МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “АНАЛІЗ ТА ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ ТА ІНСТРУМЕНТІВ АУДИТУ ІНФОРМАЦІЙНОЇ 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

_____ Данило ЄЛЬЧАНІНОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Данило ЄЛЬЧАНІНОВ
Ім’я, ПРІЗВИЩЕ

Керівник: Михайло ЗАПОРОЖЧЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____
Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____” _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Єльчанінову Данилу Олексійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Аналіз та оцінка ефективності методів та інструментів аудиту інформаційної безпеки”,
керівник кваліфікаційної роботи ЗАПОРОЖЧЕНКО Михайло
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій "Про закріплення тем випускних кваліфікаційних робіт та призначення наукових керівників на 2023-2024 н.р. за студентами першого (бакалаврського) рівня вищої освіти". № 36 від 27.02.24

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *методика аудиту інформаційної безпеки, методи та інструменти аудиту інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1. Провести аналіз регуляторного середовища у сфері аудиту інформаційної безпеки.
   4.2. Дослідити алгоритм та методи аудиту інформаційної безпеки.
   4.3. Провести порівняльний аналіз інструментів аудиту інформаційної безпеки.
   4.4. Розробити рекомендації щодо вдосконалення методів аудиту інформаційної безпеки.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз регуляторного середовища у сфері аудиту інформаційної безпеки.	08.04.2024	
4.	Дослідження алгоритму та основних характеристик методів аудиту інформаційної безпеки.	22.04.2024	
5.	Порівняльний аналіз інструментів аудиту інформаційної безпеки, оцінка їх ефективності та розробка рекомендацій.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ЕК.	__.06.2024	

Здобувач вищої освіти _____ Данило ЄЛЬЧАНІНОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Єльчанінов Д.О до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “Аналіз та оцінка ефективності методів та інструментів аудиту інформаційної безпеки ”

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ЄЛЬЧАНІНОВ Данило у кваліфікаційній роботі провів аналіз регуляторного середовища у сфері аудиту інформаційної безпеки, дослідив алгоритм та методи аудиту інформаційної безпеки, провів порівняльний аналіз інструментів аудиту інформаційної безпеки, розробив практичні рекомендації за темою дослідження.

ЄЛЬЧАНІНОВ Данило показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ЄЛЬЧАНІНОВА Данила на оцінку “_____” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Єльчанінов Д.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Єльчанінова Данила
на тему “Аналіз та оцінка ефективності методів та інструментів аудиту інформаційної безпеки ”

Актуальність. З розвитком технологій і збільшенням кількості цифрових загроз, організації стикаються з необхідністю постійного оновлення та вдосконалення заходів забезпечення інформаційної безпеки. Аудит дозволяє перевірити ефективність впроваджених заходів, виявити потенційні проблеми та вразливості, а також визначити шляхи їх вирішення. Крім того, з появою нових законодавчих вимог щодо захисту персональних даних, аудит інформаційної безпеки стає необхідним елементом для дотримання вимог цих стандартів. Таким чином, актуальність аудиту інформаційної безпеки виходить далеко за межі технічних аспектів і стає стратегічним фактором успіху для будь-якої організації. З огляду на зазначене дослідження методів та інструментів аудиту інформаційної безпеки є актуальним науковим завданням.

Позитивні сторони.

1. У роботі детально досліджено методи та інструменти аудиту інформаційної безпеки, проведено їх порівняльний аналіз.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Автор опрацював значну джерельну базу: 45 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо вдосконалення методів аудиту інформаційної безпеки та вибору відповідних інструментів.

Недоліки.

1. Доцільно було б приділити більше уваги вивченню критеріїв та показників для оцінки ефективності впроваджуваних методів та інструментів аудиту.

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

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

Рецензент:
_____ _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена аналізу та оцінці ефективності методів та інструментів аудиту інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 16 рисунків, висновків і списку використаних джерел із 45 найменувань. Загальний обсяг роботи становить 69 аркушів, з яких 4 аркуши займають перелік умовних скорочень та список використаних джерел.

Метою роботи є проведення порівняльного аналізу та оцінка ефективності методів та інструментів аудиту інформаційної безпеки.

Об'єктом дослідження є методи та інструменти аудиту ІБ.

Предмет дослідження – теоретичні та практичні аспекти оцінювання ефективності методів та інструментів аудиту інформаційної безпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до аудиту інформаційної безпеки.

Як результат у роботі проведено дослідження алгоритму аудиту інформаційної безпеки, аналіз особливостей застосування інструментів аудиту інформаційної безпеки, досліджено основні методи аудиту; проведено порівняльний аналіз інструментів аудиту інформаційної безпеки; розроблено практичні рекомендації щодо вдосконалення методів аудиту інформаційної безпеки.

Галузь застосування. Розроблені підходи можуть бути використані при формування програми та плану аудиту, при проведенні внутрішніх аудитів інформаційної безпеки, при підготовці до сертифікації системи управління інформаційною безпекою.

Ключові слова: АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ОЦІНКА ЕФЕКТИВНОСТІ ІНСТРУМЕНТІВ АУДИТУ.

ABSTRACT

The qualification work is devoted to the analysis and evaluation of the effectiveness of information security audit methods and tools. The work consists of an introduction, three chapters containing 16 figures, conclusions and a list of used sources from 45 titles. The total volume of the work is 69 sheets, of which 4 sheets are occupied by a list of conventional abbreviations and a list of used sources.

The purpose of the study is to conduct a comparative analysis and evaluate the effectiveness of information security audit methods and tools.

The object of the research is information security audit methods and tools.

The subject of the study is theoretical and practical aspects of evaluating the effectiveness of information security audit methods and tools.

Research methods. To solve the above-mentioned scientific task, the work uses methods of analysis and synthesis, comparison, classification, expert assessment, and a systematic approach to information security audit.

As a result, the study examines the algorithm of information security audit, analyses the features of information security audit tools, investigates the main audit methods; conducts a comparative analysis of information security audit tools; develops practical recommendations for improving information security audit methods.

Field of application. The developed approaches can be used in the development of an audit program and plan, in conducting internal information security audits, and in preparing for the certification of an information security management system.

Keywords: INFORMATION SECURITY AUDIT, INFORMATION SECURITY MANAGEMENT SYSTEM, AUDIT TOOLS EFFECTIVENESS EVALUATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ІС	Інформаційна система
ПЗ	Програмне забезпечення
СУВ	Система управління вразливостями
СУІБ	Система управління інформаційною безпекою

ВСТУП

Актуальність теми. У сучасному світі, де цифрові технології проникають у всі сфери життя, питання захисту інформації набувають особливої актуальності та значущості. Ростуть загрози для конфіденційності, цілісності та доступності даних, що зумовлює необхідність впровадження ефективних заходів забезпечення інформаційної безпеки. Аудит інформаційної безпеки стає важливим інструментом для перевірки, аналізу та оцінки результативності та ефективності функціонування впроваджених заходів захисту та системи управління інформаційною безпекою в цілому. Для забезпечення впевненості у результатах аудиту інформаційної безпеки доцільно проаналізувати різні підходи до його проведення та оцінки його результативності.

З огляду на зазначене дослідження методів та інструментів аудиту інформаційної безпеки та оцінка їх ефективності є актуальним науковим завданням.

Мета роботи полягає у проведенні порівняльного аналізу та оцінці ефективності методів та інструментів аудиту інформаційної безпеки.

Об'єктом дослідження є методи та інструменти аудиту інформаційної безпеки.

Предмет дослідження **–** теоретичні та практичні аспекти оцінювання ефективності методів та інструментів аудиту інформаційної безпеки.

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

1. Провести аналіз регуляторного середовища у сфері інформаційної безпеки.
2. Проаналізувати алгоритм проведення аудиту інформаційної безпеки.
3. Проаналізувати методи та інструменти аудиту інформаційної безпеки.
4. Провести порівняльну характеристику інструментів аудиту інформаційної безпеки.
5. Розробити рекомендації щодо вдосконалення методів аудиту інформаційної безпеки.

Методи дослідження. Вирішення завдань, поставлених у дослідженні, здійснювалося за допомогою методів теоретичного синтезу та системного аналізу, які застосовувалися при вивченні методів та інструментів аудиту інформаційної безпеки. Аналіз та оцінка ефективності методів та інструментів аудиту інформаційної безпеки проводились з використанням структурного аналізу , порівняння даних та діаграм.

Практичне значення одержаних результатів. Використання отриманих результатів дослідження дозволить здійснити обґрунтований вибір методів та інструментів аудиту інформаційної безпеки, що є важливим компонентом управління інформаційною безпекою організації.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ПРОВЕДЕННЯ АУДИТУ ІБ

1.1 Визначення ролі аудиту в забезпеченні ІБ організації

Роль аудиту в забезпеченні ІБ організації надзвичайно важлива і багатогранна. Аудити ІБ охоплюють систематичний процес оцінки, перевірки та контролю механізмів захисту інформації, які використовуються в організації. Основною метою є виявлення слабких місць, загроз і вразливостей у системах і процесах, якими зловмисники можуть скористатися для отримання несанкціонованого доступу до конфіденційних даних.

По-перше, аудит допомагає організаціям оцінити ефективність їхніх поточних заходів безпеки. Аудитори ретельно перевіряють політику, процедури, технологічні рішення та поведінкові аспекти, пов’язані з ІБ. Це включає перевірку конфігурацій мережевих пристроїв, серверів, баз даних, систем контролю доступу та інших компонентів ІТ-інфраструктури. Завдяки цій комплексній оцінці організації можуть отримати об’єктивну перспективу щодо стану своєї ІБ та визначити, чи вона відповідає встановленим стандартам і нормативним вимогам. Ця оцінка має вирішальне значення, оскільки вона забезпечує орієнтир для вимірювання стану безпеки організації в порівнянні з найкращими галузевими практиками та вимогами відповідності [1].

Окрім виявлення технічних вразливостей, аудити сприяють розвитку культури безпеки в організації. У процесі аудиту часто беруть участь співробітники, завдяки чому вони підвищують усвідомлення важливості ІБ та їх особистої відповідальності за захист даних. Така підвищена обізнаність зменшує ймовірність людської помилки, що є поширеною причиною витоку інформації. Залучаючи персонал до процесу аудиту, організації можуть сприяти почуттю власності та підзвітності серед працівників, що є важливим для підтримки надійних практик ІБ.

Важливою складовою процесу аудиту є формулювання рекомендацій і плану дій щодо підвищення ІБ. Після аналізу аудитори надають детальний звіт

із описом виявлених недоліків і пропозицією конкретних заходів щодо їх усунення. Ці рекомендації можуть включати оновлення ПЗ, покращення процедур контролю доступу, покращення шифрування даних або проведення додаткового навчання персоналу. План дій служить для організації дорожньою картою для систематичного усунення вразливостей і зміцнення своєї безпеки. Реалізація цих рекомендацій може призвести до значного покращення здатності організації захищати конфіденційну інформацію та пом’якшувати потенційні загрози.

Також аудит відіграє ключову роль у забезпеченні дотримання законодавчих та нормативних вимог. У багатьох галузях промисловості діють спеціальні правила, що регулюють зберігання та обробку конфіденційної інформації. Регулярні аудити дозволяють організаціям забезпечити дотримання цих вимог, уникаючи таким чином штрафів, санкцій і шкоди репутації. Дотримання таких нормативних актів, як Загальний регламент захисту даних (GDPR), Закон про перенесення та підзвітність медичного страхування (HIPAA) і Закон Сарбейнса-Окслі (SOX) є не лише юридичним зобов’язанням, але й важливим аспектом підтримки довіри зацікавлених сторін. Аудити допомагають організаціям продемонструвати свою відданість захисту конфіденційної інформації та підтримці прозорості своїх операцій.

Крім того, аудит забезпечує механізм постійного вдосконалення ІБ. Регулярно оцінюючи заходи безпеки та визначаючи області для покращення, організації можуть адаптуватися до мінливого середовища загроз. Кіберзагрози постійно змінюються, і регулярно з’являються нові вразливості. Регулярні аудити гарантують, що організації залишаються пильними та активними у вирішенні потенційних ризиків. Цей підхід постійного вдосконалення допомагає організаціям випереджати кіберзагрози та підтримувати надійну безпеку з часом.

1.2 Сутність, цілі та принципи аудиту ІБ

Аудит ІБ є невід'ємною частиною загальної стратегії безпеки організації. Він пропонує комплексний підхід до виявлення та зменшення ризиків, підвищення обізнаності співробітників щодо важливості захисту інформації, забезпечення дотримання вимог законодавства та підтримки високого рівня довіри з боку клієнтів і партнерів [2]. За допомогою аудитів організації можуть не тільки захистити свої дані від загроз, але й підвищити свою конкурентоспроможність на ринку, демонструючи високий рівень відповідальності та професіоналізму в ІБ. Систематично усуваючи вразливості та постійно вдосконалюючи заходи безпеки, організації можуть створити стійкий захист від кіберзагроз і захистити свої цінні інформаційні активи.

Аудит ІБ являє собою фундаментальний компонент управління ІБ в сучасних організаціях. Це передбачає систематичну оцінку, аналіз і перевірку заходів, спрямованих на захист інформаційних ресурсів від несанкціонованого доступу, зміни, втрати або знищення. Основною метою такого аудиту є виявлення вразливостей і недоліків у системах ІБ, надання рекомендацій щодо їх усунення та підвищення загальної безпеки організації.

Основна мета аудиту ІБ полягає в тому, щоб переконатися, що ІС організації відповідають відповідному законодавству, внутрішнім політикам і стандартам, таким як ISO/IEC 27001. Відповідність цим стандартам не тільки відповідає законодавчим і нормативним вимогам, але й демонструє відданість для підтримки надійної системи безпеки [3]. Крім того, аудит спрямований на запобігання потенційним загрозам та інцидентам, які можуть призвести до втрати конфіденційної інформації, фінансових втрат або шкоди репутації. Завчасно виявляючи та усуваючи вразливості, організації можуть зменшити ризики до того, як вони матеріалізуються у значні інциденти безпеки.

