини.

– Фокус на пріоритетах. Співпраця із зовнішніми фахівцями дозволяє внутрішнім командам зосередитися на стратегічних завданнях, а не на рутинному адмініструванні [26].

Ключові технології, що лежать в основі MSSP та MDR-сервісів

Для реалізації керованих сервісів у сфері IT-безпеки провайдери MSSP та MDR залучають різні технологічні рішення, залежно від глибини інтеграції та рівня реагування на інциденти. Відмінності між ними насамперед полягають у технологічному фокусі, масштабі відповідальності та ступені операційної зрілості.

MSSP – Керування системами захисту

У фокусі Managed Security Service Providers (MSSP) – підтримка, адміністрування та оновлення систем безпеки, зокрема:

– NG-FW (Next-Generation Firewall) та UTM-системи – сучасні міжмережеві екрани, що забезпечують фільтрацію трафіку на рівні додатків (Cisco ASA, Fortinet FortiGate, Palo Alto NGFW).

– Системи виявлення аномалій (UEBA), що аналізують поведінкові патерни користувачів.

– Системи управління привілеями (PAM), які контролюють доступ до критичних ресурсів.

– Засоби захисту електронної пошти, антивірусні платформи, рішення для моніторингу вебтрафіку.

– Інструменти для централізованого оновлення й логування.

MSSP переважно працює як інтегратор і адміністратор засобів захисту, націлений на підтримку безперервної працездатності захисного контуру.

MDR – Аналітика, виявлення та реагування

У свою чергу, MDR (Managed Detection and Response) орієнтований на операційну активність із фокусом на виявлення інцидентів, розслідування й оперативну відповідь. Це досягається шляхом використання:

– SIEM (Security Information and Event Management) – збір і кореляція подій із різних джерел.

– XDR / EDR / NDR – рішення для глибокого аналізу подій на кінцевих точках, у мережі та хмарі.

– Cyber Deception – технології активного обману зловмисника для виявлення на ранніх етапах.

– SOAR (Security Orchestration, Automation and Response) – автоматизовані платформи для реагування на інциденти [27].

На відміну від MSSP, де основна мета – підтримка інфраструктури, MDR забезпечує виявлення загроз, кореляцію подій, ескалацію інцидентів, проведення розслідувань і розробку відповідних дій. Упровадження MDR-рішення без залучення експертної команди SOC є малоефективним, оскільки самі по собі технології не забезпечують безпеку без належної аналітики та реакції.

3.2 Ефективне використання Open-source рішень для аудиту

В умовах обмеженого бюджету, характерного для багатьох малих і

середніх підприємств, використання безкоштовного open-source програмного забезпечення є дієвим підходом до впровадження базових практик кібербезпеки. Відкриті рішення дають можливість виконувати аудит систем, виявляти вразливості, здійснювати моніторинг безпеки без ліцензійних витрат, забезпечуючи при цьому гнучкість налаштування та прозорість функціоналу.

Однією з найпоширеніших задач у процесі аудиту є сканування вразливостей, що дозволяє своєчасно виявити потенційні точки атаки. Для цього активно використовуються такі системи, як OpenVAS, AlienVault, Nmap, Lynis, Wazuh та інші [28].

Таблиця 3.2

Найпопулярніші open-source інструменти для аудиту безпеки

Назва	**Призначення**	**Особливості**
OpenVAS	Сканування вразливостей	Підтримує десятки тисяч вразливостей, інтеграція з GVM
Lynis	Аудит конфігурацій UNIX/Linux	Аналізує налаштування, виводить рекомендації
AlienVault	Веб-сканер	Виявлення слабких конфігурацій веб-серверів

Продовження таблиці 3.2

Nmap	Аналіз портів і сервісів	Підтримує скриптовий аналіз (NSE)
Wazuh	SIEM-платформа, моніторинг подій	Реагування на інциденти, логування, відповідність стандартам
OSQuery	SQL-запити до системних параметрів	Ідеально підходить для живого аудиту робочих станцій

Приклад використання OpenVAS

OpenVAS (Greenbone Vulnerability Scanner) є одним із найпотужніших інструментів для оцінки вразливостей. Він дозволяє проводити повноцінне сканування мережі, визначати рівень ризиків, генерувати звіти з рекомендаціями. Ось базовий приклад команди для запуску сканування (через GVM-CLI):

```
gvm-cli socket --gmp-username admin --gmp-password "your_password" << EOF
<create_target><name>Local Scan</name><hosts>192.168.1.1</hosts></create_target>
EOF
```

Рис. 3.3. Типова схема використання OpenVAS у внутрішній мережі

Схема демонструє взаємодію між OpenVAS, сервером сканування, базою вразливостей (NVTs) та цільовими вузлами в локальній інфраструктурі.

Комбіноване використання: OSQuery + Wazuh

Ще одним ефективним підходом є поєднання Wazuh (як SIEM-агента) з OSQuery – потужним інструментом для збору даних у вигляді SQL-запитів до системних таблиць. Це дозволяє автоматизувати контроль цілісності, моніторинг змін файлів, відстеження аномалій у поведінці користувачів. На рисунку 3.4 відображено, як OSQuery виконує запити до локальної системи, передає результати у Wazuh-агент, а той – на центральний сервер з SIEM-інтерфейсом для подальшого аналізу [29].

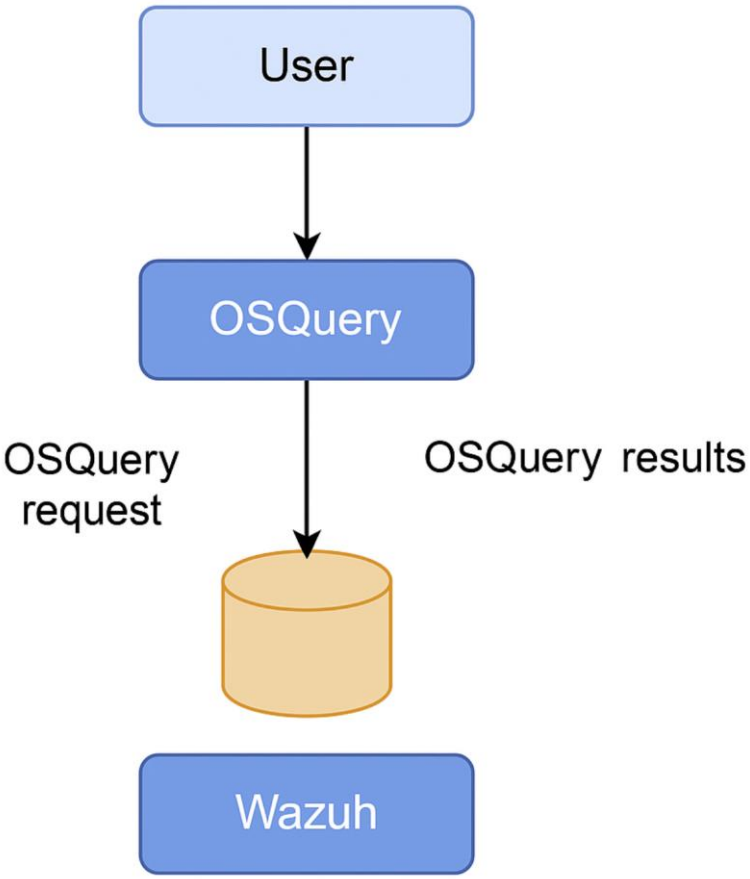

Рис. 3.4. Схема взаємодії OSQuery з Wazuh

Переваги open-source інструментів в аудиті:

1. Доступність і прозорість – можливість перевірити вихідний код і впевнитися у відсутності бекдорів.
2. Гнучкість – легко налаштовуються під індивідуальні потреби.
3. Спільнота – активні користувачі забезпечують регулярне оновлення, патчі та нові плагіни.
4. Інтеграція – більшість рішень підтримують API, що дозволяє будувати кастомізовані системи аудиту й моніторингу [29].

Фрагмент типового звіту сканування OpenVAS (Markdown-стиль). Звіт сканування цілі: 192.168.1.15 Дата: 2025-04-06 Інструмент: OpenVAS / GVM

Статус: Завершено.

Резюме:

Тип уразливості	Кількість
Високий ризик (High)	3
Середній ризик (Medium)	7
Низький ризик (Low)	15
Інформаційні	20

Виявлені критичні уразливості:

1. CVE-2022-1388 (F5 BIG-IP iControl REST Auth Bypass)
- Статус: Відкрита
- Рішення: Негайне оновлення системи
- Порт: 443/tcp
2. SMB Signing Disabled
- Статус: Вразливість до MITM-атак
- Рекомендація: Увімкнути підписування SMB
3. OpenSSH Outdated Version
- Версія: 7.4p1
- Ризик: Уразливість до CVE-2018-15473

3.3 Побудова безпечної інфраструктури на основі SIEM-моніторингу

Розгортання AlienVault OSSIM

Встановлення системи виконується через завантаження офіційного ISO-образу, який вже містить Debian та всі необхідні модулі.

1. Завантажити ISO з сайту AT&T Cybersecurity [30].
2. Створити завантажувальну флешку або віртуальну машину (наприклад, у VirtualBox або VMware).
3. Після запуску – вибрати повну установку (Install AlienVault OSSIM 64-bit).
4. У процесі інсталяції вказуються:

- IP-адреса та сітка вручну
- назва хосту
- root-пароль

5. Після завершення інсталяції система перезавантажується і доступна через веб-інтерфейс:
   https://<ip-адреса>/ossim

Першим етапом підготовки до розгортання SIEM-системи стало завантаження актуальної версії дистрибутива AlienVault OSSIM з офіційного сайту. Для запуску системи було використано середовище VirtualBox, встановлене на персональний комп'ютер користувача. Віртуальна машина з представленими параметрами показана на рисунку 3.5 [31].