До того ж, аудит ІБ допомагає оптимізувати витрати, пов'язані із заходами ІБ, шляхом визначення зайвих або неефективних механізмів захисту. Ця оптимізація витрат має вирішальне значення, оскільки організації прагнуть

ефективно розподіляти свої ресурси, гарантуючи, що інвестиції в безпеку забезпечують максимальну цінність і ефективність.

Основними принципами аудиту ІБ є неупередженість, об'єктивність і систематична методологія. Аудитори повинні діяти незалежно, надаючи неупереджену оцінку стану ІБ. Ця незалежність має важливе значення для того, щоб результати аудиту були достовірними та вільними від будь-яких потенційних конфліктів інтересів. Збереження конфіденційності зібраних даних має вирішальне значення для запобігання несанкціонованому розголошенню, тим самим захищаючи конфіденційну інформацію організації під час і після процесу аудиту.

Системний підхід вимагає, щоб аудит охоплював усі аспекти ІБ, включаючи технічні, організаційні та процедурні заходи. Це всебічне охоплення гарантує, що жоден аспект безпеки організації не буде пропущено, дозволяючи ретельно оцінити її сильні та слабкі сторони.

Процес проведення аудиту ІБ включає кілька важливих етапів (рис. 1.1). Спочатку окреслюються цілі та обсяг аудиту, що дозволяє зосередитися на найважливіших аспектах безпеки. Визначення сфери допомагає зосередити зусилля на сферах, які є найбільш сприйнятливими до ризиків і мають найбільший вплив на загальну безпеку організації. Далі йде збір та аналіз інформації щодо існуючих заходів безпеки, політики та процедур. Цей етап передбачає проведення співбесід із співробітниками, перевірку документів, тестування ІС. Збір різноманітних джерел даних забезпечує цілісне уявлення про середовище безпеки організації.

На основі зібраної інформації складається розгорнутий звіт. У цьому звіті детально описано виявлені вразливості, оцінено їхній потенційний вплив і надано дієві рекомендації щодо їх пом'якшення. Рекомендації розроблено для усунення конкретних недоліків, враховуючи унікальний операційний контекст організації та схильність до ризику.

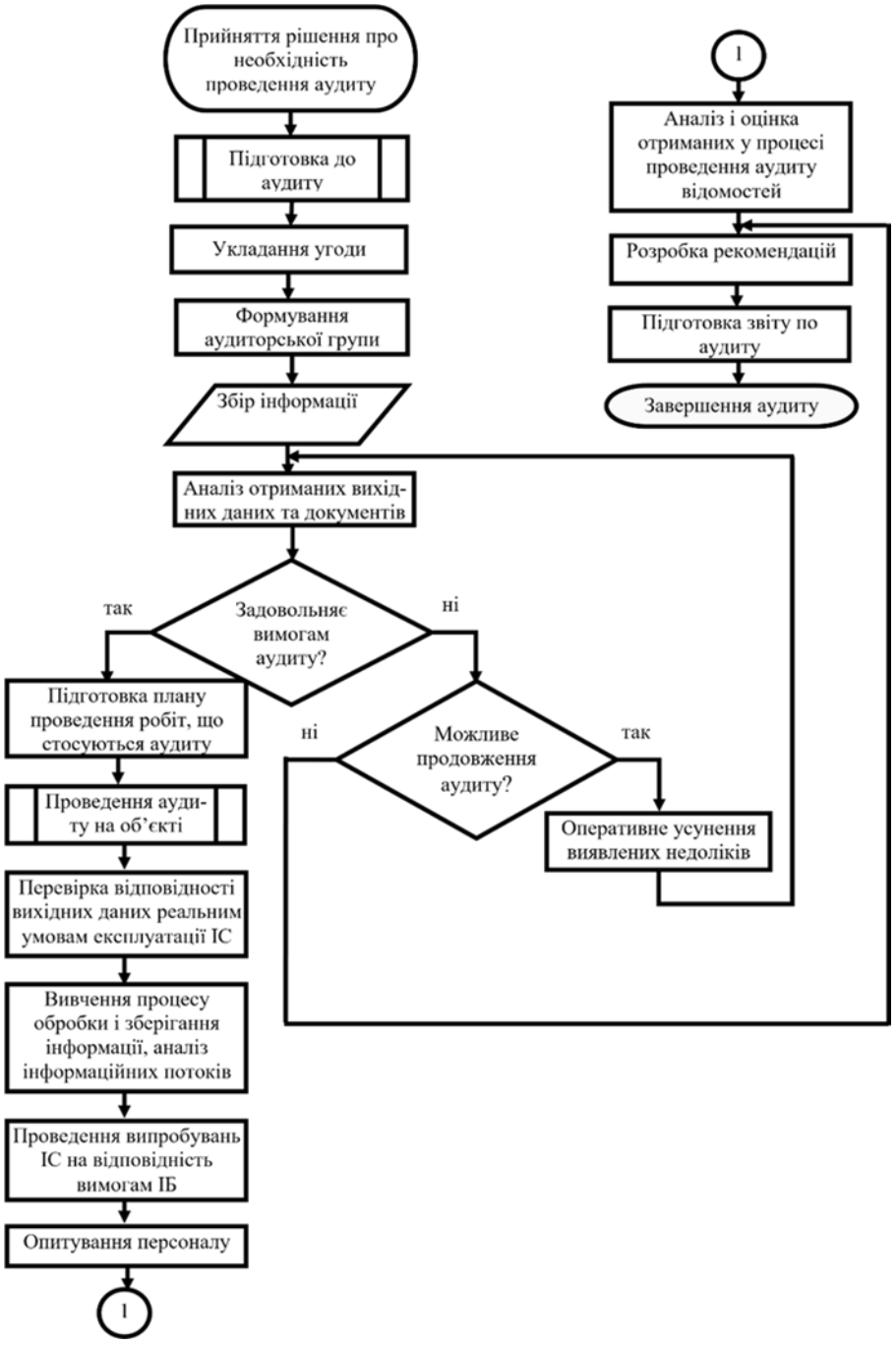

Рис. 1.1 Схема процесу аудиту безпеки ІС

Аудити ІБ мають стратегічне значення для організацій, оскільки забезпечують високий рівень захисту інформаційних ресурсів і дотримання найкращих практик ІБ. Регулярні перевірки підвищують обізнаність працівників щодо питань ІБ, сприяючи розвитку культури безпеки в організації. Вони також стимулюють постійне вдосконалення внутрішніх процесів, забезпечуючи розвиток заходів безпеки у відповідь на нові загрози та технологічний прогрес.

Крім того, вони сприяють стійкості організації проти зовнішніх і внутрішніх загроз. Виявляючи та усуваючи прогалини в безпеці, організації можуть покращити свою здатність запобігати, виявляти та реагувати на інциденти безпеки. Ця стійкість має вирішальне значення для підтримки безперервності бізнесу та захисту репутації та активів організації [6].

Підсумовуючи, аудит ІБ є життєво важливим інструментом для організацій, які прагнуть підтримувати надійні методи безпеки та гарантувати відповідність нормативним і галузевим стандартам. Систематично оцінюючи та вдосконалюючи свої заходи безпеки, організації можуть захистити свої інформаційні ресурси, оптимізувати інвестиції в безпеку та створити надійну безпеку, здатну протистояти різноманітним загрозам [4]. Регулярні та ретельні перевірки ІБ є невід'ємною частиною підтримки довіри зацікавлених сторін, захисту важливої інформації та досягнення довгострокового успіху бізнесу.

1.3 Аналіз регуляторного середовища у сфері аудиту ІБ

Сфера аудиту ІБ відзначається незмінним значенням у забезпеченні стабільності та надійності сучасних ІС. Ця важливість ще більше підкреслюється динамічним нормативним середовищем, яке постійно розвивається, в якому працюють аудитори ІБ. Оскільки технологічний прогрес продовжує змінювати ландшафт кібербезпеки, а організації все більше покладаються на цифрову інфраструктуру для зберігання конфіденційних даних і керування ними, нормативна база, що регулює аудит ІБ, повинна постійно адаптуватися для вирішення нових проблем і загроз.

Помітною тенденцією в поточному нормативному середовищі є посилення уваги до безпеки даних і захисту інформаційних ресурсів. Ця тенденція зумовлена визнанням критичної важливості захисту конфіденційних даних від кіберзагроз, витоку даних і несанкціонованого доступу. Відповідно, регуляторні органи вводять нові правила та стандарти, які розмежовують обов'язки та

практику аудиторів з ІБ, прагнучи підняти планку професіоналізму та компетентності в цій галузі [5].

Центральним елементом ефективного аудиту ІБ є встановлення надійних вимог до кваліфікації та сертифікації аудиторів. Ці вимоги служать основою для забезпечення того, щоб аудитори володіли необхідними знаннями, навичками та досвідом для проведення комплексних аудитів і точної оцінки рівня ІБ в організації. Встановлюючи високі стандарти кваліфікації аудиторів, регуляторні органи сприяють загальній ефективності та надійності аудитів ІБ.

Більше того, нормативне середовище для аудитів ІБ включає міжнародно визнані стандарти, такі як ISO/IEC 27001, NIST, SP-800 [5]. Це включення глобальних стандартів не лише сприяє послідовності та гармонізації практики аудиту, але також сприяє транскордонній співпраці та взаємному визнанню результатів аудиту. В епоху, коли підприємства працюють у глобальному масштабі, а дані перетинають міжнародні кордони, дотримання міжнародних стандартів стає обов’язковим для забезпечення єдиного та ефективного підходу до перевірок ІБ.

Незважаючи на успіхи, досягнуті в нормативно-правовій базі, залишаються проблеми, пов’язані зі швидким розвитком технологій і появою нових загроз безпеці. Динамічний характер кібербезпеки вимагає постійного оновлення та перегляду нормативних вказівок, що створює постійну проблему для регуляторів, щоб підтримувати відповідність і ефективність у нагляді за аудитами ІБ [6].

Крім того, міжнародна співпраця відіграє вирішальну роль у вирішенні складнощів аудиту ІБ, особливо для організацій, які здійснюють глобальні операції. Стандартизовані підходи до аудиту ІС у різних юрисдикціях не лише спрощують процеси аудиту, але й підвищують загальну стійкість організацій до ризиків кібербезпеки.

Підсумовуючи, нормативне середовище для аудитів ІБ характеризується своєю складністю, динамічністю та глобальною взаємопов’язаністю. Завдяки суворим кваліфікаційним вимогам, інтеграції міжнародних стандартів і

безперервній співпраці регуляторні органи прагнуть підтримувати цілісність і ефективність аудитів ІБ, що в кінцевому підсумку сприяє захисту та стійкості інформаційних активів у все більш цифровому світі.

Численні стандарти відіграють ключову роль у визначенні важливих вимог і найкращих практик для виконання аудитів ІБ в організаційних налаштуваннях. Серед цих стандартів наріжним каменем виступає ISO/IEC 27001:2022, який зосереджується на комплексній розробці, систематичному впровадженні, ефективному управлінні та постійному вдосконаленні СУІБ [1]. Цей стандарт працює в структурованій структурі, охоплюючи багатогранні методології для проведення оцінки ризиків, формулювання надійних політик і процедур ІБ та розробки складних механізмів контролю для постійного моніторингу та оцінки.

Паралельно, ISO/IEC 27002:2022 виділяється як незамінний ресурс, який надає докладні рекомендації та стратегічні ідеї для оркестрування ефективних практик управління ІБ в різних організаційних сферах. У цьому всеосяжному документі міститься спектр загальних принципів і прагматичних вказівок, що охоплюють сфери захисту активів, стратегічного управління доступністю, захисту конфіденційності, забезпечення цілісності даних, перевірки автентичності та зміцнення протоколів невідмовності. Дотримуючись детальних директив, викладених у ISO/IEC 27002:2022, організації можуть систематично зміцнювати свою ІБ, підвищуючи стійкість до безлічі кіберзагроз і вразливостей.

Крім того, структура COBIT [4] (контрольні цілі для інформаційних і суміжних технологій) постає як надійна модель управління, стратегічно розроблена для впорядкування аспектів управління та контролю ІТ в організаційних рамках. COBIT окреслює структурований підхід, розмежовуючи критичні процеси, процедурні рамки та необхідні засоби контролю, необхідні для забезпечення оптимальної відповідності мандатам ІБ та найкращим галузевим практикам. Завдяки прийняттю COBIT організації можуть культивувати культуру ефективного управління, зміцнюючи свої можливості для проактивного управління та пом’якшення ризиків ІБ.

Крім того, структура кібербезпеки NIST (Національний інститут стандартів і технологій) набуває надзвичайного значення, особливо в контексті посилення стійкості кібербезпеки в критичних секторах інфраструктури в Сполучених Штатах. Ця ретельно структурована структура охоплює багатогранну архітектуру, яка об’єднує основні управлінські елементи разом із комплексним набором вимог і стратегічних рекомендацій. Вони охоплюють цілісну ідентифікацію інформаційних активів, надійні механізми захисту, складні протоколи виявлення загроз, стратегії швидкого реагування на інциденти та стійкі структури відновлення. Дотримуючись принципів NIST Cybersecurity Framework, організації, що працюють у сферах критичної інфраструктури, можуть підвищити свою кіберстійкість, зміцнюючи захист від складних кіберзагроз і агресивних вторгнень.

Синергічна інтеграція цих основоположних стандартів служить основою для вдосконалення парадигм ІБ в організаційних екосистемах [7]. Використовуючи стратегічні ідеї та тактичні рамки, визначені цими стандартами, організації можуть орієнтуватися в складній місцевості сучасних цифрових ландшафтів із підвищеною пильністю та міцною стійкістю. Ці стандарти не тільки дають організаціям можливість зменшувати ризики, пов’язані з втратою або неправильним використанням інформації, але й каталізують культуру проактивного управління ризиками та постійного вдосконалення в динамічній сфері управління ІБ.

Висновки до розділу 1

Було охарактеризовано цілі та принципи аудиту. Це систематична незалежна перевірка інформаційних систем у постійному пошуку відповідності. Аудит ІБ відіграє ключову роль у забезпеченні захисту інформаційних активів організації. Його мета – виявлення вразливостей, оцінці ефективності існуючих заходів безпеки та забезпеченні відповідності нормативним вимогам і стандартам. Аудит допомагає виявити недоліки в системі безпеки,

запропонувати коригувальні дії та забезпечити керівництво об'єктивною інформацією для прийняття стратегічних рішень.

Були визначені цілі та принципи аудиту які включають перевірку відповідності політик і процедур ІБ, оцінку захисту інформаційних активів, а також виявлення та аналіз потенційних загроз і вразливостей. Основними принципами аудиту ІБ є об'єктивність, незалежність, конфіденційність і компетентність.

Також проаналізовано регуляторне середовище аудиту інформаційної безпеки. В аудиту ІБ використовуються різні стандарти та нормативні документи. Найбільш відомими є стандарти ISO/IEC 27001, які визначають вимоги до створення, впровадження, підтримки та постійного покращення СУІБ. Інші важливі стандарти включають NIST (National Institute of Standards and Technology) Cybersecurity Framework, COBIT (Control Objectives for Information and Related Technologies). Визначено, що використання цих стандартів дозволяє забезпечити системний підхід до захисту інформаційних ресурсів та підвищити рівень кібербезпеки організації.

Розділ 2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ОСОБЛИВОСТЕЙ ЗАСТОСУВАННЯ ІНСТРУМЕНТІВ АУДИТУ ІБ

2.1 Визначення ключових етапів аудиту ІБ

Аудит ІБ для забезпечення відповідності ISO/IEC 27001 є фундаментальним процесом для захисту інформаційних активів організації. Цей комплексний аудит включає кілька методичних кроків для перевірки дотримання встановлених стандартів і визначення областей для покращення. Кожен етап аудиту має вирішальне значення для забезпечення надійності та ефективності СУІБ організації.

1. Підготовчий етап. Процес аудиту починається з ретельної підготовчої фази. На цьому етапі ретельно визначаються цілі, обсяг і критерії аудиту. Це передбачає визначення конкретних аспектів ІБ, які необхідно вивчити, і визначення вимог ISO/IEC 27001, які можна застосувати. На цьому етапі важливо залучити ключові зацікавлені сторони, щоб переконатися, що цілі аудиту узгоджуються із загальною стратегією ІБ організації. Додатково збирається команда кваліфікованих і досвідчених аудиторів. Аудитори повинні мати глибоке розуміння стандартів ISO/IEC 27001, а також практичний досвід проведення подібних аудитів.

2. Попередній розгляд документації. Наступний етап передбачає попередню перевірку документації СУІБ організації. Це включає комплексний аналіз існуючих політик, процедур і записів. Аудитори прискіпливо переглядають ці документи, щоб зрозуміти, як організація впровадила вимоги стандарту. Ця перевірка документації служить основою для виявлення потенційних прогалин і підготовки до перевірки на місці. Це також допомагає аудиторам ознайомитися з СУІБ організації, сприяючи більш цілеспрямованому та ефективнішому інспектуванню на місці.

3. Перевірка на місці. Після перевірки документації аудитори переходять до етапу перевірки на місці. Це передбачає кілька ключових заходів:

- інтерв'ю з ключовим персоналом: аудитори проводять детальні інтерв'ю з ключовими співробітниками, щоб отримати уявлення про практику ІБ в організації. Ці інтерв’ю допомагають аудиторам зрозуміти, як політики та процедури застосовуються на практиці;
- оцінка заходів фізичної безпеки. Аудитори оцінюють засоби контролю фізичної безпеки для захисту інформаційних активів. Це включає перевірку засобів контролю доступу, систем спостереження та інших заходів фізичної безпеки;
- спостереження за робочими процесами. Аудитори спостерігають за повсякденними робочими процесами, щоб оцінити, як політики ІБ реалізуються в операціях у реальному часі. Це допомагає виявити будь-які розбіжності між задокументованими процедурами та фактичною практикою;
- аналіз систем контролю доступу. Аудитори аналізують механізми контролю доступу організації, щоб переконатися, що лише авторизований персонал має доступ до конфіденційної інформації. Це включає перегляд рівнів доступу користувачів, процесів автентифікації та систем моніторингу.

4. Оцінка управління ризиками. Критичним компонентом аудиту є оцінка процесів управління ризиками організації, які є центральними для ISO/IEC 27001. Аудитори оцінюють методи, що використовуються для ідентифікації, аналізу та оцінки ризиків. Вони перевіряють, як пріоритети встановлюються та як керуються ризиками, а також оцінюють ефективність заходів контролю для зниження виявлених ризиків до прийнятного рівня. Цей етап також включає перевірку відповідності вибраних засобів контролю вимогам, викладеним у Додатку А стандарту. Ефективне управління ризиками гарантує, що організація може завчасно виявляти потенційні загрози та усунути їх.

5. Аудиторська звітність. Після завершення перевірки на місці аудитори складають детальний аудиторський звіт. У цьому звіті описано всі виявлені невідповідності, недоліки та області для покращення. Звіт має бути всеосяжним, чітким і дієвим, дозволяючи організації зрозуміти необхідні коригувальні дії. Зазвичай він містить короткий виклад висновків, детальний опис

невідповідностей і рекомендації щодо покращення. Аудиторський звіт служить дорожньою картою для організації щодо підвищення рівня ІБ.

6. Впровадження коригувальних дій. Останній етап процесу аудиту включає аналіз і впровадження коригувальних дій. Організація повинна розробити та виконати план дій для вирішення виявлених проблем. Цей план має окреслювати конкретні кроки для виправлення невідповідностей, розподілу відповідальності та встановлення часових рамок реалізації. Ефективна комунікація та координація між різними відділами мають вирішальне значення для забезпечення успішного виконання коригувальних дій. Після впровадження коригувальних заходів може бути проведений наступний аудит, щоб переконатися, що недоліки були належним чином усунені.

7. Постійне вдосконалення. Проведення аудиту ІБ на відповідність вимогам ISO/IEC 27001 – це не одноразова подія, а повторюваний процес, спрямований на постійне вдосконалення СУІБ. Регулярні перевірки необхідні для своєчасного виявлення та усунення недоліків. Вони допомагають забезпечити високий рівень захисту інформаційних активів і постійну відповідність міжнародним стандартам. Постійно відстежуючи та вдосконалюючи свої практики ІБ, організації можуть краще адаптуватися до нових загроз і зберегти довіру своїх зацікавлених сторін. Регулярні аудити також демонструють прагнення підтримувати найвищі стандарти ІБ, що може підвищити репутацію та конкурентну перевагу організації.

Підсумовуючи, аудит ІБ на відповідність вимогам ISO/IEC 27001 є комплексним і систематичним процесом, який вимагає ретельного планування, виконання та подальших дій. Кожен етап аудиту сприяє ретельному оцінюванню СУІБ організації, гарантуючи, що він ефективний у захисті інформаційних активів і відповідає міжнародним стандартам. Прийнявши культуру безперервного вдосконалення, організації можуть підвищити рівень ІБ та досягти довгострокового успіху.

2.2 Дослідження методів аудиту ІБ

Аудит ІБ є критично важливим компонентом управління ризиками, необхідним для забезпечення захисту інформаційних активів організації. Розвиток ландшафту загроз у поєднанні зі зростаючими нормативними вимогами вимагає комплексного та суворого підходу до аудиту. Існує кілька методологій аудиту, кожна з яких адаптована до конкретних характеристик та ІС даної організації. Інтеграція цих методологій забезпечує цілісне уявлення про стан безпеки організації [7].

Одним із основних методів є тестування на проникнення. У цьому підході аудитори імітують тактику потенційних зловмисників, щоб проникнути в систему та виявити вразливі місця. Цей метод є особливо цінним, оскільки він забезпечує реалістичну оцінку того, наскільки добре поточні заходи безпеки можуть протистояти реальним сценаріям атак. Тестування на проникнення може виявити широкий спектр вразливостей, від помилок ПЗ та помилок конфігурації до слабкої політики паролів і людського фактору. Імітуючи фактичні методи атак, організації можуть отримати уявлення про ефективність свого захисту та потенційний вплив порушень безпеки. Результати тестів на проникнення дають змогу розробити цільові стратегії пом’якшення, покращуючи загальну систему безпеки.

Аудит конфігурацій – ще один важливий метод, який зосереджується на перевірці налаштувань апаратного та ПЗ на відповідність встановленим стандартам і політикам безпеки. Цей метод має вирішальне значення, оскільки неправильні конфігурації або невідповідні налаштування можуть створити серйозні вразливості, які нелегко виявити іншими засобами. Аудит конфігурації передбачає ретельний аналіз налаштувань системи, засобів контролю доступу, мережевих конфігурацій і встановлення ПЗ. Він гарантує, що системи налаштовані відповідно до найкращих практик і організаційної політики. Цей процес не тільки допомагає виявити прогалини в безпеці, але й забезпечує дотримання нормативних вимог. Регулярні аудити конфігурації необхідні для

підтримки цілісності та безпеки ІС у технологічному середовищі, що швидко змінюється.

Аналіз журналів – це широко використовуваний метод аудиту ІБ. Журнали, які записують події в ІС, ретельно перевіряються, щоб виявити аномальні дії, які можуть свідчити про спроби несанкціонованого доступу або інші порушення безпеки. Журнали забезпечують детальний запис системної діяльності, включаючи дії користувача, системні зміни та мережевий трафік. Аналізуючи ці журнали, аудитори можуть визначити закономірності та тенденції, які можуть означати інциденти безпеки. Аналіз журналу дає змогу виявляти підозрілі дії, наприклад повторювані невдалі спроби входу, незвичні шаблони доступу та спроби викрадання даних [8]. Цей метод також підтримує зусилля з реагування на інциденти, забезпечуючи хронологічний запис подій, допомагаючи у реконструкції інцидентів та визначенні основних причин. Крім того, аналіз журналів сприяє дотриманню правових і нормативних вимог, демонструючи належну обачність у моніторингу та управлінні подіями безпеки.

Опитування та інтерв'ю є ще одним важливим компонентом аудиту ІБ. Співбесіди з персоналом допомагають оцінити їхню обізнаність із політикою безпеки та виявити потенційні проблеми у внутрішніх процесах. Ці взаємодії дають цінну інформацію про людський аспект безпеки, включно з поведінкою співробітників, дотриманням протоколів безпеки та усвідомленням потенційних загроз. Опитування збирають вичерпні дані про методи безпеки організації, висвітлюючи слабкі місця, які можуть бути пропущені іншими методами аудиту. За допомогою структурованих анкет та особистих інтерв’ю аудитори можуть оцінити ефективність навчальних програм безпеки, виявити прогалини в знаннях і зрозуміти культурні аспекти безпеки в організації. Цей метод також полегшує ідентифікацію внутрішніх загроз, які можуть становити значні ризики для ІБ [8].

Оцінка відповідності міжнародним стандартам, таким як ISO/IEC 27001, також має вирішальне значення. Ці стандарти визначають вимоги до СУІБ, забезпечуючи основу для управління та захисту конфіденційної інформації. Аудит відповідності цим стандартам допомагає оцінити, наскільки ІБ організації

відповідає передовій світовій практиці, і визначає області для вдосконалення. Аудити відповідності передбачають комплексний аналіз політики, процедур і засобів контролю, щоб переконатися, що вони відповідають визначеним стандартам. Отримання та підтримка сертифікації за визнаними стандартами підвищує довіру до організації та демонструє її прихильність ІБ. Крім того, перевірки відповідності допомагають організаціям випереджати нормативні вимоги та уникнути можливих санкцій за їх невиконання.

Крім того, автоматизовані інструменти відіграють важливу роль в перевірках безпеки [9]. Ці інструменти можуть виконувати низку завдань, від сканування мереж на наявність вразливостей до моніторингу системи в реальному часі. Автоматизовані інструменти використовують передові технології, такі як штучний інтелект і машинне навчання, щоб ефективніше виявляти загрози безпеці та реагувати на них. Наприклад, сканери вразливостей можуть швидко виявляти слабкі місця в конфігураціях програмного та апаратного забезпечення, а системи виявлення вторгнень відстежують мережевий трафік на наявність ознак зловмисної діяльності. Використання автоматизованих інструментів підвищує ефективність аудиту, дозволяючи швидко ідентифікувати потенційні загрози та реагувати на них. Ці інструменти також надають можливості постійного моніторингу, що дозволяє організаціям підтримувати проактивну позицію безпеки. Автоматизація зменшує навантаження на аудиторів, дозволяючи їм зосередитися на більш складних і стратегічних аспектах процесу аудиту [9].

Підсумовуючи, аудит ІБ охоплює різноманітні методології, кожна з яких має свої унікальні переваги та обмеження. Застосування комбінації цих методів забезпечує комплексну оцінку стану ІБ організації та сприяє розробці ефективних стратегій покращення. Інтеграція тестування на проникнення, аудиту конфігурації, аналізу журналів, опитувань, інтерв’ю, оцінки відповідності та автоматизованих інструментів забезпечує надійну структуру для виявлення та зменшення ризиків безпеки. Завдяки регулярним і систематичним аудитам організації можуть підвищити свою стійкість проти

кіберзагроз, захистити конфіденційну інформацію та забезпечити дотримання нормативних вимог. Ретельний і якісно проведений аудит ІБ є незамінним для підтримки довіри зацікавлених сторін, захисту активів організації та досягнення довгострокових цілей безпеки.