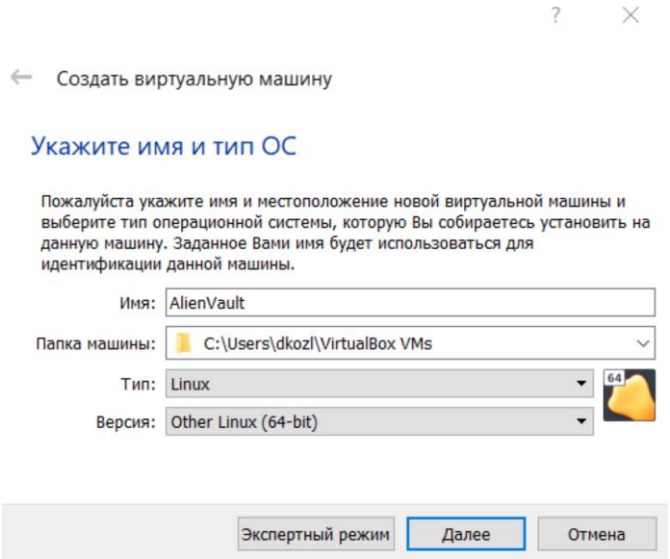

Рис. 3.5. Назва та тип операційної системи при створенні віртуальної машини для OSSIM

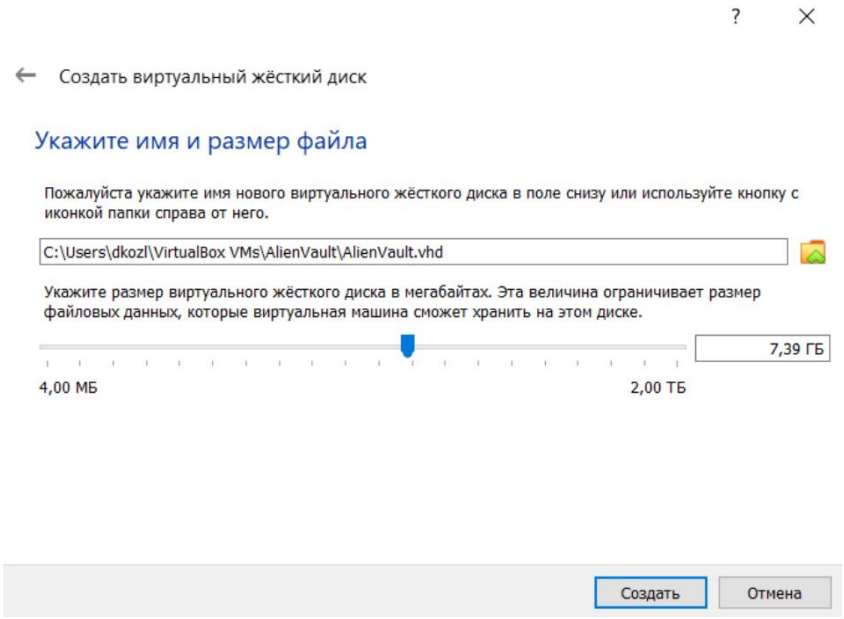

Рис. 3.6. Назва файлу віртуальної машини та розмір віртуального диска

Після створення та запуску віртуальної машини необхідно вказати завантажувальний образ дистрибутива OSSIM як джерело інсталяції. У цьому випадку ISO-образ було змонтовано за допомогою стороннього програмного забезпечення DAEMON Tools Lite, що надало змогу відобразити диск у системі під літерою E.

Під час першого запуску ВМ у VirtualBox образ було підключено як віртуальний CD/DVD-диск, після чого система автоматично розпочала процедуру інсталяції. На рисунку 3.7 показано вибір змонтованого ISO-образу OSSIM у віртуальному приводі (диск E:), що дозволяє ініціювати інсталяцію системи безпосередньо у VirtualBox [32].

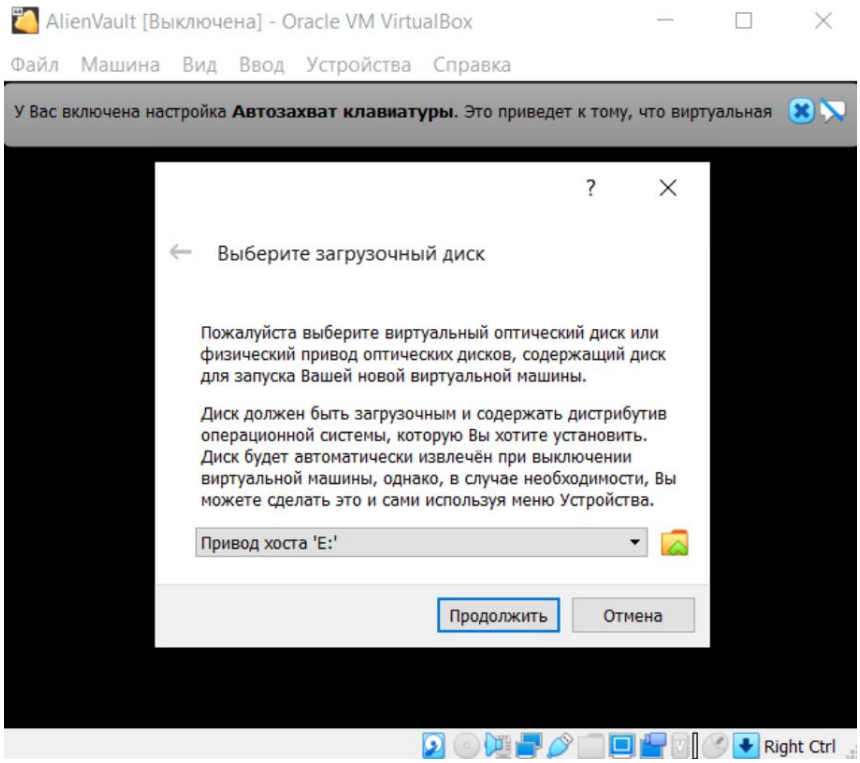

Рис. 3.7. Вибір завантажувального диска для встановлення OSSIM

На наступному етапі інсталяції користувачеві пропонується список доступних режимів запуску. Потрібно обрати перший варіант – "Install AlienVault OSSIM 64-bit", що передбачає типову установку системи та відповідає класичному процесу встановлення Debian [32].

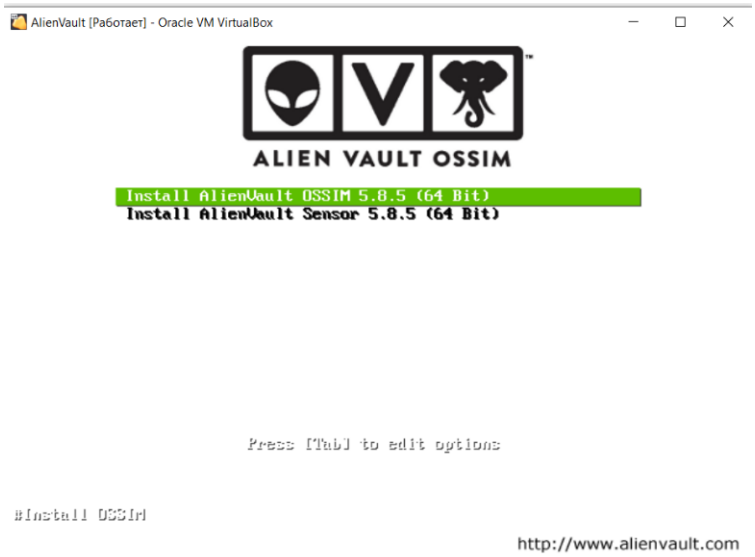

Рис. 3.8. Вибір варіанту встановлення OSSIM у стартовому меню

Після запуску інсталятора першою дією є вибір мови інтерфейсу, після

чого система переходить до завантаження необхідних компонентів. Далі користувач переходить до налаштування мережевого інтерфейсу.

У процесі конфігурації потрібно вручну ввести статичну IP-адресу, яка буде використовуватись для доступу до веб-інтерфейсу OSSIM.

На рис. 3.9 зображено приклад встановлення локальної IP-адреси – у даному випадку це 192.168.1.150, яка згодом дозволить здійснювати вхід до SIEM-системи через браузер.

Рис. 3.9. Визначення IP-адреси для доступу до SIEM-системи OSSIM

Наступним кроком після введення IP-адреси є задання маски підмережі, яка у типовому середовищі локальної мережі становить 255.255.255.0. Завершення мережевих налаштувань означає, що конфігурація віртуальної машини повністю готова до запуску [33].

Після перезавантаження системи залишається виконати авторизацію через консоль та перевірити доступність SIEM-системи через вебінтерфейс, ввівши IP-адресу, зазначену раніше, у рядок браузера.

На рисунках 3.10 та 3.11 показано відповідно процес авторизації в інтерфейсі OSSIM та вигляд головної сторінки системи після успішного підключення.

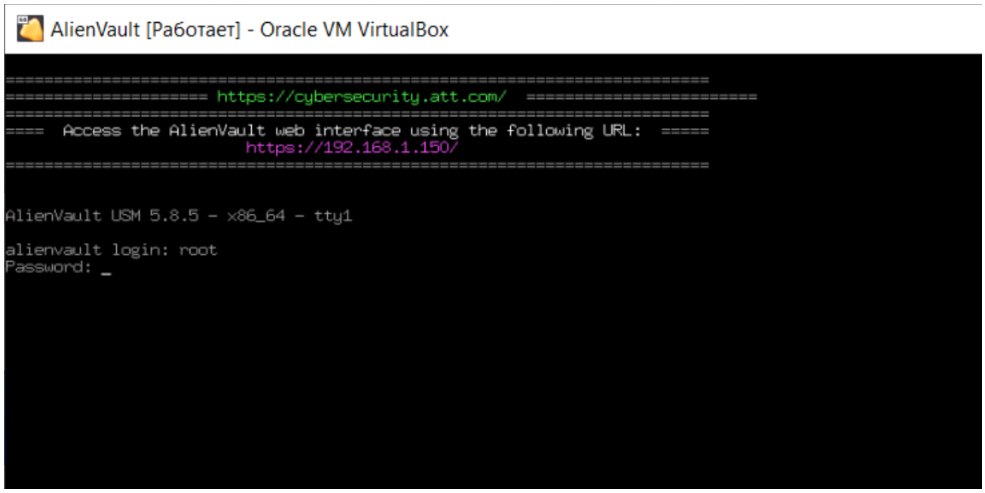

Рис. 3.10 – Авторизація в інтерфейсі AlienVault OSSIM

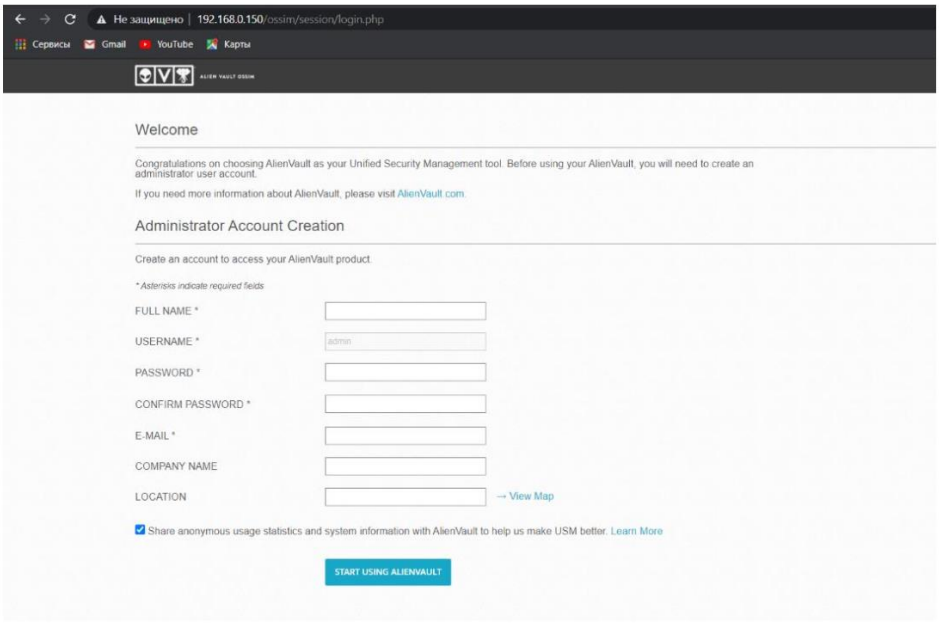

Рис. 3.11 Вхід до веб-інтерфейсу OSSIM через браузер

Конфігурація клієнтських систем у рамках SIEM-інфраструктури

Після успішного запуску та доступу до OSSIM через веб-інтерфейс, наступним кроком є додавання хостів до моніторингу. У даному випадку було вирішено додати локальний ноутбук користувача як клієнтську частину для демонстрації функціональності системи [33-34].