Аналіз методів аудиту ІБ. Аналіз методів аудиту ІБ вимагає розгляду кожного методу з урахуванням його особливостей, переваг та недоліків, а також взаємодії між ними для досягнення максимального рівня захисту ІС організації [9].

Тестування на проникнення (penetration testing) є одним з найбільш ефективних методів для виявлення вразливостей у системах безпеки. Воно полягає у використанні методів, аналогічних тим, що застосовуються хакерами, для спроби проникнути в ІС організації. Це дозволяє побачити, як реальні атаки можуть вплинути на систему та наскільки ефективно працюють існуючі заходи захисту. Основні переваги цього методу включають можливість реальної оцінки безпеки системи та виявлення потенційних загроз до того, як їх зможуть використати зловмисники. Недоліки полягають у високій вартості, ризику пошкодження систем під час тестування, а також можливості пропуску деяких вразливостей, які не були використані в конкретному тесті.

Аудит конфігурацій є ще одним важливим методом, що дозволяє перевіряти налаштування апаратного та ПЗ на відповідність встановленим стандартам і політикам безпеки. Неправильні або невідповідні налаштування можуть створювати серйозні ризики для безпеки, тому аудит конфігурацій допомагає виявити та виправити такі проблеми. Основна перевага цього методу полягає у можливості попередження проблем безпеки до їх виникнення. Однак, цей метод є трудомістким і потребує значних ресурсів, особливо у великих організаціях з великою кількістю систем і різноманітним ПЗ [10].

Аналіз логів є потужним інструментом для виявлення аномалій і потенційних інцидентів безпеки. Логи містять детальну інформацію про всі дії, що відбуваються в ІС, включаючи спроби доступу, зміну файлів та інші операції. Аналізуючи ці записи, аудитори можуть виявити незвичайні дії, які можуть

свідчити про спроби несанкціонованого доступу або інші порушення безпеки. Основна перевага аналізу логів полягає в його здатності виявляти інциденти, які можуть залишатися непоміченими іншими методами. Однак, цей метод потребує складних інструментів для аналізу і може бути неефективним без належного налаштування і розуміння контексту.

Метод опитувань та інтерв'ю з персоналом дозволяє оцінити обізнаність співробітників з політиками безпеки і виявити слабкі місця у внутрішніх процесах. Інтерв'ю зі співробітниками допомагають отримати інформацію про реальні практики безпеки, які використовуються в організації, і виявити проблеми, які можуть бути непомітними при інших методах. Переваги цього методу включають можливість отримання цінної інсайдерської інформації і виявлення проблем на людському рівні. Недоліки полягають у суб'єктивності отриманої інформації і залежності від чесності та відкритості співробітників.

Оцінка відповідності стандартам, таким як ISO/IEC 27001, є важливим методом для забезпечення дотримання міжнародних норм і стандартів у галузі ІБ. Цей метод дозволяє структурувати процеси безпеки і впроваджувати передові практики. Основна перевага оцінки відповідності стандартам полягає у можливості формалізувати і систематизувати процеси управління безпекою [10]. Однак, цей метод може бути затратним і вимагати значних зусиль для досягнення і підтримки відповідності стандартам.

Автоматизовані інструменти для аудиту безпеки, такі як сканери вразливостей та системи моніторингу в реальному часі, значно підвищують ефективність аудиту. Вони можуть швидко виявляти і реагувати на потенційні загрози, забезпечуючи постійний моніторинг і захист. Переваги автоматизованих інструментів включають швидкість і ефективність виявлення загроз, а також можливість виконання складних завдань без значних витрат часу і ресурсів. Недоліки полягають у тому, що автоматизація не може повністю замінити людський фактор і аналітичні здібності, необхідні для розуміння контексту і прийняття обґрунтованих рішень.

Таким чином, кожен метод аудиту ІБ має свої унікальні переваги і недоліки, і жоден з них не є універсальним. Ефективний аудит вимагає використання комбінації різних методів, що дозволяє забезпечити всебічну оцінку стану ІБ в організації [11]. Застосування тестування на проникнення, аудиту конфігурацій, аналізу логів, опитувань та інтерв'ю, оцінки відповідності стандартам і автоматизованих інструментів разом дозволяє створити комплексну систему захисту, яка здатна реагувати на різноманітні загрози і забезпечувати високий рівень безпеки інформаційних ресурсів організації.

2.3. Аналіз інструментів, що застосовуються для проведення аудиту ІБ

Системи управління вразливостями (СУВ) відіграють ключову роль в забезпеченні кібербезпеки організацій, дозволяючи ідентифікувати, оцінювати та усувати вразливості в їх ІС. Робота таких систем полягає в постійному моніторингу та аналізі ПЗ, мережевого обладнання та інших компонентів інфраструктури для виявлення потенційних загроз та ризиків.

Основний етап роботи СУВ – це виявлення вразливостей. Для цього використовуються різноманітні методи, такі як сканування мережі, аналіз коду та моніторинг активності. Сканери вразливостей періодично перевіряють систему на наявність відомих вразливостей, порівнюючи дані з базою даних відомих загроз. Ці сканери можуть бути як автоматичними, так і ручними, де останні використовуються для більш глибокого аналізу специфічних компонентів [12].

Після виявлення вразливостей наступним кроком є їх оцінка. СУВ використовують різні критерії для визначення критичності виявлених проблем, включаючи потенційний вплив на систему, ймовірність експлуатації та наявність відомих експлойтів. Для цього часто використовуються загальноприйняті стандарти оцінки вразливостей, такі як CVSS (Common Vulnerability Scoring System), що дозволяє ранжувати вразливості за шкалою від 0 до 10.

Оцінивши вразливості, СУВ переходять до фази усунення. Це може включати оновлення ПЗ, встановлення патчів, зміну конфігурацій системи або застосування інших заходів захисту. СУВ також забезпечують відстеження процесу усунення вразливостей, генеруючи звіти про статус виправлення та рекомендації щодо подальших дій.

Інтеграція з іншими системами безпеки є важливою особливістю сучасних СУВ. Наприклад, вони можуть взаємодіяти з SIEM-системами, системами попередження вторгнень (IDS/IPS) та іншими інструментами для створення більш комплексного підходу до кібербезпеки. Це дозволяє автоматизувати процес реагування на інциденти та покращити координацію між різними командами безпеки [16].

Крім того, сучасні СУВ часто використовують елементи машинного навчання та штучного інтелекту для покращення точності виявлення вразливостей та зменшення кількості хибних спрацьовувань. Вони також можуть використовувати інформацію про загрози в реальному часі (threat intelligence) для швидшого реагування на нові загрози та їх експлойти.

Загалом, системи управління вразливостями є невід'ємною частиною стратегії кібербезпеки будь-якої сучасної організації. Вони забезпечують проактивний підхід до захисту інформаційних активів, знижуючи ризики від можливих атак та забезпечуючи безперервну безпеку IT-інфраструктури.

Тестування на проникнення, або пен-тестинг, є важливою складовою забезпечення кібербезпеки. Воно дозволяє організаціям виявляти та усувати вразливості в їхніх системах до того, як їх зможуть використати зловмисники. Інструменти тестування на проникнення призначені для автоматизації цього процесу, дозволяючи експертам з кібербезпеки виявляти слабкі місця в ІС ефективно та надійно [13].

Робота інструментів тестування на проникнення базується на ряді технік та методів, які імітують дії потенційних зловмисників. Вони виконують ряд автоматизованих завдань, включаючи сканування портів, аналіз мережевого трафіку, перевірку веб-застосунків, експлуатацію вразливостей та аналіз

конфігурацій безпеки. В залежності від мети тестування, інструменти можуть бути орієнтовані на різні аспекти безпеки, такі як мережі, веб-додатки, мобільні пристрої або навіть фізичні системи.

Одним з найпоширеніших інструментів для пен-тестингу є Metasploit. Це потужна платформа з відкритим кодом, яка дозволяє користувачам тестувати вразливості, розробляти та запускати експлойти, а також створювати власні модулі для проведення специфічних тестів. Metasploit підтримує широкий спектр експлойтів та має зручний інтерфейс для автоматизації та аналізу результатів тестування.

Моніторинг і аналіз мережевого трафіку є критичними елементами для забезпечення безпеки та ефективності мережі. Інструменти моніторингу мережевого трафіку дозволяють адміністраторам і аналітикам отримувати уявлення про роботу мережі, виявляти потенційні проблеми та забезпечувати відповідність політикам безпеки.

Основні функції інструментів моніторингу включають збір, аналіз і візуалізацію даних про мережевий трафік. Вони можуть відслідковувати кількість переданих пакетів, їх розмір, протоколи, джерела і призначення, а також час передачі. Ці дані дозволяють створювати загальну картину про використання мережі та виявляти аномалії, які можуть вказувати на проблеми, такі як мережеві збої або кібератаки.

Процес збору даних про мережевий трафік здійснюється за допомогою різних методів. Одним із основних є використання мережевих сенсорів або агентів, які встановлюються на мережевих пристроях або серверах. Вони захоплюють мережеві пакети та передають їх до центрального сервера для подальшого аналізу. Іншим методом є використання SPAN-портів (Switch Port Analyzer) або мережевих TAPів (Test Access Point), які копіюють трафік з одного або декількох портів комутатора для аналізу.

Після збору дані аналізуються за допомогою різних методів і алгоритмів. Наприклад, методи статистичного аналізу можуть використовуватися для виявлення аномалій у трафіку, таких як незвично високе навантаження або

підозріла активність. Крім того, методи машинного навчання та штучного інтелекту можуть застосовуватися для виявлення складніших патернів і прогнозування майбутніх подій. Інструменти аналізу також можуть надавати можливості для проведення глибокого аналізу пакетів (DPI – Deep Packet Inspection), що дозволяє детально розглядати вміст мережевих пакетів і виявляти небажані або шкідливі дані.

Результати аналізу зазвичай візуалізуються у вигляді графіків, звітів і дашбордів, що дозволяє адміністраторам швидко оцінити стан мережі та приймати обґрунтовані рішення. Наприклад, вони можуть визначити, які додатки використовують найбільше ресурсів, чи є проблеми з продуктивністю в певних сегментах мережі або які користувачі генерують найбільше трафіку.

Окрім виявлення проблем і аномалій, інструменти моніторингу мережевого трафіку відіграють важливу роль у забезпеченні безпеки. Вони можуть виявляти і запобігати атакам, таким як DoS (Denial of Service), DDoS (Distributed Denial of Service), мережеві черв'яки та інші види шкідливого ПЗ. Інтеграція з системами виявлення та запобігання вторгнень (IDS/IPS) дозволяє забезпечити більш комплексний підхід до захисту мережі [14].

Загалом, інструменти моніторингу та аналізу мережевого трафіку є незамінними для сучасних підприємств, що прагнуть забезпечити стабільність, безпеку та ефективність своїх мережевих інфраструктур. Вони надають можливість не тільки виявляти й усувати поточні проблеми, але й прогнозувати майбутні, забезпечуючи проактивний підхід до управління мережею.

Системи безпеки та керування подіями, відомі також як SIEM (Security Information and Event Management), є ключовими компонентами сучасної кібербезпеки. Вони забезпечують централізовану функцію моніторингу, аналізу та реагування на інциденти, що дозволяє організаціям захищати свої інформаційні ресурси від загроз.

Основна ідея SIEM полягає у зборі, аналізі та кореляції даних з різних джерел. Це включає журнали подій, мережеві потоки, дані з пристроїв безпеки, такі як міжмережеві екрани, антивірусні програми, системи виявлення вторгнень

(IDS) та системи запобігання вторгнень (IPS). Завдяки цьому, SIEM може надавати всебічну картину стану безпеки в реальному часі.

Процес роботи SIEM починається з збору даних. Кожен пристрій у мережі, що генерує журнали або події, відправляє їх до SIEM-системи. Ці дані можуть включати як структуровані, так і неструктуровані формати, що потребує їх попередньої обробки. На цьому етапі важливо забезпечити, щоб зібрані дані були повними і точними, оскільки від цього залежить ефективність подальшого аналізу.

Наступний етап – це нормалізація даних. Оскільки різні системи та пристрої можуть використовувати різні формати для збереження своїх журналів, SIEM-система приводить ці дані до єдиного стандарту. Це дозволяє ефективніше проводити їх аналіз і кореляцію. Нормалізація включає очищення даних, видалення дублюючої інформації та стандартизацію полів.

Ключовим елементом роботи SIEM є кореляція подій. Цей процес дозволяє визначити зв'язки між окремими подіями та виявити потенційно шкідливу активність, яка може бути непомітною при аналізі окремих подій. Наприклад, спроби входу в систему з різних географічних місць за короткий проміжок часу можуть вказувати на компрометацію облікового запису. Кореляційні правила налаштовуються на основі відомих шаблонів атак, аномалій у поведінці користувачів та інших критеріїв.

SIEM також надає можливості для аналізу даних та створення звітів. Аналітики безпеки можуть використовувати ці інструменти для проведення розслідувань інцидентів, виявлення тенденцій та вразливостей. Звіти можуть включати як детальну інформацію про конкретні інциденти, так і загальні огляди стану безпеки організації.

Реагування на інциденти є ще одним важливим аспектом роботи SIEM. Коли система виявляє потенційну загрозу, вона може автоматично генерувати оповіщення, відправляти повідомлення відповідальним фахівцям або навіть вживати заходів для нейтралізації загрози, таких як блокування підозрілих IP-

адрес або ізоляція заражених пристроїв. Ці дії допомагають швидко зменшити шкоду та запобігти подальшому поширенню загрози.