Для цього у веб-інтерфейсі OSSIM було запущено автоматичне сканування локальної мережі в межах підмережі 192.168.0.0/16, у якій знаходяться як SIEM-сервер, так і клієнтський ноутбук.

На рисунку 3.12 зображено процес запуску мережевого сканування з інтерфейсу OSSIM для виявлення активних пристроїв у локальному середовищі.

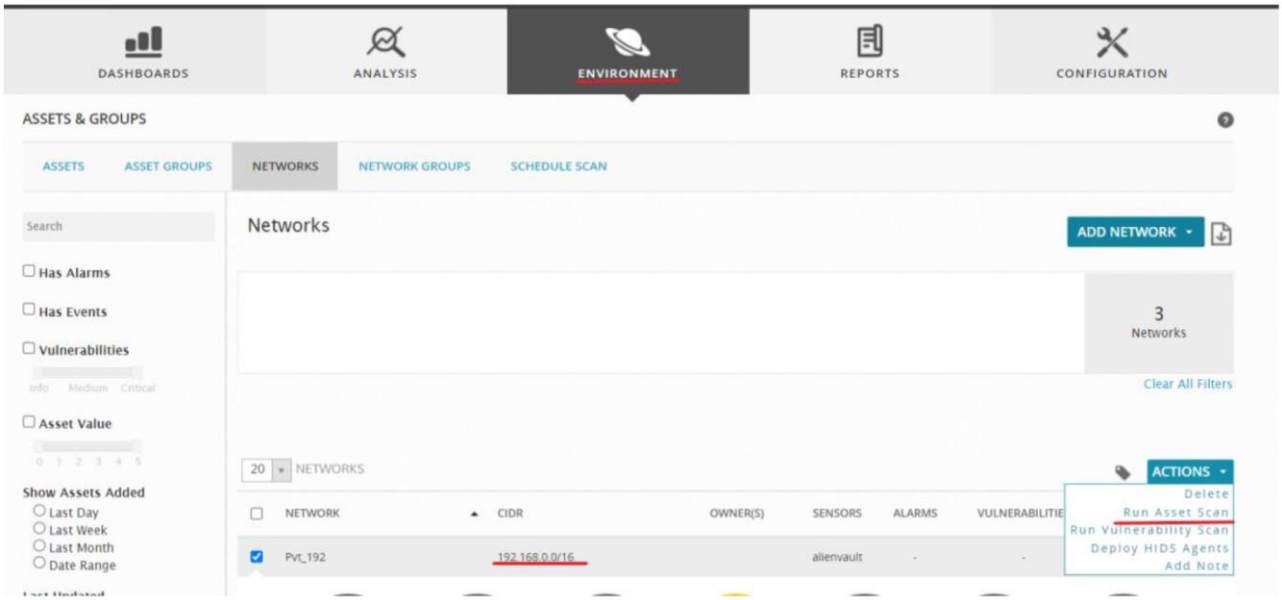

Рис. 3.12. Автоматичне сканування мережі 192.168.0.0/16 для виявлення клієнтських хостів

Після завершення сканування система автоматично формує список активних пристроїв, виявлених у зазначеному діапазоні IP-адрес. Ці хости можуть бути додані до моніторингу для подальшого аналізу подій безпеки. На рисунку 3.13 представлено результат сканування мережі – список клієнтських пристроїв, доступних для інтеграції у SIEM-середовище [35].

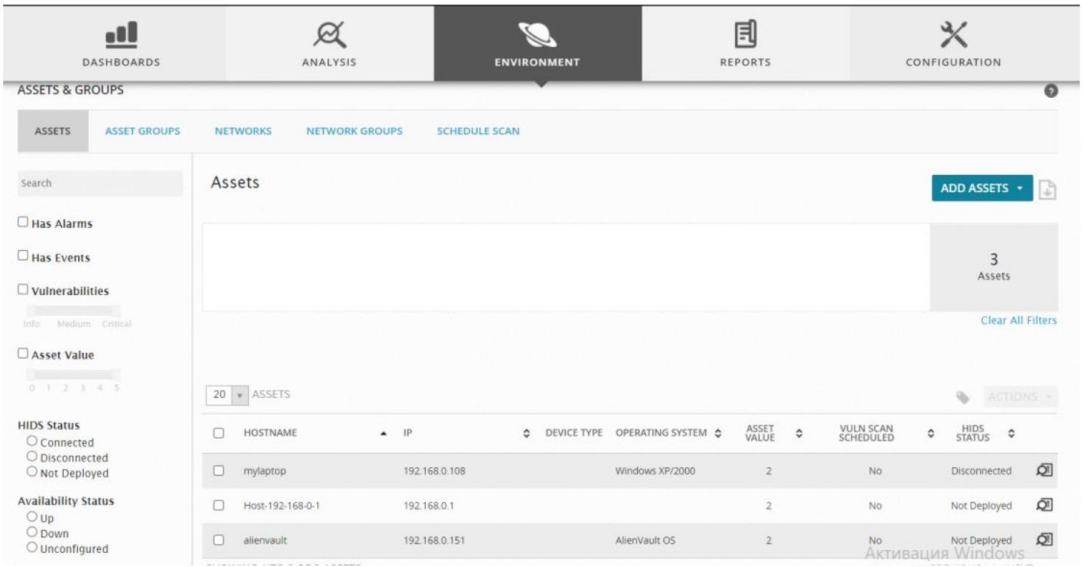

Рис. 3.13. Результати сканування: виявлені пристрої в локальній мережі

Після додавання виявленого пристрою до системи, OSSIM автоматично починає збирати телеметрію про його активність, відкриті порти, запущені служби, а також реєструє відповідні події безпеки.

На рисунку 3.14 продемонстровано, що система вже почала фіксувати активність з обраного хосту, що підтверджує успішну інтеграцію клієнтського пристрою до середовища моніторингу.

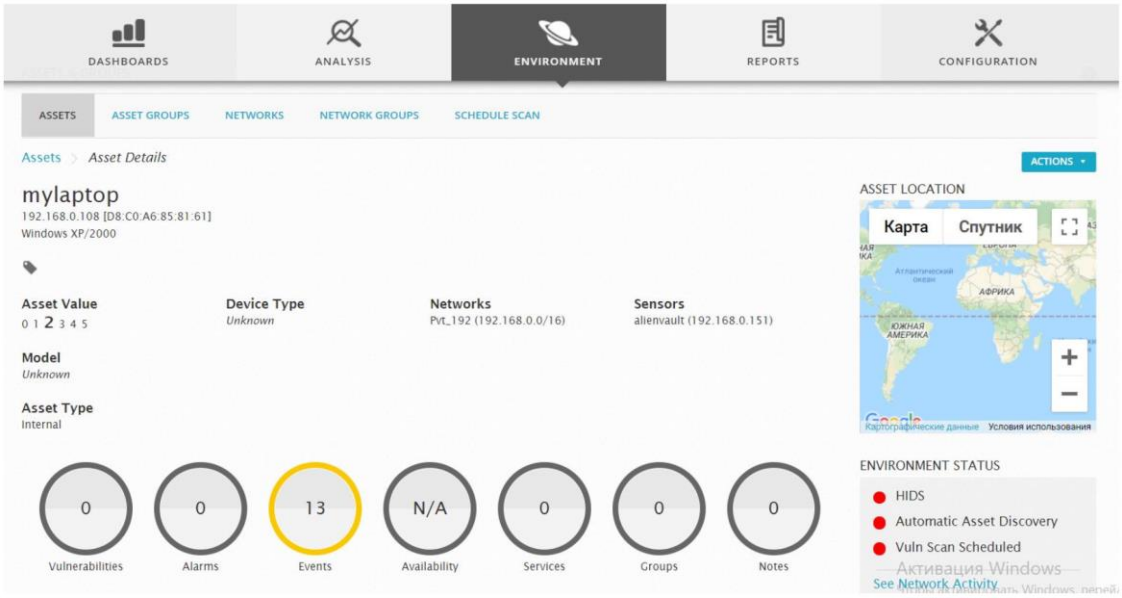

Рис. 3.14. Візуалізація активності з клієнтського хоста в інтерфейсі OSSIM

Після завершення інтеграції клієнтських пристроїв адміністратор отримує можливість здійснювати повноцінний моніторинг подій безпеки та стану інфраструктури за допомогою зручного веб-інтерфейсу OSSIM. Одним із ключових функціональних блоків є розділ Dashboards, який надає інтерактивну панель із ключовими індикаторами безпеки [34-36].

Тут відображаються:

- загальна кількість загроз, розподілених за рівнем серйозності;
- статус вразливостей для конкретних мережевих вузлів;
- карта ризиків у реальному часі;
- статистика спрацювань правил SIEM та загальна активність агентів;
- статуси сенсорів і служб.

На рисунку 3.15 показано приклад інтерфейсу OSSIM Dashboard, що

ілюструє основні компоненти серверної частини системи.

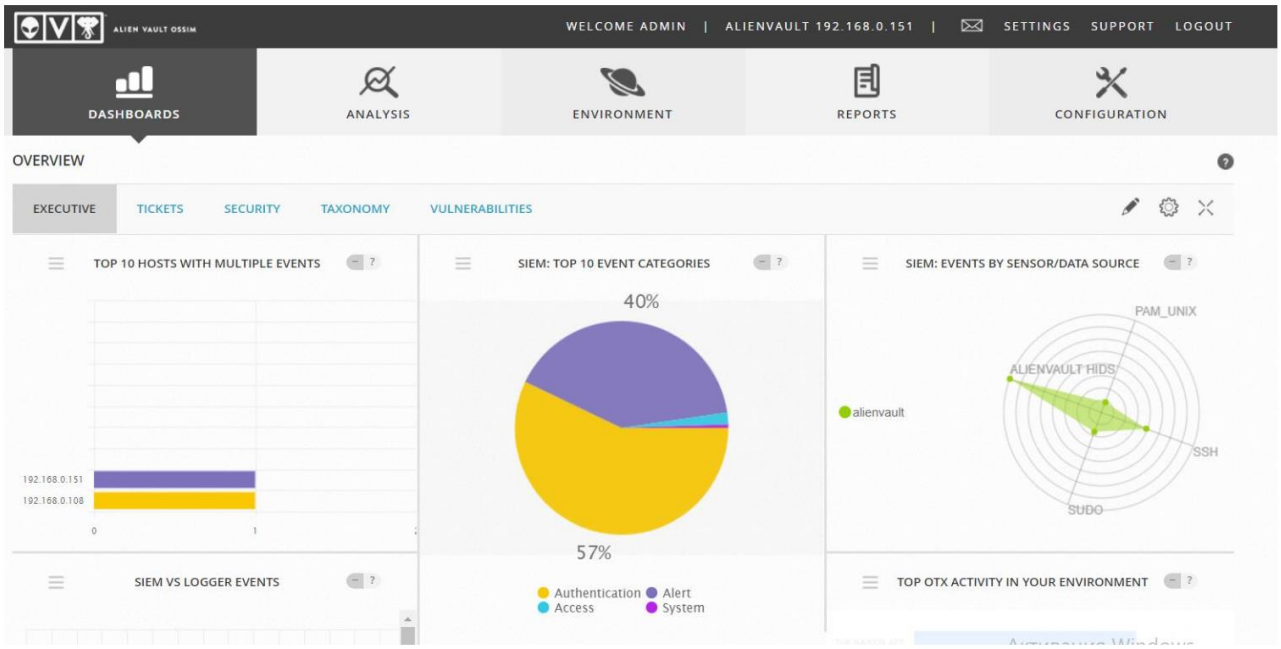

Рис. 3.15. Інтерфейс OSSIM Dashboard з оглядовою інформацією про стан системи безпеки

Ще одним важливим розділом інтерфейсу OSSIM є Analysis – функціональний модуль, який відповідає за деталізований аналіз безпекових подій та логів з підключених пристроїв.