Загалом, системи SIEM є потужним інструментом для забезпечення кібербезпеки. Вони об'єднують збір, нормалізацію, кореляцію та аналіз даних з різних джерел, що дозволяє своєчасно виявляти та реагувати на загрози. Це робить їх незамінними для організацій, які прагнуть захистити свої інформаційні ресурси від сучасних кіберзагроз.

Аналіз шкідливих програм є важливим аспектом сучасної кібербезпеки, оскільки шкідливе ПЗ постійно еволюціонує, стає більш складним і загрожує різним аспектам комп'ютерних систем та мереж. Інструменти аналізу шкідливих програм дозволяють дослідникам виявляти, досліджувати та нейтралізувати ці загрози, а також розробляти відповідні захисні механізми.

Існують різні методи та інструменти аналізу шкідливих програм, які можна умовно поділити на статичний та динамічний аналіз. Статичний аналіз передбачає дослідження шкідливого коду без його виконання. Це включає аналіз вихідного коду, дизасемблювання та декомпіляцію. Основні інструменти для статичного аналізу включають IDA Pro, Ghidra та Radare2. Ці інструменти дозволяють дослідникам розбирати виконувані файли, аналізувати їхню структуру та ідентифікувати потенційно небезпечні ділянки коду. Важливою складовою статичного аналізу є використання сигнатурного аналізу, який порівнює код з базою відомих сигнатур шкідливих програм [15].

Динамічний аналіз, на відміну від статичного, включає виконання шкідливого ПЗ в контрольованому середовищі з метою спостереження за його поведінкою. Основні інструменти для динамічного аналізу включають пісочниці (sandbox), такі як Cuckoo Sandbox, а також відладчики, як-от OllyDbg та x64dbg. Використання пісочниць дозволяє створити ізольоване середовище, де можна безпечно виконувати шкідливий код і спостерігати за його взаємодією з системою, мережевою активністю та змінами у файловій системі. Відладчики дозволяють дослідникам крок за кроком виконувати програму, аналізуючи її поведінку на рівні процесора та пам'яті.

Крім того, важливою складовою аналізу шкідливих програм є використання інструментів для аналізу мережевого трафіку, таких як Wireshark, які дозволяють виявляти шкідливу мережеву активність, наприклад, зв'язок з командними серверами або передачу конфіденційної інформації.

Сучасні інструменти аналізу шкідливих програм також включають механізми автоматизації, такі як YARA та Snort, які дозволяють автоматично виявляти та класифікувати шкідливі програми на основі попередньо визначених правил та сигнатур.

Ще одним важливим аспектом є використання інструментів зворотного проектування (reverse engineering), що дозволяють зрозуміти логіку роботи шкідливого ПЗ та розробити засоби для його нейтралізації. Це включає аналіз алгоритмів шифрування, що використовуються шкідливим ПЗ, методів його поширення та механізмів приховування.

Таким чином, інструменти аналізу шкідливих програм є складним і багатогранним набором технологій та методів, що дозволяють дослідникам ефективно виявляти, аналізувати та протидіяти шкідливим програмам. Вони включають як статичні, так і динамічні методи аналізу, автоматизовані системи виявлення та класифікації, а також засоби для аналізу мережевого трафіку та зворотного проектування. Кожен з цих інструментів та методів має свої переваги та обмеження, і їхнє комбіноване використання дозволяє забезпечити максимально ефективний захист від сучасних кіберзагроз.

Інструменти оцінки конфігурації та відповідності вимогам безпеки відіграють важливу роль у забезпеченні ІБ організацій. Вони допомагають ідентифікувати, оцінювати та усувати вразливості в ІТ-інфраструктурі, забезпечуючи відповідність встановленим стандартам безпеки та політикам. Ці інструменти використовуються для проведення аудиту конфігурацій, моніторингу змін, оцінки ризиків та забезпечення дотримання вимог нормативних актів.

Робота інструментів оцінки конфігурації та відповідності вимогам безпеки починається з збору даних про поточний стан системи. Це включає інформацію

про конфігурацію мережевих пристроїв, серверів, робочих станцій, ПЗ та інших компонентів інфраструктури. Збір даних може здійснюватися за допомогою агентів, які встановлюються на кожному пристрої, або безагентних методів, коли інформація збирається дистанційно через мережеві протоколи.

Після збору даних інструменти проводять порівняння поточного стану системи з еталонними конфігураціями та вимогами безпеки. Це може включати перевірку відповідності конфігурацій загальноприйнятим стандартам, таким як CIS Benchmarks, NIST, ISO 27001, а також внутрішнім політикам безпеки організації. Інструменти оцінюють відповідність налаштувань різним вимогам, наприклад, чи використовуються складні паролі, чи включено шифрування даних, чи встановлено необхідні патч [16].

Одним з ключових аспектів роботи цих інструментів є виявлення вразливостей. Вони аналізують конфігурації та налаштування з метою виявлення потенційних загроз, які можуть бути використані зловмисниками. Це можуть бути незахищені порти, відсутні оновлення, слабкі паролі або інші фактори, які можуть підвищувати ризик компрометації системи.

Після виявлення вразливостей інструменти надають рекомендації щодо їх усунення. Це можуть бути конкретні інструкції з налаштування системи, оновлення ПЗ або зміни в політиках безпеки. Деякі інструменти можуть автоматично виправляти певні проблеми або надавати засоби для автоматизації процесу усунення вразливостей.

Інструменти оцінки конфігурації та відповідності вимогам безпеки також забезпечують моніторинг змін у системі. Вони можуть відстежувати зміни в конфігураціях і попереджати адміністраторів про потенційно небезпечні дії. Це дозволяє оперативно реагувати на зміни та запобігати виникненню нових вразливостей.

Звітування є ще одним важливим аспектом роботи цих інструментів. Вони генерують детальні звіти про стан системи, виявлені вразливості, ступінь відповідності вимогам безпеки та виконані дії з усунення проблем. Ці звіти

допомагають організаціям оцінювати ефективність заходів безпеки, виявляти слабкі місця та планувати подальші дії для підвищення рівня захищеності.

Загалом, інструменти оцінки конфігурації та відповідності вимогам безпеки є невід'ємною частиною сучасної СУІБ. Вони забезпечують комплексний підхід до управління безпекою, дозволяють ідентифікувати та усувати вразливості, забезпечувати відповідність стандартам та політикам безпеки, а також підвищують загальний рівень захищеності ІТ-інфраструктури організації.

Висновки до розділу 2

В розділі було проаналізовано та досліджено методи та інструменти аудиту інформаційної безпеки. У ході роботи було виявлено, що кожен з розглянутих методів та інструментів має свої унікальні переваги та недоліки, а їх комбіноване використання є найбільш ефективним підходом для забезпечення комплексної безпеки ІС організації.

Тестування на проникнення дозволяє виявити реальні вразливості та оцінити ефективність захисних заходів шляхом імітації дій зловмисників, хоча й несе певний ризик для стабільності системи. Аудит конфігурацій допомагає забезпечити належні налаштування апаратного та ПЗ, що запобігає появі потенційних загроз, проте є трудомістким і ресурсозатратним процесом. Аналіз логів є потужним інструментом для ретроспективного виявлення аномалій та інцидентів, хоча вимагає складних інструментів для аналізу та належного розуміння контексту. Опитування та інтерв'ю з персоналом дозволяють виявити слабкі місця у внутрішніх процесах та оцінити обізнаність співробітників з політиками безпеки, хоча цей метод є суб'єктивним і залежить від чесності та відкритості респондентів. Оцінка відповідності міжнародним стандартам, таким як ISO/IEC 27001,NIST SP 800-53, COBIT дозволяє структурувати процеси безпеки та впроваджувати передові практики, але є затратною та вимагає постійних зусиль для підтримки відповідності.

Підсумовуючи, можна впевнено сказати що тільки комплексний підхід до аудиту ІБ, який включає комбінацію різних методів та інструментів, дозволяє забезпечити всебічну оцінку та ефективне управління ризиками.

Розділ 3 ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ ТА ІНСТРУМЕНТІВ АУДИТУ ІБ

3.1. Порівняльний аналіз інструментів аудиту ІБ

Проведення аудиту ІБ вимагає використання різноманітних інструментів, кожен з яких має свої переваги та обмеження. У сукупності ці інструменти забезпечують комплексний підхід до ідентифікації, аналізу та управління загрозами та ризиками, таким чином створюючи надійну структуру для захисту інформаційних активів організації. Основні технології та інструменти включають в себе такі:

1. Системи управління вразливостями: Qualys, Nessus і OpenVAS є трьома з найпоширеніших інструментів для проведення оцінки вразливостей в ІС. Кожна з цих систем має свої унікальні характеристики, переваги та недоліки, що робить їх придатними для різних сценаріїв використання.

Qualys [18] – це комерційна платформа для управління вразливостями, яка забезпечує комплексне рішення для безпеки. Вона підтримує широкий спектр функцій, включаючи сканування мереж, управління вразливостями, відповідність вимогам безпеки та моніторинг політик. Основні переваги Qualys включають високу точність виявлення, потужні аналітичні інструменти та можливість інтеграції з іншими системами безпеки. Крім того, Qualys пропонує хмарне рішення, що дозволяє здійснювати сканування з будь-якої точки світу без необхідності встановлення локального обладнання. Серед недоліків можна виділити високу вартість послуг та складність налаштування, що може вимагати додаткових ресурсів і часу. Для кращого розуміння було додано рис. 3.1, на якому зображено інтерфейс програми Qualys.

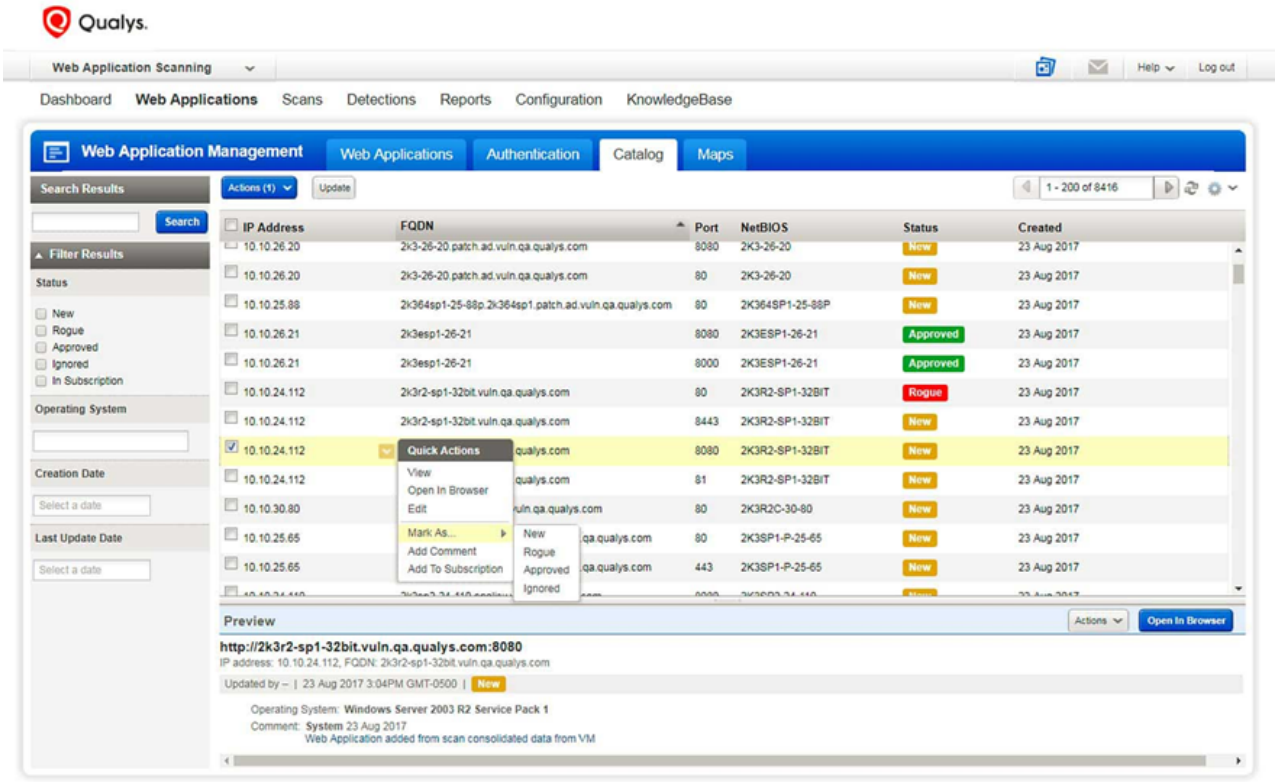

Рис. 3.1. Інтерфейс програми Qualys

Nessus [19], розроблений компанією Tenable, є одним з найпопулярніших інструментів для сканування вразливостей. Він відомий своєю ефективністю та точністю виявлення вразливостей, підтримує великий набір плагінів для різних типів сканувань і регулярно оновлюється для забезпечення актуальності бази даних вразливостей. Переваги Nessus включають простоту використання, гнучкість налаштувань та високу швидкість сканування. До того ж, Nessus має зручний інтерфейс та потужні звітні функції. Однак, Nessus є комерційним продуктом, і його повнофункціональна версія потребує підписки. Це може стати недоліком для малих підприємств або організацій з обмеженим бюджетом.

OpenVAS (Open Vulnerability Assessment System) [20] – це відкритий інструмент для сканування вразливостей, який є частиною проекту Greenbone. OpenVAS забезпечує потужні можливості для виявлення вразливостей і є популярним вибором серед організацій, що віддають перевагу рішенням з відкритим кодом. Переваги OpenVAS включають безкоштовність використання, високу гнучкість та налаштовуваність, а також активну спільноту користувачів і

розробників, які постійно вдосконалюють продукт. Водночас, OpenVAS може бути складним у встановленні та налаштуванні, особливо для новачків. Крім того, продуктивність системи може знижуватися при обробці великого обсягу даних.