Даний розділ відіграє ключову роль у процесі виявлення, класифікації та реагування на інциденти безпеки, оскільки надає розгорнуту інформацію, зібрану з хостів у реальному часі.

Інформація представлена у вигляді:

- сигналів тривоги з вказаним джерелом, ціллю та рівнем ризику,
- подій SIEM із зазначенням модуля-детектора,
- відкритих тікетів (інцидентів) для обробки,
- сирих логів, які можуть бути корисними для ручного аналізу.

На рисунку 3.16 представлено інтерфейс розділу Analysis, де зображено панель керування подіями, тривогами та логами, що надходять із підключених клієнтів [37].

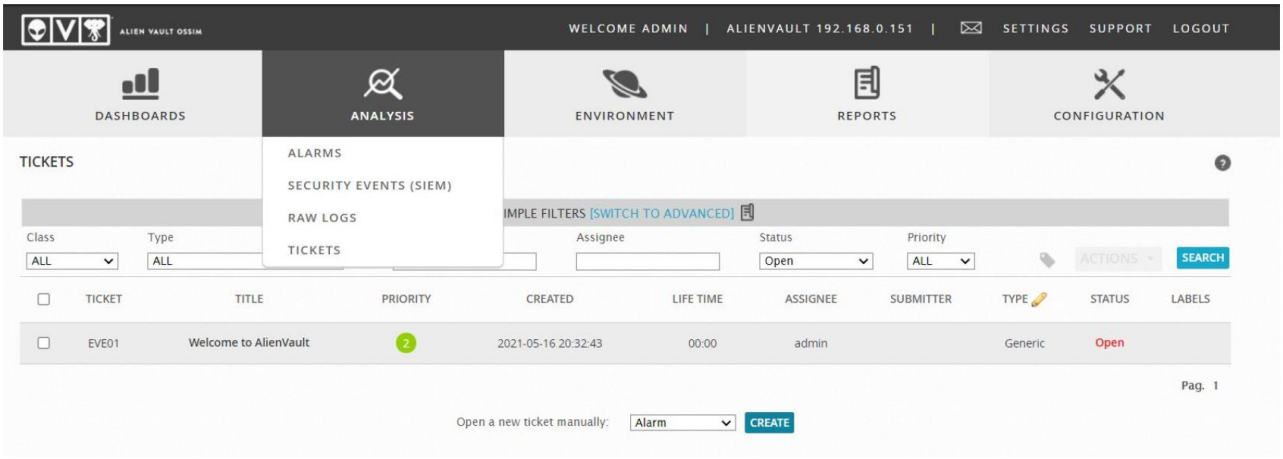

Рис. 3.16. Модуль Analysis у веб-інтерфейсі OSSIM з подіями безпеки

Середовище (Environment) – це розділ інтерфейсу сервера OSSIM, який відповідає за конфігурацію пристроїв, що входять до інфраструктури організації. У цьому меню можна переглядати інформацію про всі підключені пристрої, об’єднані групи, мережеві сегменти, а також уразливості, мережевий трафік і параметри виявлення загроз. Візуальне представлення інтерфейсу цього розділу наведено на Рисунку 3.17 – Інтерфейс розділу "Середовище" в OSSIM.

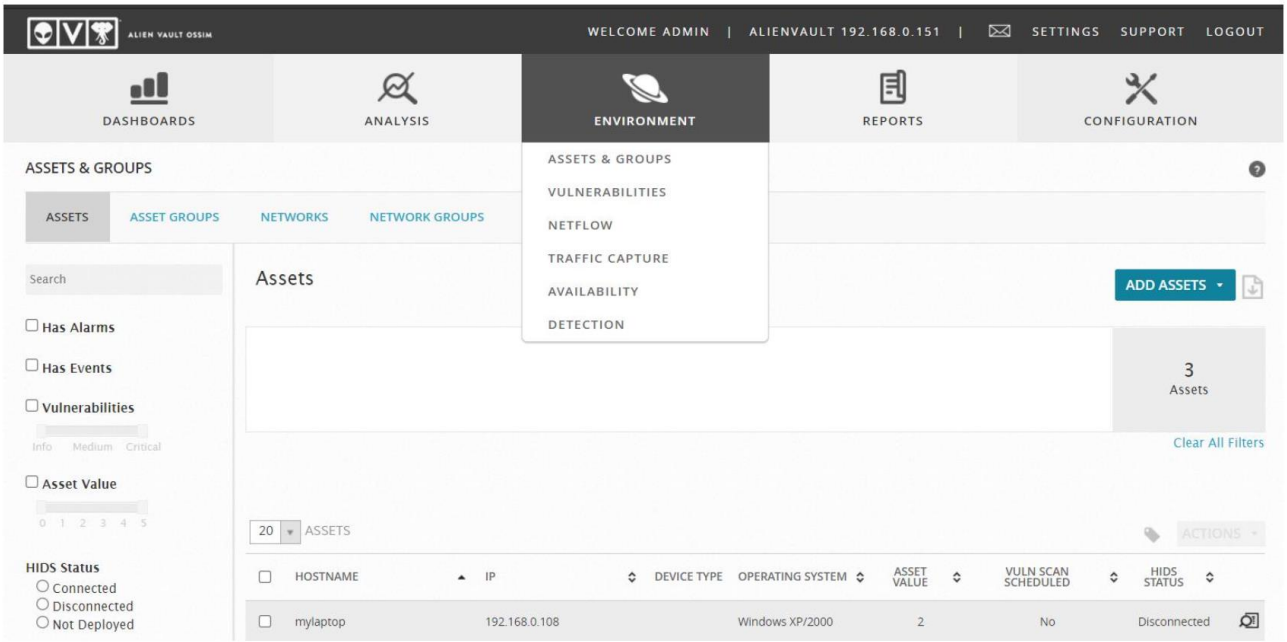

Рис. 3.17. Вкладка "Середовище" в інтерфейсі OSSIM

Звітність (Reports) – невід’ємна складова функціональності будь-якого сервера, що виконує роль реєстрації та моніторингу подій. У системі OSSIM

модуль звітності дозволяє формувати детальні звіти, які можуть бути надзвичайно корисними під час аналізу подій, пов’язаних із конкретним хостом. Генеровані звіти допомагають виявити аномалії, простежити дії користувачів або атакувальників, а також підготуватися до аудиту безпеки. Приклад інтерфейсу модуля звітності наведено на Рисунку 3.18 – Інтерфейс модуля звітності OSSIM [38].

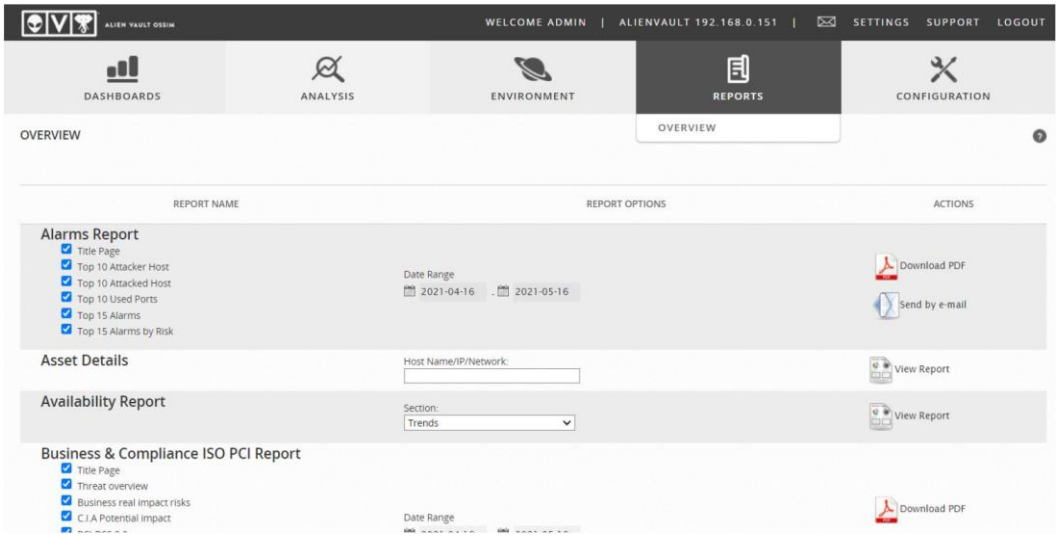

Рис. 3.18. Інтерфейс модуля звітності OSSIM

Конфігурація (Configuration) – це розділ, призначений для керування основними параметрами системи AlienVault SIEM (OSSIM). За його допомогою адміністратор може змінювати налаштування сервера, зокрема IP-адресу інтерфейсу управління, підключати додаткові хости для моніторингу та логування, а також додавати або видаляти різноманітні сенсори й плагіни залежно від потреб інфраструктури. Інтерфейс цього розділу представлено на Рис. 3.19.