Для наочності, було створено порівняльну діаграму розглянутих інструментів (рис. 3.2).

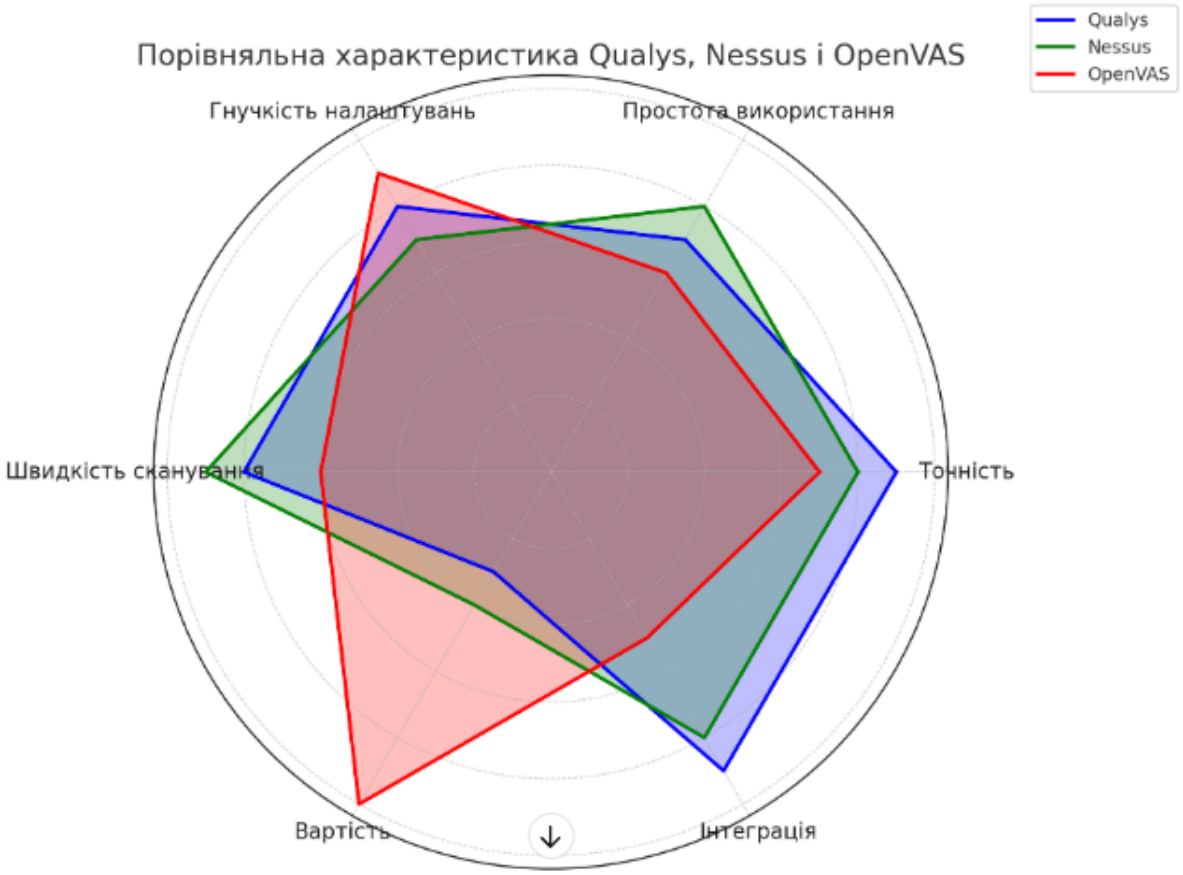

Рис. 3.2. Порівняльна діаграма Qualys, Nessus, OpenVAS

Як видно з діаграми, кожен з інструментів має свої сильні і слабкі сторони. Qualys вирізняється високою точністю і інтеграцією, але поступається у вартості. Nessus має високу швидкість сканування і простоту використання, але теж є комерційним продуктом. OpenVAS, будучи безкоштовним і гнучким, вимагає більше зусиль для налаштування та може поступатися в продуктивності.

2. Інструменти тестування на проникнення. Сучасні ІС потребують надійних засобів захисту від кіберзагроз, і важливу роль у цьому відіграють інструменти для тестування безпеки. До найбільш поширених та потужних

інструментів у цій галузі належать Metasploit, Burp Suite і OWASP ZAP. Кожна з цих програм має свої особливості, переваги та недоліки.

Metasploit [21] – це інструмент для проведення тестів на проникнення, який відомий своєю потужністю та функціональністю. Він дозволяє створювати, тестувати та використовувати експлойти для виявлення вразливостей у системах.

Metasploit має велику базу даних експлойтів, що постійно оновлюється, та потужні функції автоматизації. До його переваг належать гнучкість, підтримка різних платформ і можливість інтеграції з іншими інструментами безпеки. Проте, Metasploit може бути складним для новачків і вимагати глибоких знань у галузі ІБ.

Burp Suite [22] – це комплексний інструмент для тестування веб-додатків, який широко використовується професіоналами у галузі безпеки. Burp Suite пропонує велику кількість інструментів для аналізу, виявлення та експлуатації вразливостей у веб-додатках. Однією з головних переваг Burp Suite є його інтерфейс, який дозволяє легко налаштовувати параметри сканування та інтегрувати різні плагіни для розширення функціональності. Однак, деякі функції Burp Suite доступні лише у платній версії, що може бути недоліком для малих компаній або незалежних дослідників.

OWASP ZAP [23] (Zed Attack Proxy) – це безкоштовний та відкритий інструмент для тестування безпеки веб-додатків, який розроблений проектом OWASP. OWASP ZAP відомий своєю простотою використання та широким набором функцій для виявлення вразливостей. Він дозволяє автоматично сканувати веб-додатки та виконувати ручне тестування. Перевагами OWASP ZAP є його відкритість, велика спільнота користувачів та розробників, а також постійне оновлення та підтримка. Водночас, OWASP ZAP може не мати деяких розширених функцій, які пропонують платні конкуренти, такі як Burp Suite.

На основі цього аналізу можна зробити висновки про переваги та недоліки кожної програми, які наведені нижче.

Metasploit:

- потужність , велика база даних експлойтів, гнучкість, підтримка різних платформ;
- складність використання для новачків, потреба у глибоких знаннях.

Burp Suite:

- зручний інтерфейс, можливість налаштування, підтримка плагінів;
- деякі функції доступні лише у платній версії.

OWASP ZAP:

- безкоштовність, простота використання, велика спільнота, постійні оновлення;
- обмеженість деяких розширених функцій порівняно з платними аналогами.

Для візуалізації порівняння цих трьох програм запропоновано діаграму (рис. 3.3).

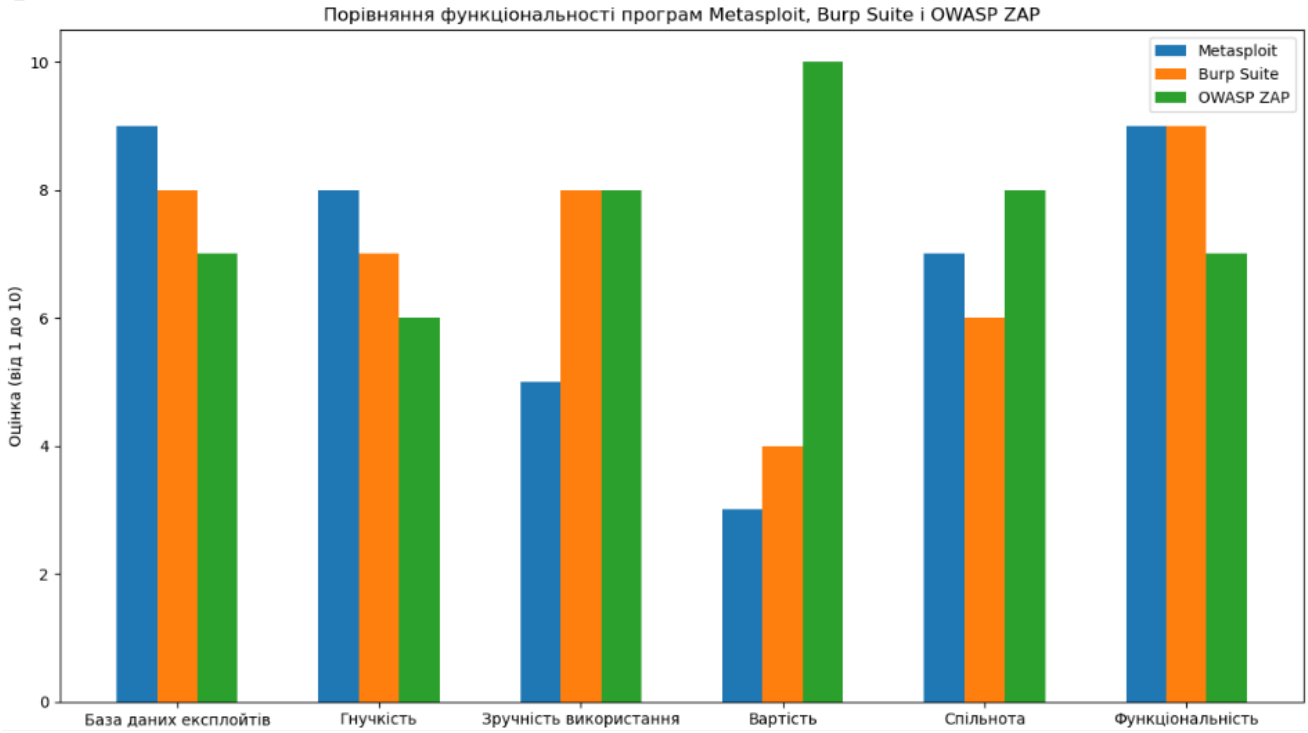

Рис. 3.3. Порівняльна діаграма Metasploit, Burp Suite, OWASP ZAP

Таким чином, кожен інструмент має свої унікальні переваги та недоліки, що дозволяє обрати найбільш підходящий для конкретних потреб у тестуванні

безпеки. Metasploit підходить для глибокого аналізу вразливостей та роботи з експлойтами, Burp Suite забезпечує комплексний підхід до тестування веб-додатків з можливістю налаштування, а OWASP ZAP пропонує доступний та простий у використанні інструмент для базового тестування безпеки веб-додатків.

3. Інструменти моніторингу та аналізу мережевого трафіку. Splunk та Wireshark є двома популярними інструментами, які широко використовуються для аналізу даних та мережевого трафіку, але кожен з них має свої унікальні особливості, що робить їх корисними у різних контекстах.

Splunk [24] – це потужна платформа для аналізу даних, яка забезпечує збір, індексацію та візуалізацію великих обсягів даних з різних джерел. Splunk використовується в основному для моніторингу та аналізу журналів (логів) з метою забезпечення безпеки, управління IT-інфраструктурою та оптимізації бізнес-процесів.

Однією з головних переваг Splunk є його здатність працювати з великими обсягами даних у режимі реального часу, забезпечуючи гнучкі можливості для пошуку та аналітики. Інтуїтивно зрозумілий інтерфейс та потужні інструменти для створення звітів і дашбордів дозволяють користувачам легко отримувати інсайти з даних.

Однак, Splunk може бути дорогим для впровадження, особливо для малих та середніх підприємств, що є його основним недоліком. Крім того, налаштування та оптимізація Splunk можуть вимагати значного часу, ресурсів та кваліфікації персоналу.

Для кращого розуміння було наведено рис. 3.4, на якому зображено інтерфейс програми Splunk.

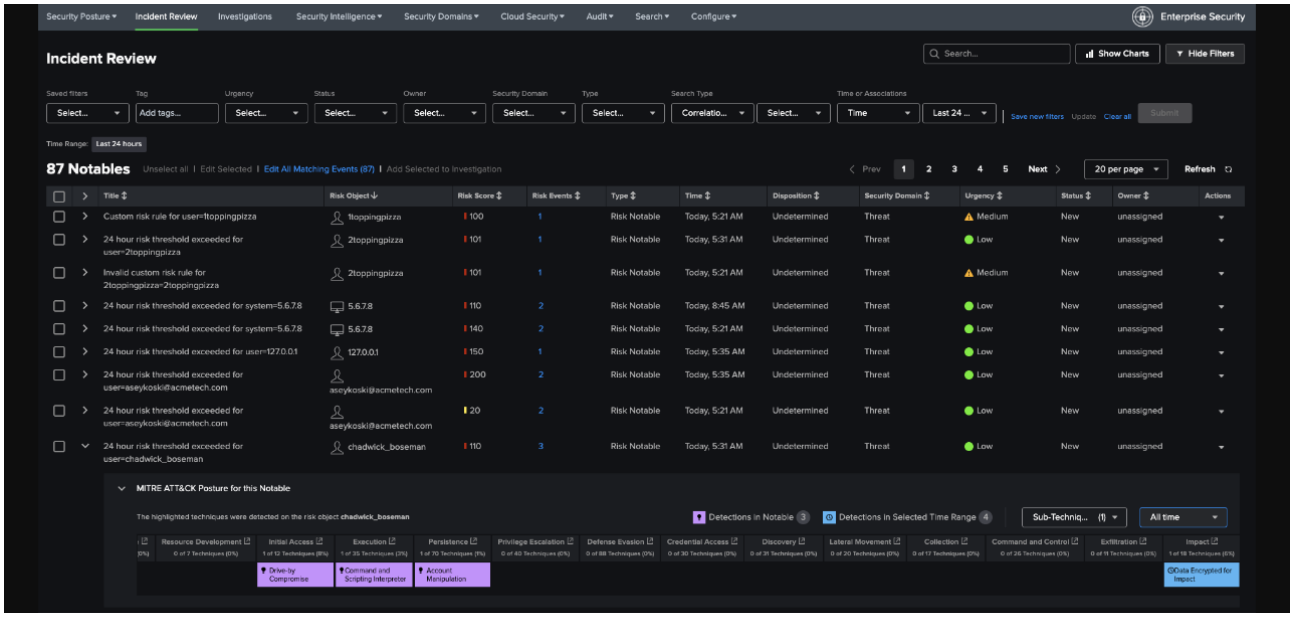

Рис. 3.4. Інтерфейс програми Splunk

Wireshark [25], у свою чергу, є провідним інструментом для аналізу мережевого трафіку. Він дозволяє захоплювати та аналізувати дані пакетів, що проходять через мережу, що робить його незамінним для діагностики мережевих проблем, дослідження безпеки та навчальних цілей. Wireshark відомий своєю детальністю та точністю аналізу, що дозволяє користувачам досліджувати пакети на найнижчому рівні.

Однією з ключових переваг Wireshark є його відкритий код, що робить його безкоштовним і доступним для всіх. Це також сприяє активному розвитку інструменту спільнотою користувачів.

Недоліками Wireshark є те, що для ефективного використання потрібні глибокі знання мережевих протоколів та структури пакетів. Крім того, Wireshark менш підходить для аналізу великих обсягів даних та не забезпечує можливостей для створення дашбордів або інтеграції з іншими системами, як це робить Splunk.

Для кращого розуміння ключових аспектів кожної з програм, запропоновано порівняльну діаграму (рис. 3.5).

Рис. 3.5. Порівняльна діаграма інструментів Splunk та Wireshark

Ця діаграма ілюструє відмінності між Splunk та Wireshark за різними характеристиками, включаючи аналіз даних, мережевий аналіз, роботу в реальному часі, інтерфейс, вартість, деталізацію та налаштування.

Підсумовуючи, Splunk є потужним інструментом для аналізу великих обсягів даних та створення аналітичних звітів, проте може бути дорогим і складним у налаштуванні. Wireshark, з іншого боку, є відмінним вибором для детального аналізу мережевого трафіку, є безкоштовним, але потребує глибоких технічних знань для ефективного використання та не підходить для аналізу великих обсягів даних або створення комплексних звітів.

4. Системи для управління ІБ та подіями (SIEM): ArcSight, QRadar і AlienVault – це три провідні SIEM-системи, кожна з яких має свої особливості, переваги та недоліки. Далі розглянуто ключові характеристики цих програм, порівняно їх функціональні можливості, переваги та недоліки, а також представлено діаграму для візуалізації порівняння.

ArcSight [26] є продуктом компанії Micro Focus, який пропонує потужні можливості для збору, аналізу та кореляції даних безпеки. Ця платформа відзначається своєю масштабованістю та гнучкістю, що дозволяє використовувати її як у великих організаціях, так і в середніх бізнесах. Основні переваги ArcSight включають високий рівень автоматизації процесів безпеки, широкі можливості інтеграції з іншими системами та гнучкість у налаштуванні кореляційних правил. Проте, ArcSight має й недоліки, серед яких складність налаштування та висока вартість впровадження та підтримки.

QRadar [27] від IBM є однією з найпопулярніших SIEM-систем на ринку завдяки своїй надійності та інтелектуальним можливостям аналізу загроз. QRadar відзначається високою точністю виявлення інцидентів безпеки завдяки потужному механізму кореляції подій і використанню машинного навчання. Серед переваг QRadar можна виділити його здатність швидко обробляти великі обсяги даних, простоту налаштування та високу продуктивність. Недоліки QRadar включають високу вартість ліцензії та потребу в значних ресурсах для ефективного функціонування. Інтерфейс QRadar представлено на рис. 3.6 [16].

Рис. 3.6. Інтерфейс програми IBM QRadar

AlienVault [28], тепер відомий як AT&T Cybersecurity, пропонує більш доступне рішення для управління ІБ. Ця платформа об'єднує в собі SIEM, управління вразливостями та моніторинг мережі, що робить її привабливою для малого та середнього бізнесу. Основні переваги AlienVault включають легкість впровадження, доступну вартість та інтеграцію з Open Threat Exchange для обміну інформацією про загрози. Проте, AlienVault має свої недоліки, такі як обмежена масштабованість для великих організацій та менш розвинені можливості кореляції подій порівняно з ArcSight та QRadar.

Далі на рис. 3.7 показано порівняння основних характеристик цих трьох платформ, зокрема функціональні можливості, вартість впровадження та підтримки, простоту використання та масштабованість.

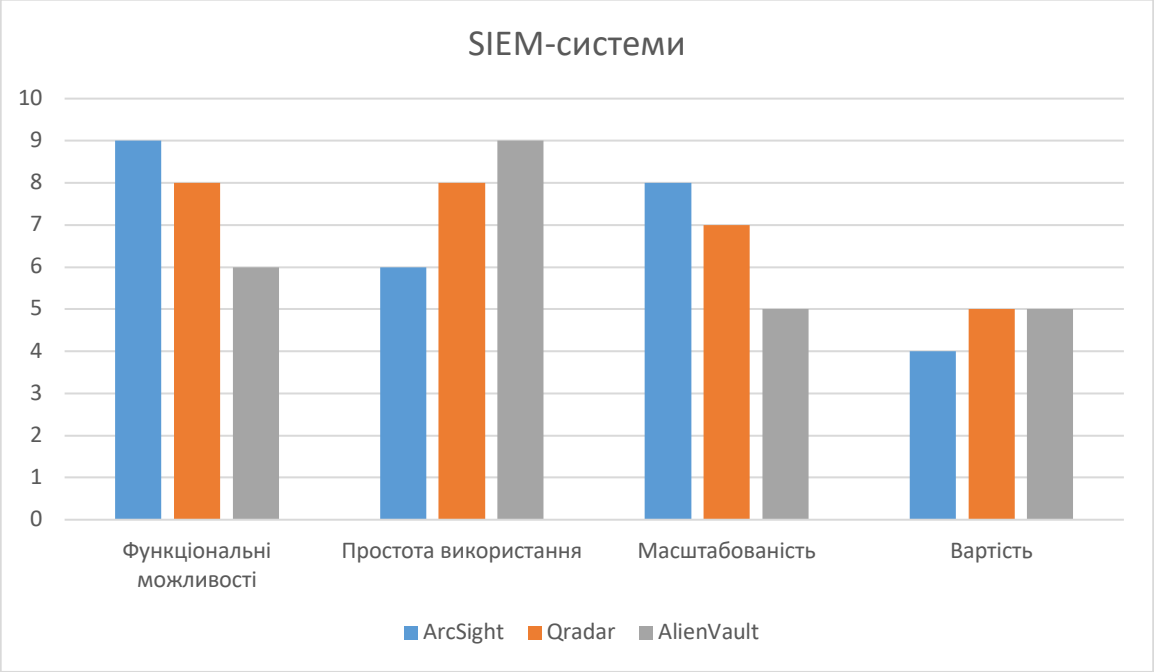

Рис. 3.7. Порівняльна діаграма ArcSight, QRadar і AlienVault

На основі вищевикладеного можна зробити висновок, що кожна з розглянутих SIEM-систем має свої унікальні переваги та недоліки, що робить їх підходящими для різних типів організацій. Вибір конкретного рішення залежить від потреб і ресурсів організації, її масштабу та специфіки ІБ.

5. Інструменти аналізу шкідливого ПЗ. Cuckoo Sandbox та VirusTotal є двома популярними інструментами для аналізу шкідливого ПЗ, кожен з яких має

свої унікальні особливості, переваги та недоліки. Cuckoo Sandbox [29] – це потужний інструмент для динамічного аналізу шкідливого ПЗ, який дозволяє користувачам виконувати підозрілі файли в ізольованому середовищі та спостерігати за їхньою поведінкою. Він надає детальні звіти про системні зміни, мережевий трафік, та взаємодії з файловою системою. Оскільки Cuckoo Sandbox є відкритим кодом, він може бути налаштований під конкретні потреби користувача, що робить його гнучким інструментом для кібербезпеки.Для кращого розуміння нижче наведено рис. 3.8. Проте, використання Cuckoo Sandbox вимагає технічних знань для встановлення та конфігурації, а також значних ресурсів для запуску та аналізу великих обсягів файлів. Це може стати перешкодою для малих організацій або користувачів без відповідного технічного досвіду.

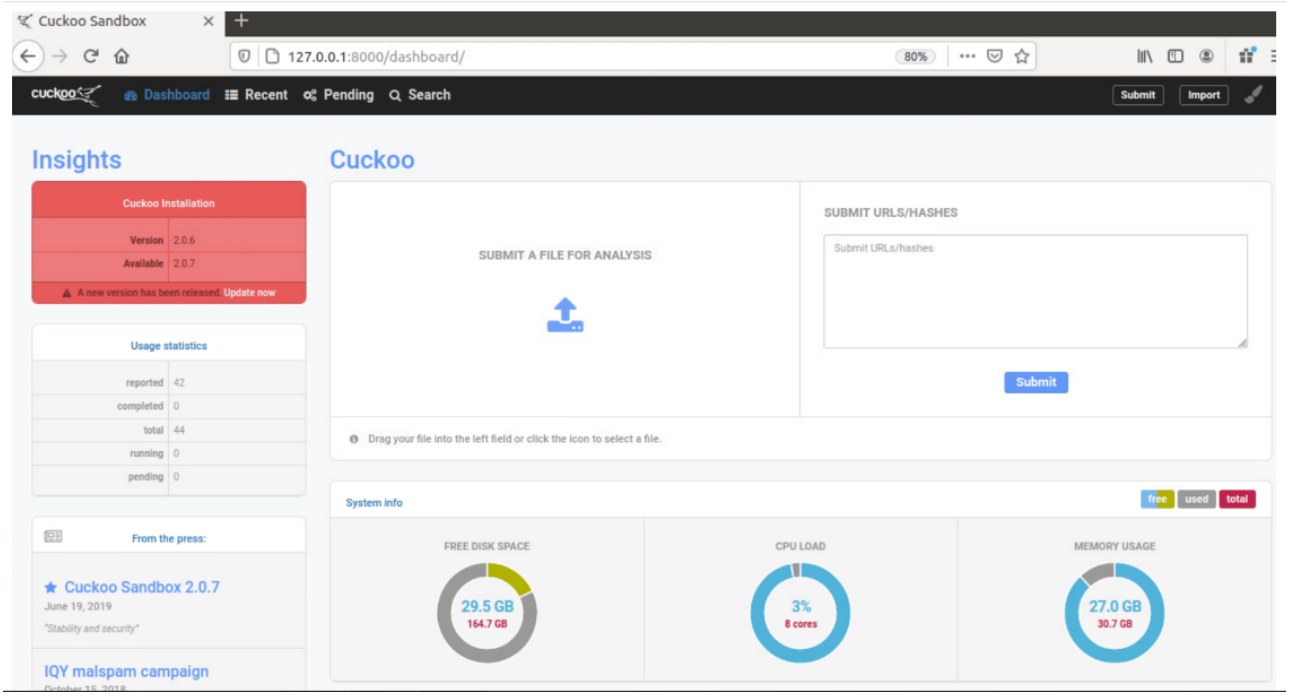

Рис. 3.8. Інтерфейс програми Cuckoo Sandbox [17]

VirusTotal [30], з іншого боку, є веб-службою, яка дозволяє користувачам завантажувати файли та URL-адреси для аналізу за допомогою більш ніж 70 антивірусних програм та сканерів. Цей інструмент дуже зручний у використанні, оскільки він не вимагає установки та конфігурації. VirusTotal швидко надає користувачам результати з багатьох джерел, що дозволяє отримати комплексне

уявлення про потенційну загрозу. Проте, основним недоліком VirusTotal є те, що він лише виконує статичний аналіз файлів та URL-адрес, що не завжди дозволяє виявити складніші шкідливі програми, які використовують динамічні техніки маскування.

Основними перевагами Cuckoo Sandbox є його гнучкість, можливість налаштування та детальний динамічний аналіз. До недоліків можна віднести складність установки та необхідність значних ресурсів. VirusTotal, навпаки, вирізняється простотою використання, швидкістю отримання результатів та можливістю сканування через велику кількість антивірусних програм. Однак, обмеженням VirusTotal є лише статичний аналіз та залежність від баз даних антивірусних програм.

Щоб наочно продемонструвати відмінності між Cuckoo Sandbox і VirusTotal, нижче представлено рис. 3.9, що порівнює основні характеристики цих двох інструментів.