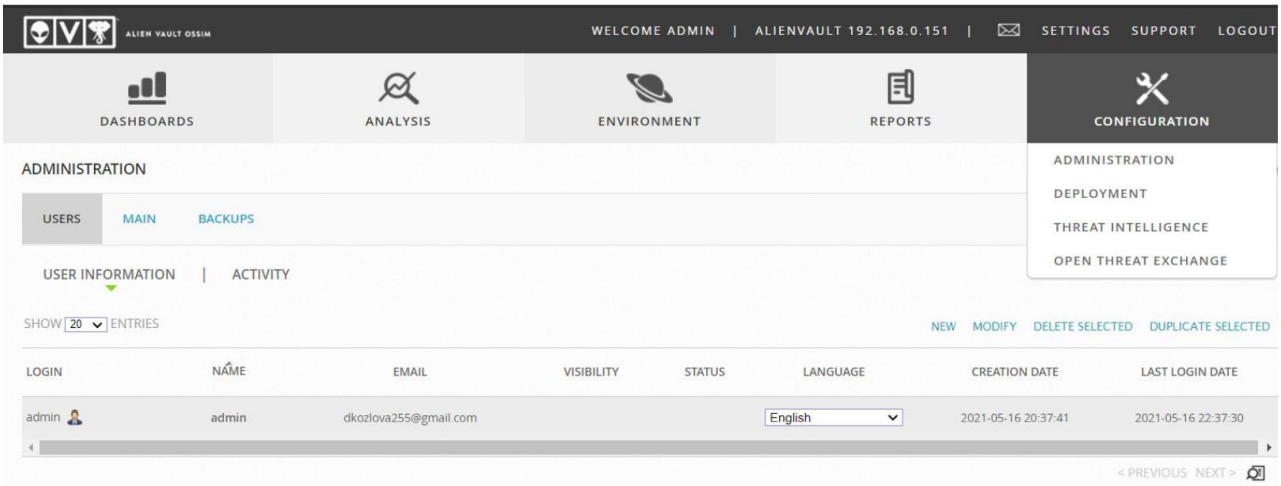

Рис. 3.19. Вкладка конфігурації системи OSSIM

Розгортання модуля EventLog Analyzer для AlienVault SIEM

Інсталяція EventLog Analyzer відбувається у звичний для більшості користувачів спосіб – за допомогою інсталяційного пакету без потреби у складних попередніх налаштуваннях. У випадку запуску модуля з робочої станції, система автоматично починає збір даних з цієї машини без додаткового втручання користувача.

Після авторизації у веб-інтерфейсі користувач одразу отримує доступ до вже зібраної інформації з локального хоста. Основний інтерфейс представлений у вигляді вкладки Dashboard, яка містить набір інформаційних панелей. Ці панелі надають стислий огляд ключових подій, що відбуваються в мережі, і дозволяють оперативно реагувати на інциденти безпеки [38].

Огляд ключових подій, а також графічні елементи для аналізу безпекової ситуації в мережі зосереджені у вкладці Dashboard. Вона служить зручною точкою входу для моніторингу та реагування. Вигляд цієї панелі можна побачити на рисунку 3.20, який ілюструє інтерфейс після першого запуску.

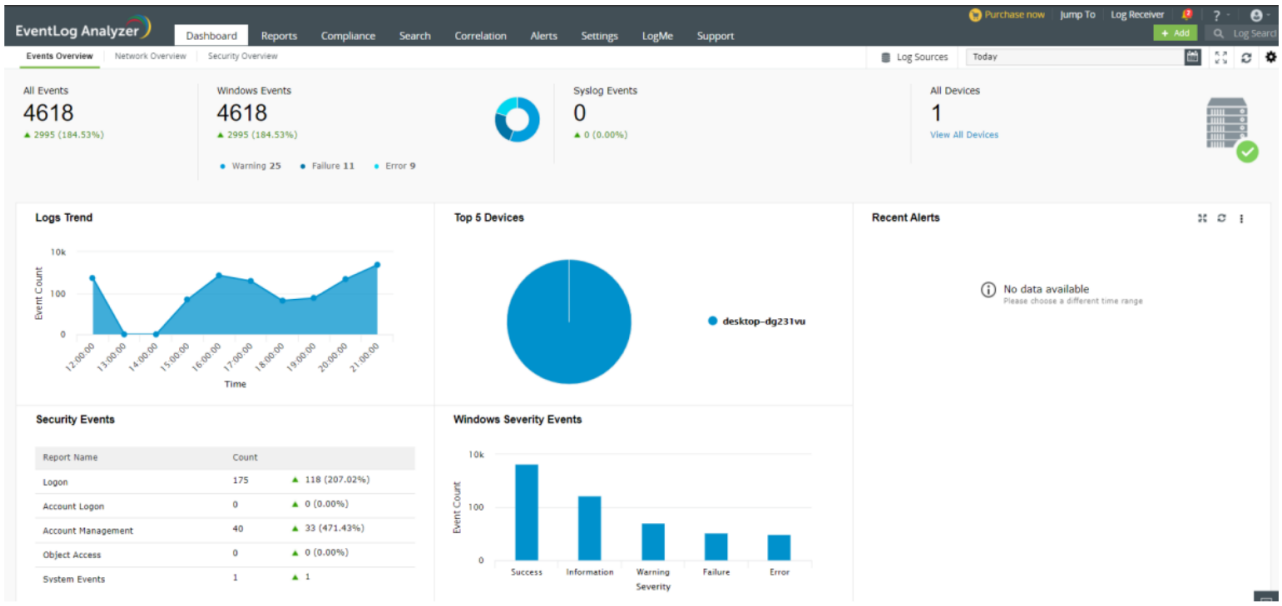

Рис. 3.20. Панель управління EventLog Analyzer після запуску.

Робота зі звітністю в EventLog Analyzer

Вкладка "Reports" у графічному інтерфейсі EventLog Analyzer надає користувачу зручний доступ до сформованих звітів, які відображають статистику подій з можливістю переходу до необроблених логів для більш глибокого аналізу. Цей функціонал особливо корисний при необхідності детального розслідування інцидентів або побудови історії подій.

Для зручності роботи передбачена система фільтрації – журнали можна відсортувати за різними критеріями, такими як тип події, IP-адреса джерела, користувач тощо. Крім того, інструмент підтримує автоматизацію: є можливість налаштувати регулярну генерацію звітів із подальшим надсиланням їх на вказану електронну адресу.

Звіти, створені під конкретні потреби, можуть бути збережені у вигляді XML-файлів, які легко експортувати та, за потреби, знову імпортувати в систему. Інтерфейс цього розділу представлено на наступній ілюстрації – рисунок 3.21 демонструє структуру звітного модулю та його основні можливості.

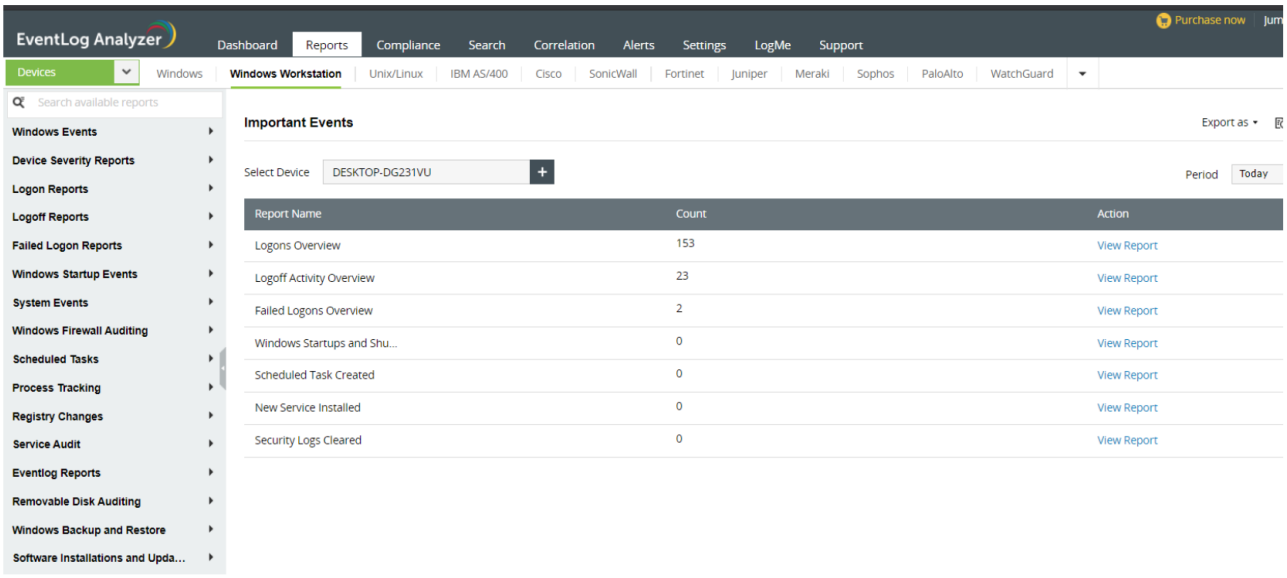

Рис. 3.21. Інтерфейс розділу звітності Reports у EventLog Analyzer

Крім стандартної аналітики подій, через вкладку Reports також доступна детальна інформація про активність користувачів у системі. Зокрема, можна переглядати історію входів і виходів, аналізувати час найбільшої активності, а також отримувати статистику за окремими користувачами – наприклад, частоту авторизацій кожного з них [39].

Такий підхід дає змогу швидко виявити аномалії або підозрілу поведінку. Функціональність цієї аналітики зручно представлена у візуальному вигляді на рисунках 3.22 та 3.23, де показано приклади статистичних зведень та розподілу активності користувачів.

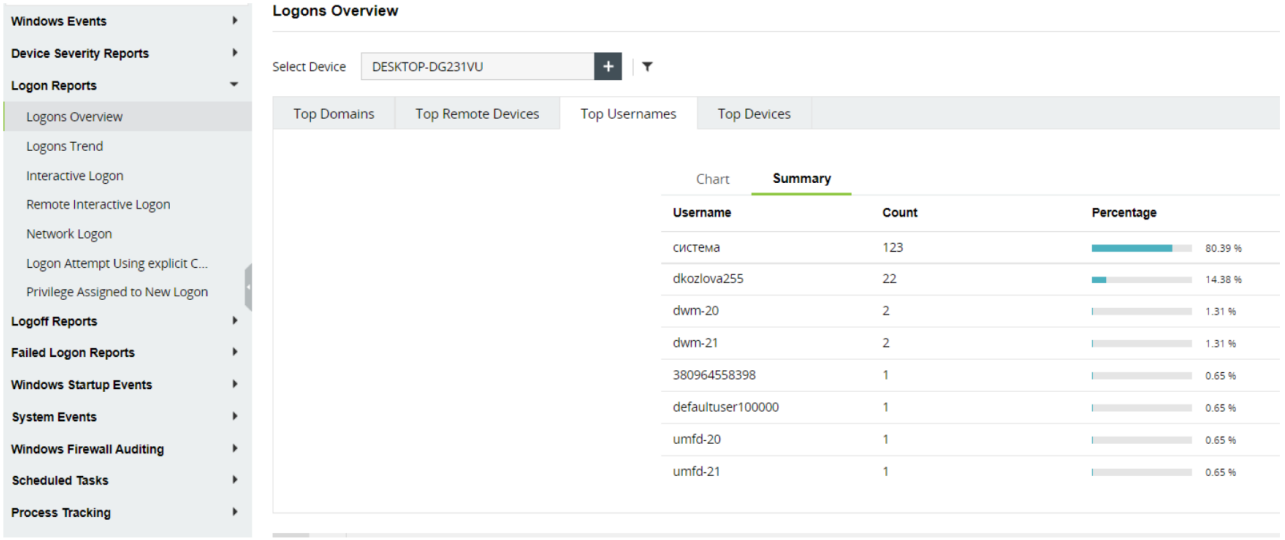

Рис. 3.22. Статистичний огляд авторизацій за користувачами

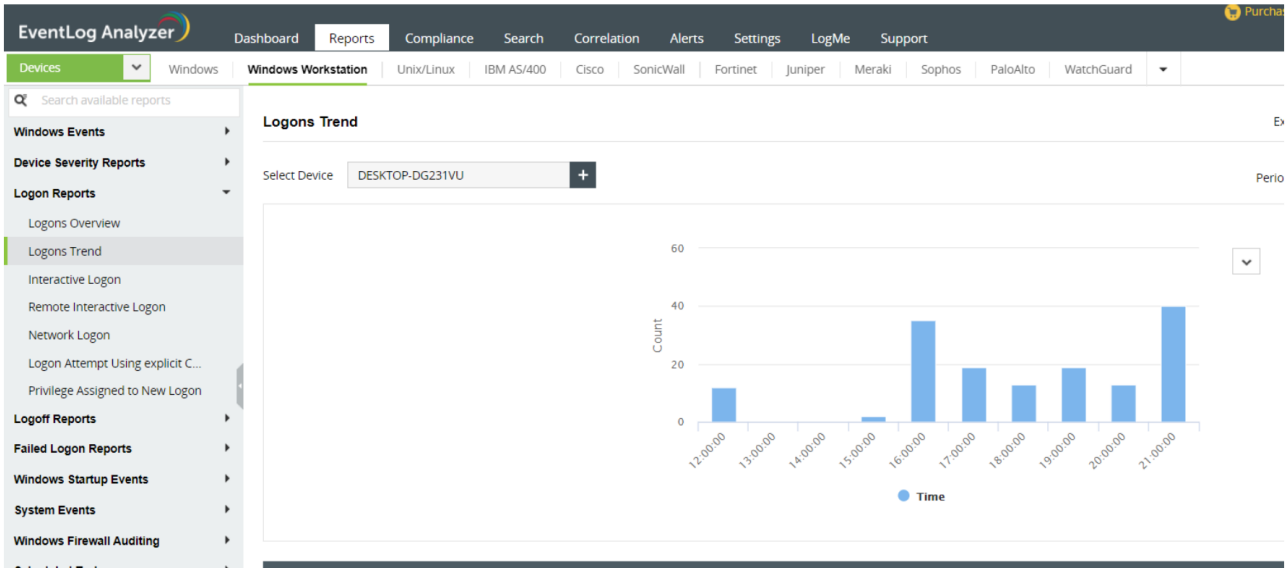

Рис. 3.23. Динаміка авторизацій у системі за часовими інтервалами

Окрім загальної інформації про вдалі входи в систему, у звітності також доступна статистика невдалих спроб авторизації. Цей функціонал дозволяє визначити причини відмов у доступі – наприклад, неправильний пароль, заблокований обліковий запис чи інші порушення. Такий аналіз є корисним для виявлення потенційних загроз або спроб несанкціонованого доступу. Приклад такої аналітики представлено на рисунку 3.24, де наведено деталізацію невдалих авторизацій.

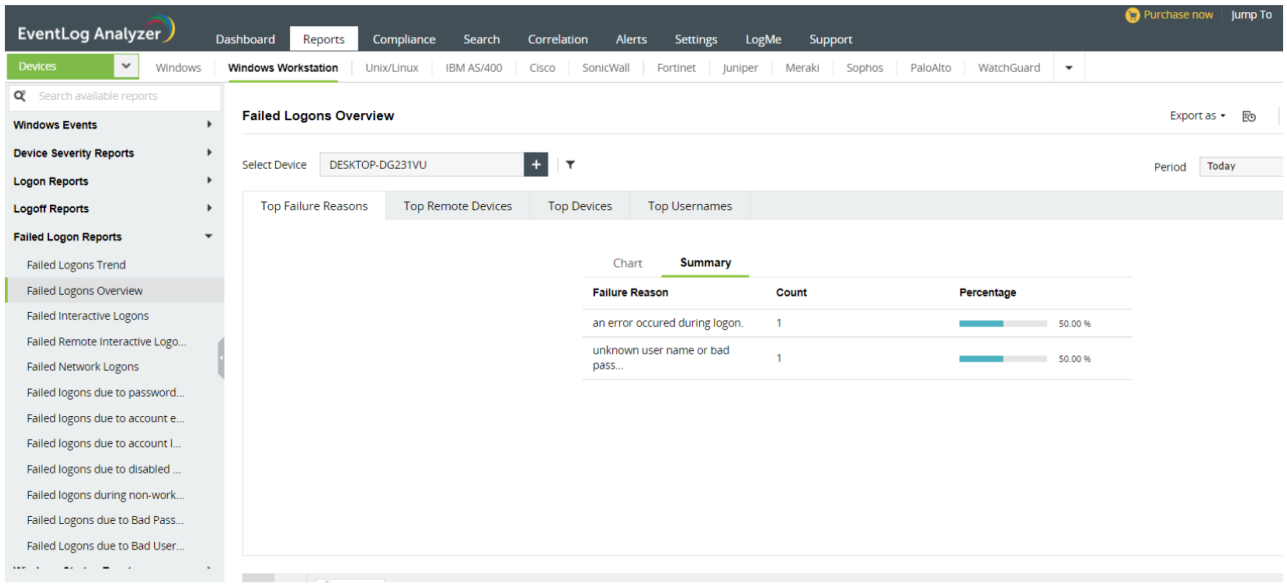

Рис. 3.24. Аналітика невдалих спроб входу в систему

Система також надає можливість аналізувати події, пов’язані з модифікаціями програмного забезпечення. Зокрема, доступна інформація про запуск і завершення роботи будь-яких сервісів, ініційованих користувачами, зміни часу на системі, а також редагування правил міжмережевих екранів. Цей тип моніторингу особливо важливий у контексті виявлення дій з підвищеними привілеями чи потенційно небажаних змін у критичних компонентах системи.

Для серверів на базі Linux можна активувати контроль за змінами у файловій системі, а також відстеження авторизацій через SSH або FTP. Окрім цього, адміністратор має змогу гнучко налаштувати перелік журналів, з яких здійснюється збір інформації.

Усе це відображено на рисунку 3.25, де представлено відповідний розділ моніторингу подій у середовищі EventLog Analyzer [39].

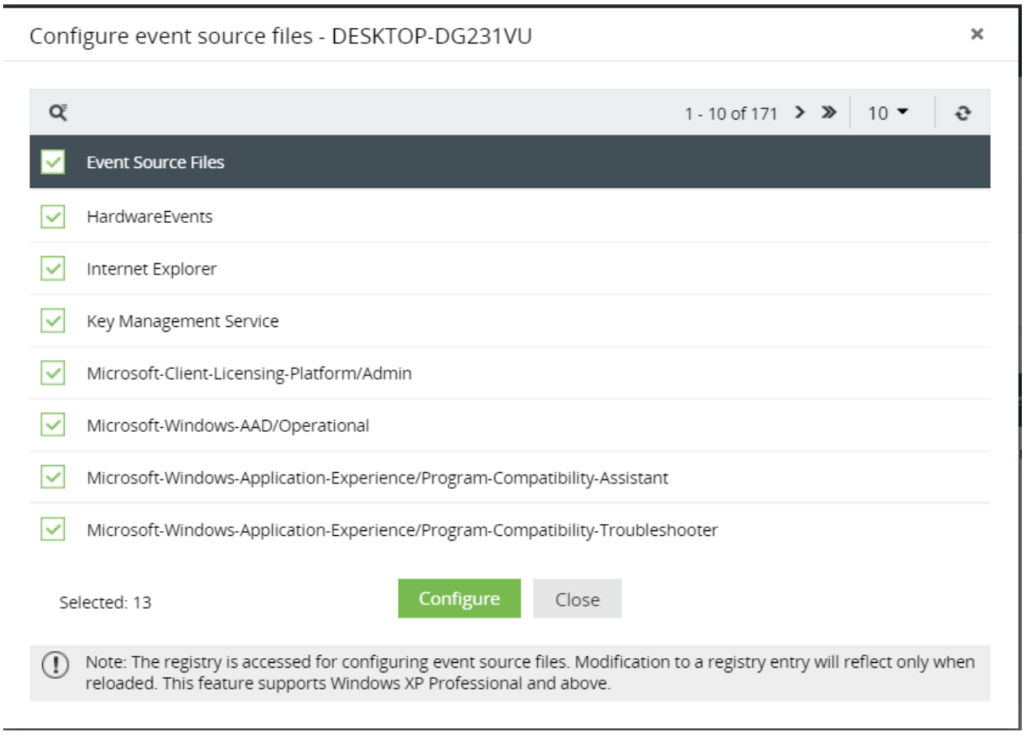

Рис. 3.25. Відстеження подій запуску, змін часу та конфігурацій

Вкладка Alerts надає користувачам можливість налаштування власних сповіщень про події, які відбуваються в системі. Адміністратор може самостійно визначити умови спрацювання алерту, вказати текст повідомлення, тип події, конкретний пристрій чи категорію логів. Завдяки цьому система оповіщення стає

максимально гнучкою та адаптованою до вимог конкретного середовища.

Приклад інтерфейсу створення сповіщень наведено на рисунку 3.26, який ілюструє процес конфігурації алертів відповідно до заданих критеріїв.

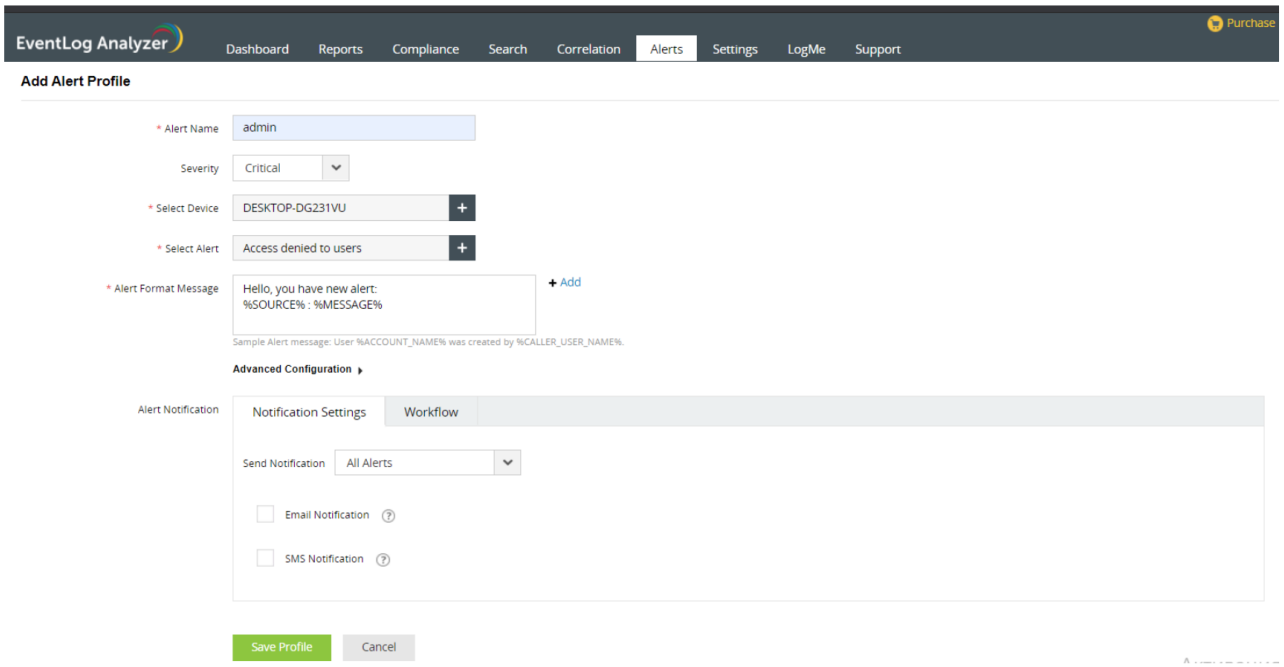

Рис. 3.26. Створення власного сповіщення в системі EventLog Analyzer

Система також дозволяє формувати кастомні звіти, які відповідають конкретним завданням або потребам адміністратора. У рамках практичного використання було створено індивідуальний звіт, який відслідковує події, пов’язані з доступом до файлів на локальному комп’ютері, а також факти їхнього видалення.

Цей звіт дозволяє ідентифікувати, хто і коли здійснив доступ або зміни до критичних файлів, що є важливим з точки зору аудиту та інформаційної безпеки.

Візуальні приклади реалізації такого звіту представлено на рисунках 3.27–3.30, які демонструють процес його побудови, застосування фільтрів та фінальний результат у вигляді зведення подій.

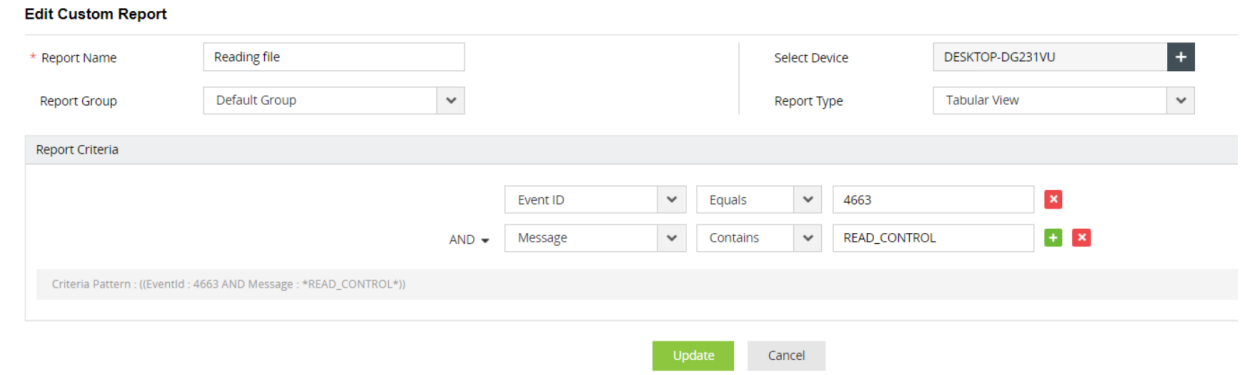

Рис. 3.27. Вибір параметрів звіту для відстеження дій з файлами

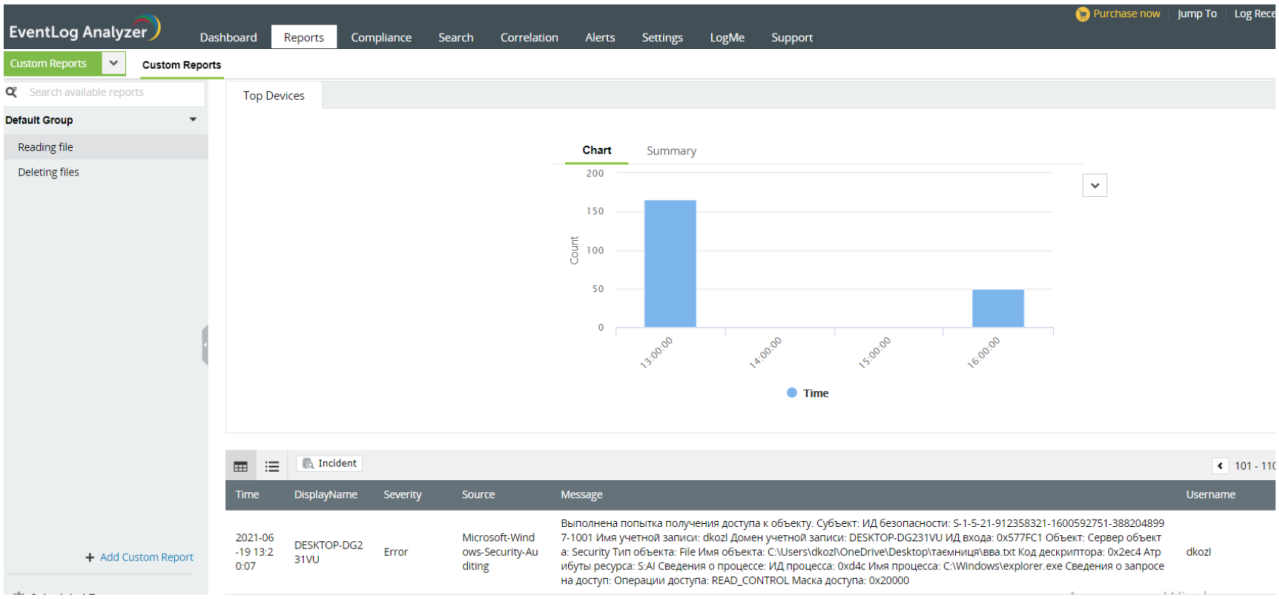

Рис. 3.28. Налаштування умов фільтрації для подій доступу до файлів

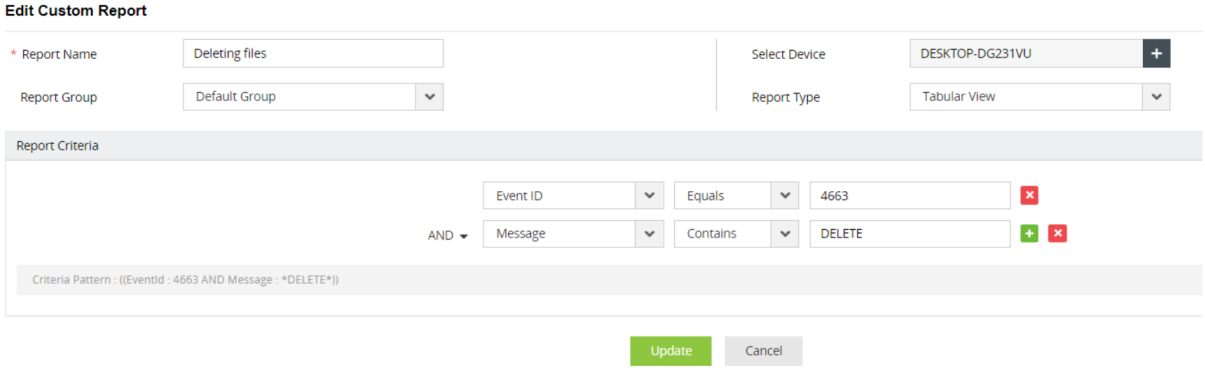

Рис. 3.29. Відображення результатів запиту: доступ до локальних файлів

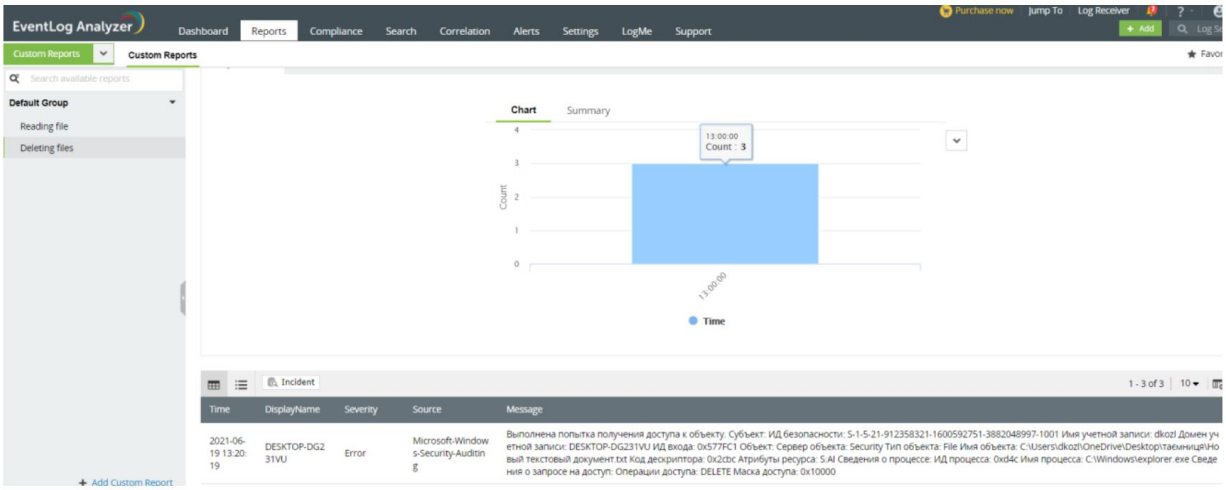

Рис. 3.30. Події видалення файлів у згенерованому звіті

Після розгортання та налаштування системи можна зробити висновок, що SIEM-рішення, зокрема AlienVault OSSIM, можуть ефективно використовуватися під час побудови комплексної системи захисту інформації відповідно до вимог Постанови Кабінету Міністрів України №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

Реалізоване рішення відповідає низці ключових положень цієї постанови, а саме [40]:

Пункт 6 – забезпечення захисту від несанкціонованого та неконтрольованого доступу до службової або конфіденційної інформації;

Пункт 7 – надання доступу до інформації виключно ідентифікованим та авторизованим користувачам;

Пункт 11 – обов’язкова реєстрація користувачів, з можливістю перегляду результатів їх ідентифікації й автентифікації, а також фіксації дій з обробки інформації чи спроб несанкціонованого доступу;

Пункт 15 – здійснення контролю за цілісністю програмного забезпечення, що використовується в інформаційній інфраструктурі підприємства.

Таким чином, впровадження OSSIM дозволяє не лише централізовано керувати подіями безпеки, а й формалізувати процеси відповідно до державних вимог у сфері захисту інформації.

3.4 Перспективи розвитку аудитів безпеки в малих і середніх компаніях

З огляду на зростаючу кількість кіберзагроз та активне впровадження цифрових технологій, аудит інформаційної безпеки стає дедалі важливішим елементом захисту навіть для малих і середніх підприємств (МСП). Попри обмежені ресурси, саме ці компанії дедалі частіше стають об’єктами атак через відносно низький рівень захищеності. У цьому контексті спостерігається підвищений інтерес до впровадження доступних SIEM-рішень, таких як OSSIM, що дозволяють автоматизувати виявлення інцидентів, проводити централізований моніторинг і забезпечувати відповідність нормативним вимогам [41].

Перспективним напрямом є інтеграція аудитів безпеки з хмарними сервісами, що дозволяє скоротити витрати на інфраструктуру та обслуговування. Крім того, розвиток open-source інструментів відкриває нові можливості для побудови гнучких і масштабованих рішень без значних капіталовкладень. Зростає також значення автоматизованих аудитів, які завдяки машинному навчанню здатні аналізувати великі обсяги логів у реальному часі та виявляти нетипові події [41].

У майбутньому очікується, що аудит інформаційної безпеки в МСП стане не просто періодичним заходом, а невід’ємною частиною бізнес-процесів, що дозволить суттєво підвищити стійкість компаній до кіберзагроз навіть за обмеженого бюджету.

Висновки до розділу 3

Розглянуто сучасні підходи до впровадження аудиту інформаційної безпеки з акцентом на практичну доцільність та гнучкість для різних типів організацій. Зокрема, аналізується ефективність аутсорсингових моделей та співпраці з постачальниками керованих сервісів безпеки (MSSP), що дозволяє

компаніям зменшити витрати, отримати доступ до висококваліфікованих фахівців та зосередитись на основному бізнесі. Також акцент зроблено на можливостях open-source інструментів, які, завдяки відкритому коду та активним спільнотам, забезпечують гнучке та економічно вигідне рішення для проведення аудиту. Окрема увага приділяється побудові безпечної IT-інфраструктури на основі SIEM-систем, які надають змогу оперативно виявляти інциденти, аналізувати ризики та реагувати на загрози в режимі реального часу. Нарешті, розкрито перспективи розвитку аудитів безпеки в малому та середньому бізнесі, де зростає попит на цифрову стійкість, з’являються нові інструменти й сервіси, що роблять процеси кіберзахисту доступнішими для ширшого кола компаній.

ВИСНОВКИ

Розглянуто теоретичні засади інформаційної безпеки, поняття аудиту та його роль у забезпеченні належного рівня захисту інформаційних активів. Особливу увагу приділено системам управління інформаційною безпекою (СУІБ), які є основою для реалізації системного підходу до забезпечення конфіденційності, цілісності та доступності інформації в організації.

Проаналізовано специфічні виклики, з якими стикаються малі та середні компанії при впровадженні систем безпеки. До них відносяться обмежені фінансові, кадрові та технічні ресурси, які значною мірою ускладнюють реалізацію повноцінних моделей управління ризиками та відповідності міжнародним стандартам. Це обґрунтовує необхідність адаптації існуючих підходів до потреб МСП.

Вивчено ключові методи аналізу та оцінки ризиків, серед яких особливої уваги заслуговують моделі OCTAVE, ISO 31000, FAIR та CRAMM. Кожен із цих підходів має свої переваги та сфери застосування, проте саме OCTAVE та ISO 31000 найкраще відповідають можливостям і реаліям малих організацій завдяки гнучкості та адаптивності.

Розглянуто міжнародні стандарти у сфері інформаційної безпеки, такі як ISO/IEC 27001, ISO/IEC 15408 та NIST SP 800-53. Вони формують нормативну основу для побудови ефективної системи безпеки, однак потребують глибокого аналізу й адаптації перед впровадженням у малих компаніях.

Розглянуто ключові методи та інструменти, що використовуються на практиці для реалізації ефективного аудиту інформаційної безпеки, зокрема в умовах обмежених ресурсів, характерних для малих та середніх компаній.

Проаналізовано підходи до планування аудиту, акцентуючи увагу на необхідності адаптації процесу до доступних можливостей організації. Було показано, що навіть при мінімальних витратах можна досягти базового рівня безпеки шляхом визначення критичних активів, складання чек-листів та застосування простих і структурованих процедур.

Розглянуто основні інструменти автоматизованої оцінки загроз, такі як SIEM-системи, IDS/IPS та сканери вразливостей (зокрема OpenVAS). Їх поєднане використання забезпечує комплексний підхід до моніторингу, виявлення атак та оцінювання стану безпеки, що особливо важливо для компаній, які не мають власного підрозділу кібербезпеки.

Приділено сучасним методикам аутентифікації та управління доступом: багатофакторній аутентифікації (MFA), системам IAM та інфраструктурі відкритих ключів (PKI). Зазначено, що навіть за обмежених ресурсів компанії можуть ефективно реалізувати ці механізми за допомогою відкритого ПЗ або хмарних рішень, що значно підвищує загальний рівень захищеності.

Розглянуто практичні аспекти впровадження аудитів інформаційної безпеки, зокрема за допомогою сучасних інструментів і підходів. Особливу увагу приділено аутсорсинговим моделям та використанню MSSP (Managed Security Service Provider), що дає змогу малим і середнім підприємствам оптимізувати витрати та отримати кваліфіковану експертизу у сфері безпеки без створення внутрішнього IT-відділу.

Продемонстровано ефективність впровадження open-source рішень, таких як AlienVault OSSIM, для побудови систем моніторингу подій безпеки. Такі рішення дозволяють автоматизувати аудит, зменшити навантаження на персонал та забезпечити відповідність чинним нормативним вимогам. Також наголошено на важливості формування безпечної інфраструктури, заснованої на проактивному виявленні інцидентів та швидкому реагуванні.

Розроблено практичні рекомендації, які можуть бути адаптовані до потреб підприємств різного масштабу. Перспективи розвитку аудитів безпеки в МСП пов’язані з подальшою автоматизацією процесів, хмарною інтеграцією та впровадженням доступних технологій, що дозволяють підвищити рівень захищеності навіть за умов обмежених ресурсів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурцев В. Внутрішній аудит компанії. Круглий стіл. 2004. № 3. С. 19–24.
2. Білуха М. Т. Курс аудиту : підруч. Київ: Вища школа : Знання, 1998. 573 с. ISBN 5-11-004719-7.
3. Kimachia K. What Is Network Security? Definition, Types, and Benefits. Enterprise Networking Planet. URL: https://www.enterprisenetworkingplanet.com/security/network-security/ (дата звернення: 25.04.2025).
4. Computer Security Institute. 2010/2011 Computer Crime and Security Survey. 2011.
5. COBIT Foundation Certificate. ISACA. URL: https://www.isaca.org/credentialing/cobit-foundation (дата звернення: 25.04.2025).
6. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. 2022. 23 p.
7. ISO 31000:2018. Risk management – Guidelines. 2018. 16 p.
8. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. 2020. 502 p.
9. ISO/IEC 15408. Information technology – Security techniques – Evaluation criteria for IT security (Common Criteria). 2009. Part 1–3.
10. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). – 2016.
11. European Union Agency for Cybersecurity (ENISA). Cybersecurity for SMEs. 2023. URL: https://www.enisa.europa.eu (дата звернення: 25.04.2025).
12. OWASP. OWASP Top 10 : Web Application Security Risks. 2023. URL: https://owasp.org (дата звернення: 25.04.2025).
13. Alberts C., Dorofee A. Managing Information Security Risks : The OCTAVE Approach. Boston : Addison-Wesley, 2002. 471 p.

14. FAIR Institute. Introduction to the Factor Analysis of Information Risk (FAIR) Model. 2022.

15. British Standards Institute. BS ISO/IEC 27005:2018. Risk Management in Information Security. London : BSI, 2018. 56 p.

16. Microsoft. Identity and Access Management Overview. 2023. URL: https://learn.microsoft.com (дата звернення: 25.04.2025).

17. Google Cloud. Best Practices for MFA. 2023. URL: https://cloud.google.com (дата звернення: 25.04.2025).

18. OpenSSL Project. Cryptography and PKI Tools. 2024. URL: https://www.openssl.org (дата звернення: 25.04.2025).

19. Whitman M. E., Mattord H. J. Principles of Information Security. 7th ed. Boston : Cengage, 2022. 656 p.

20. Stallings W. Network Security Essentials : Applications and Standards. 6th ed. Boston : Pearson, 2021. 544 p.

21. Yakymenko I., Kasyanchuk M., Nykolajchuk Ya. Matrix Algorithms of Processing of the Information Flow in Computer Systems Based on Theoretical and Numerical Krestenson’s Basis. Proceedings of the X–th International Conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET–2010). L’viv–Slavske, 2010. P. 408–410.

22. Nykolaychuk Ya. M., Kasianchuk M. M., Yakymenko I. Z. Theoretical Foundations of the Modified Perfect Form of Residue Number System. Cybernetics and Systems Analysis. 2016. P. 219–223.

23. Lenstra H. W. Divisors in Residue Classes. Mathematics of Computation. 1984. Vol. 42, No. 165. P. 331–340.

24. Lakhani G. Some Fast Residual Arithmetic Adders. International Journal of Electronics. 1994. P. 225–240.

25. Khanna R. How to Use Elasticsearch, Logstash and Kibana to Visualise Logs in Python in Realtime. URL: https://www.freecodecamp.org/news/how-to-use-elasticsearch-logstashand-kibana-to-visualise-logs-in-python-in-realtime-acaab281c9de/ (дата звернення: 25.04.2025).

26. IBM QRadar Security Intelligence Platform (NDcPP21) Security Target. January 15, 2020. 32 p.

27. Santos O., Stuppi J. CCNA Security 210-260 Official Cert Guide : CCNA Sec 210-260 OCG. Indianapolis : Cisco Press, 2015. 700 p.

28. Santos O., Muniz J., De Crescenzo S. CCNA Cyber Ops SECFND# 210-250 Official Cert Guide. Indianapolis : Cisco Press, 2017. 672 p.

29. Messier R. CEH V10 Certified Ethical Hacker Study Guide. Indianapolis : John Wiley & Sons, 2019. 584 p.

30. Warsinske J., Graff M., Henry K., Hoover C., Malisow B., Murphy S., Vasquez M. The Official (ISC)² Guide to the CISSP CBK Reference. Indianapolis : John Wiley & Sons, 2019. 928 p.

31. ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management. 2018. 56 p.

32. ISO/IEC 27011:2016. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations. 2016. 31 p.

33. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. 2013. 23 p.

34. ISO/IEC 27006:2015. Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems. 2015. 35 p.

35. Каменська Т. О. Внутрішній аудит : сучасний погляд Київ: ДП «Інформаційно-аналітичне агентство», 2010. 491 с.

36. Міжнародний стандарт аудиту 315 «Ідентифікація та оцінка ризиків суттєвих викривлень через розуміння суб'єкта господарювання і його середовища». URL: http://apu.com.ua/files/temp/Ukr-block_T1-2010.pdf (дата звернення: 25.04.2025).

37. GAAP: Standards and Rules for Accountants official site. URL: https://www.investopedia.com/terms/g/gaap.asp (дата звернення: 25.04.2025).

38. Shulman R. D. Teach. Innovate. Inspire. Every which way. URL: https://www.apple.com/education/higher-education/ (дата звернення: 25.04.2025).

39. Голубничий Д. Ю., Коломійцев О. В., Третяк В. Ф., Рязанін С. Г. Технології аудиту кібербезпеки інформаційних систем. Scientific Collection «InterConf» : Proceedings of the 7th International Scientific and Practical Conference «Challenges in Science of Nowadays», November 26–28, 2020, Washington, USA. EnDeavours Publisher, 2020. P. 333–342.

40. Pasquini A., Galiè E. COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process. Proceedings of FIKUSZ ’13. 2013. P. 67–76.

41. Савченко В. Я., Зотов В. О., Кириленко С. А. та ін. Аудит : навч.-метод. посіб. для самост. вивч. Київ : КНЕУ, 2003. 268 с.