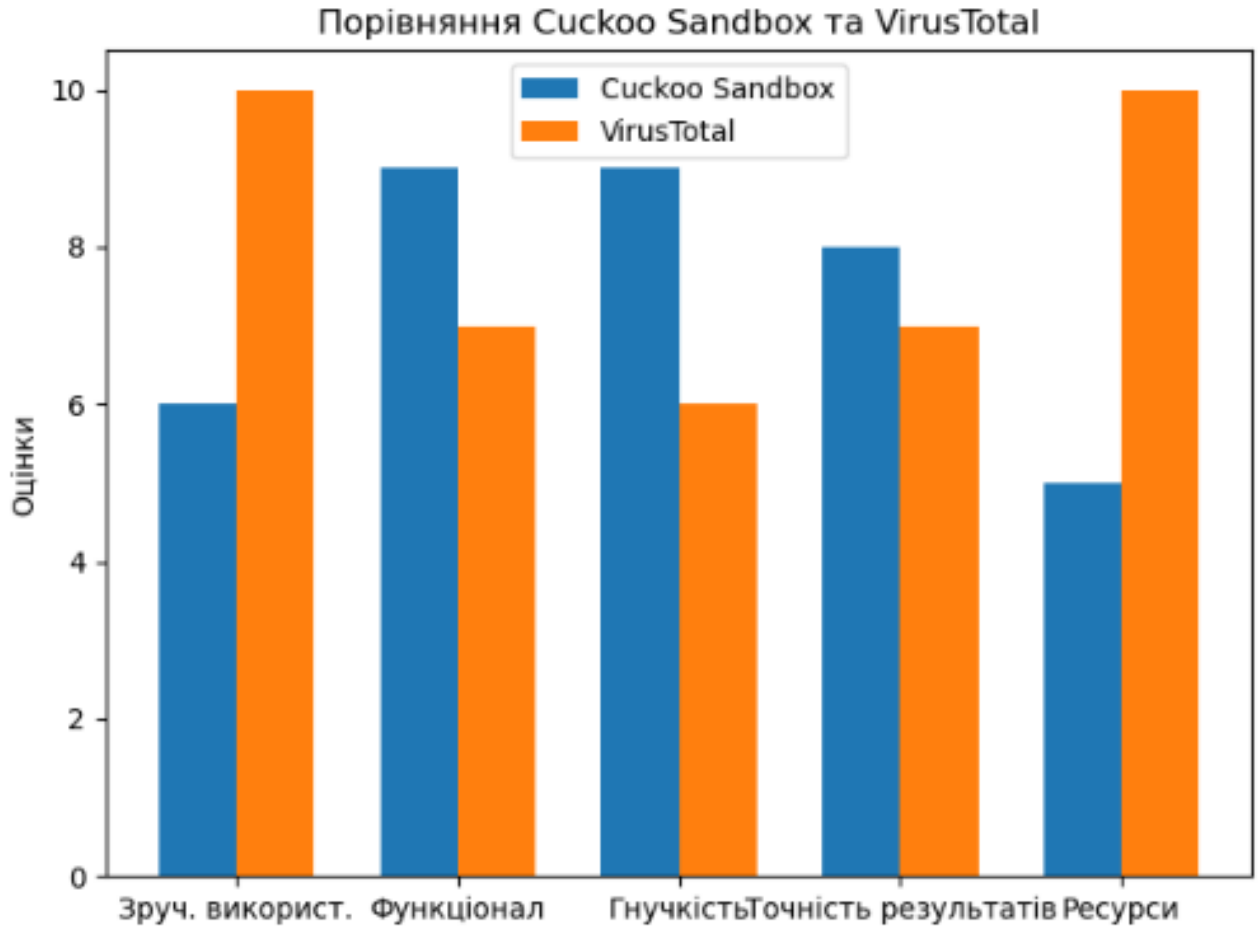

Рис. 3.9. Порівняльна діаграма Cuckoo Sandbox та VirusTotal

Так як ці програми безкоштовні, то вартість не була додана до порівняльної характеристики цих програм.

В цілому, вибір між Cuckoo Sandbox і VirusTotal залежить від конкретних потреб користувача або організації. Для глибокого та детального аналізу шкідливого ПЗ з використанням динамічних методів Cuckoo Sandbox є більш підходящим інструментом. Водночас, для швидкого та зручного сканування великої кількості файлів на наявність відомих загроз VirusTotal є оптимальним вибором.

6. Інструменти оцінки конфігурації та відповідності вимогам безпеки. Tripwire та CIS-CAT. Обидві програми призначені для моніторингу конфігурацій та виявлення змін, проте мають різні підходи до виконання своїх функцій та різні можливості.

Tripwire [31] – це система виявлення змін у файлах і каталогах, яка працює на основі створення та перевірки контрольних сум файлів. Програма використовується для виявлення несанкціонованих змін у файловій системі, що може свідчити про можливі загрози безпеці. Tripwire має потужний механізм конфігурації, який дозволяє налаштовувати правила перевірки для різних типів файлів та каталогів. Програма також надає можливість генерувати звіти про зміни, що можуть бути використані для аудиту та аналізу.

Серед переваг Tripwire можна виділити:

- високий рівень точності у виявленні змін;
- гнучкість у налаштуванні правил перевірки;
- можливість інтеграції з іншими системами безпеки.

Однак, Tripwire має і свої недоліки:

- висока складність налаштування та управління;
- високі вимоги до ресурсів, особливо на великих системах;
- відсутність деяких функцій, таких як автоматичне виправлення конфігурацій.

CIS-CAT (CIS Configuration Assessment Tool) [32] – це інструмент для оцінки відповідності конфігурацій системи стандартам безпеки, розробленим

Center for Internet Security (CIS). CIS-CAT дозволяє автоматично перевіряти конфігурації операційних систем, баз даних, веб-серверів та інших програм на відповідність рекомендаціям CIS. Програма генерує докладні звіти про відповідність конфігурацій, що можуть бути використані для аудиту та виправлення виявлених недоліків. Для кращого розуміння на рис. 3.10 зображений інтерфейс програми CIS-CAT.

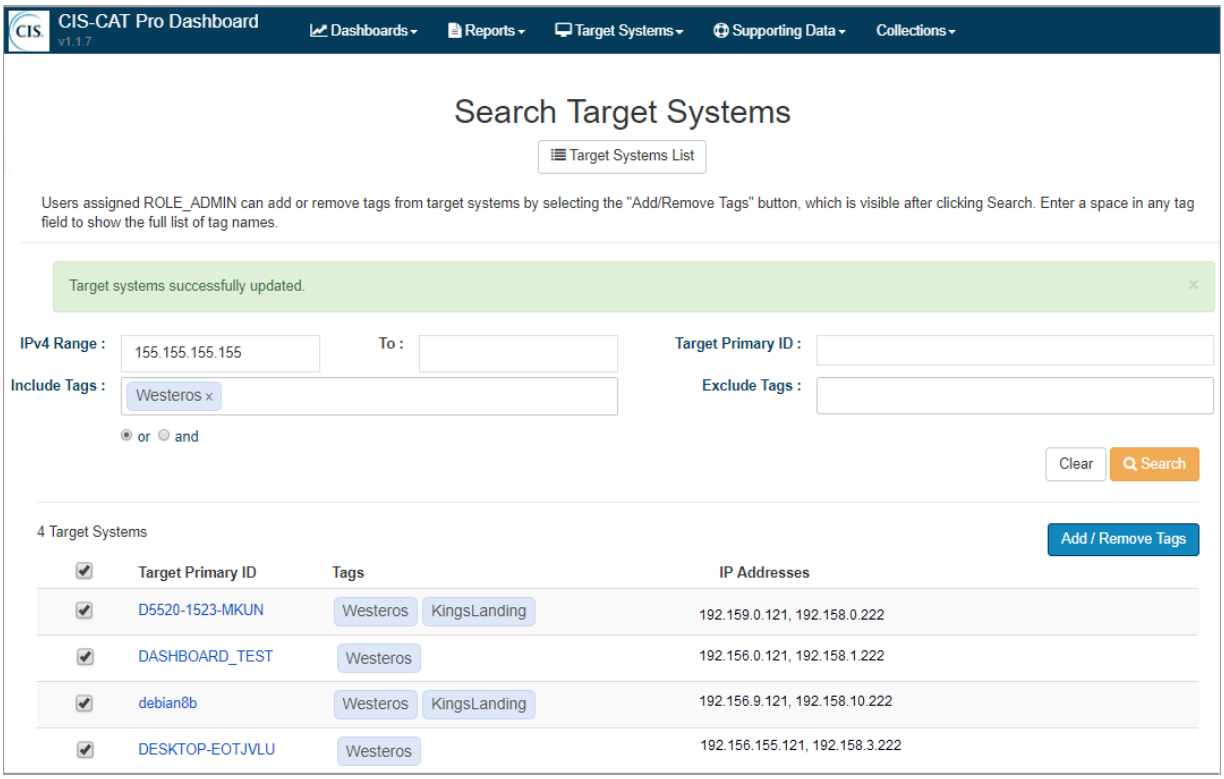

Рис. 3.10. Інтерфейс програми Cis-Cat Pro [21]

Переваги CIS-CAT включають:

- простота у використанні завдяки готовим шаблонам перевірок;
- можливість швидкої оцінки відповідності конфігурацій стандартам ІБ;
- інтеграція з іншими інструментами для автоматизації виправлення конфігурацій;

Серед недоліків CIS-CAT варто відзначити:

- обмежена гнучкість у налаштуванні перевірок порівняно з Tripwire.;
- менший набір функцій для виявлення змін у файловій системі;

- залежність від стандартів CIS, що може бути недостатнім для специфічних вимог деяких організацій;

На рис. 3.11 нижче представлено порівняння основних функцій Tripwire та CIS-CAT, що дозволяє наочно побачити відмінності між цими двома інструментами.

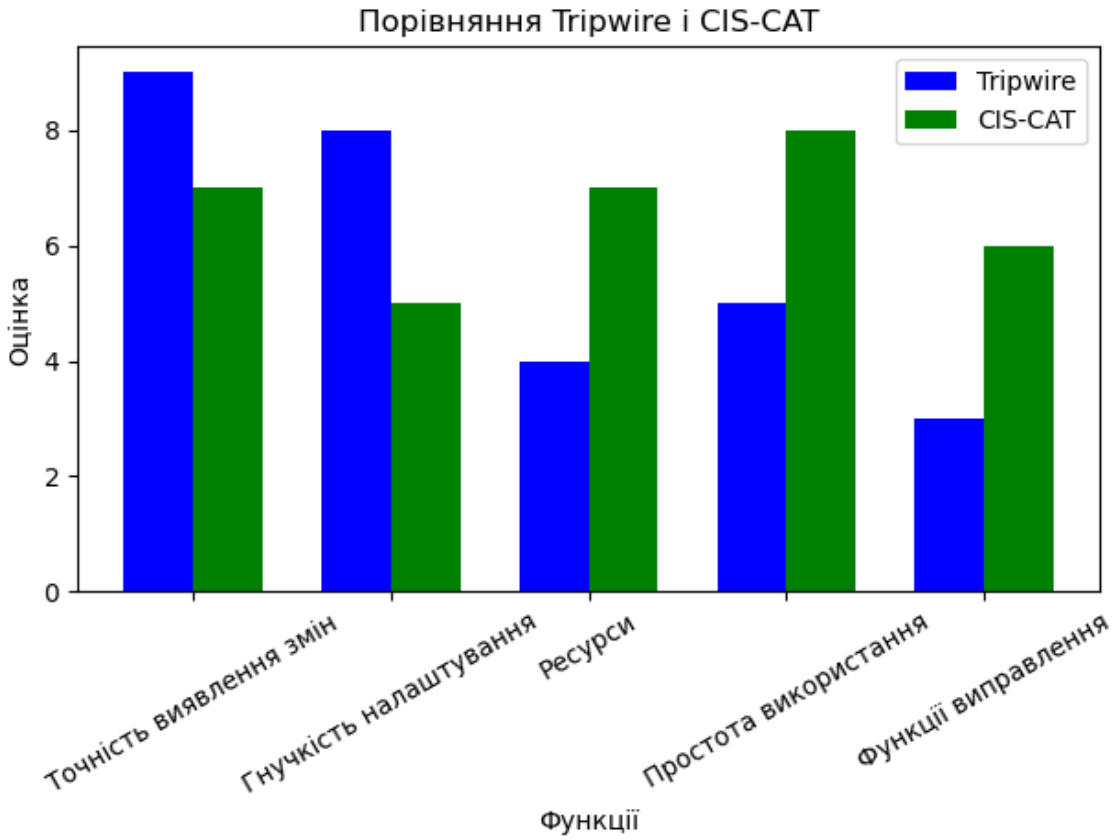

Рис. 3.11. Порівняльна діаграма Tripwire та CIS-CAT

Таким чином, вибір між Tripwire та CIS-CAT залежить від конкретних потреб організації. Tripwire підходить для більш детального моніторингу змін у файловій системі, тоді як CIS-CAT забезпечує швидку та просту оцінку відповідності конфігурацій стандартам безпеки. Обидва інструменти мають свої сильні та слабкі сторони, і оптимальний вибір залежить від специфіки завдань, що стоять перед командою ІБ.

7. Інструменти управління ризиками. RSA Archer та ServiceNow GRC (Governance, Risk, and Compliance) є двома провідними рішеннями у сфері управління ризиками, відповідності та корпоративного управління. Обидві

платформи пропонують потужні інструменти для автоматизації та покращення процесів GRC, але мають свої унікальні особливості та відмінності.

RSA Archer [33], розроблена компанією RSA Security, відома своєю високою адаптивністю та масштабованістю. Вона дозволяє організаціям налаштовувати свої рішення відповідно до специфічних потреб, використовуючи різні модулярні компоненти. Archer пропонує багатий набір функцій для управління ризиками, відповідністю, безпекою інформації та інцидентами. Однією з головних переваг Archer є її здатність інтегруватися з різними системами та інструментами, що дозволяє створити єдину платформу для управління всіма аспектами GRC.

ServiceNow GRC [34], з іншого боку, є частиною платформи ServiceNow, відомої своїми рішеннями для управління IT та бізнес-процесами. ServiceNow GRC забезпечує інтеграцію з іншими продуктами ServiceNow, що дозволяє використовувати єдину платформу для управління як IT, так і бізнес-процесами. ServiceNow GRC пропонує інтуїтивно зрозумілий інтерфейс, що спрощує процес навчання та використання. Крім того, платформа надає можливості для автоматизації процесів за допомогою робочих процесів та скриптів, що дозволяє зменшити ручну роботу та підвищити ефективність. Інтерфейс ServiceNow GRC представлено на рис. 3.12.

З точки зору функціональності, обидві платформи пропонують аналогічні можливості для управління ризиками, відповідністю та аудитом. Вони обидві підтримують моделі оцінки ризиків, моніторинг відповідності, управління політиками та процедурами, а також управління інцидентами. Однак, RSA Archer пропонує більш гнучкі можливості налаштування, що може бути критично важливим для організацій з унікальними потребами. ServiceNow GRC, з іншого боку, виграє у зручності використання та інтеграції з іншими продуктами ServiceNow, що може бути важливим для організацій, які вже використовують інші рішення цієї платформи.

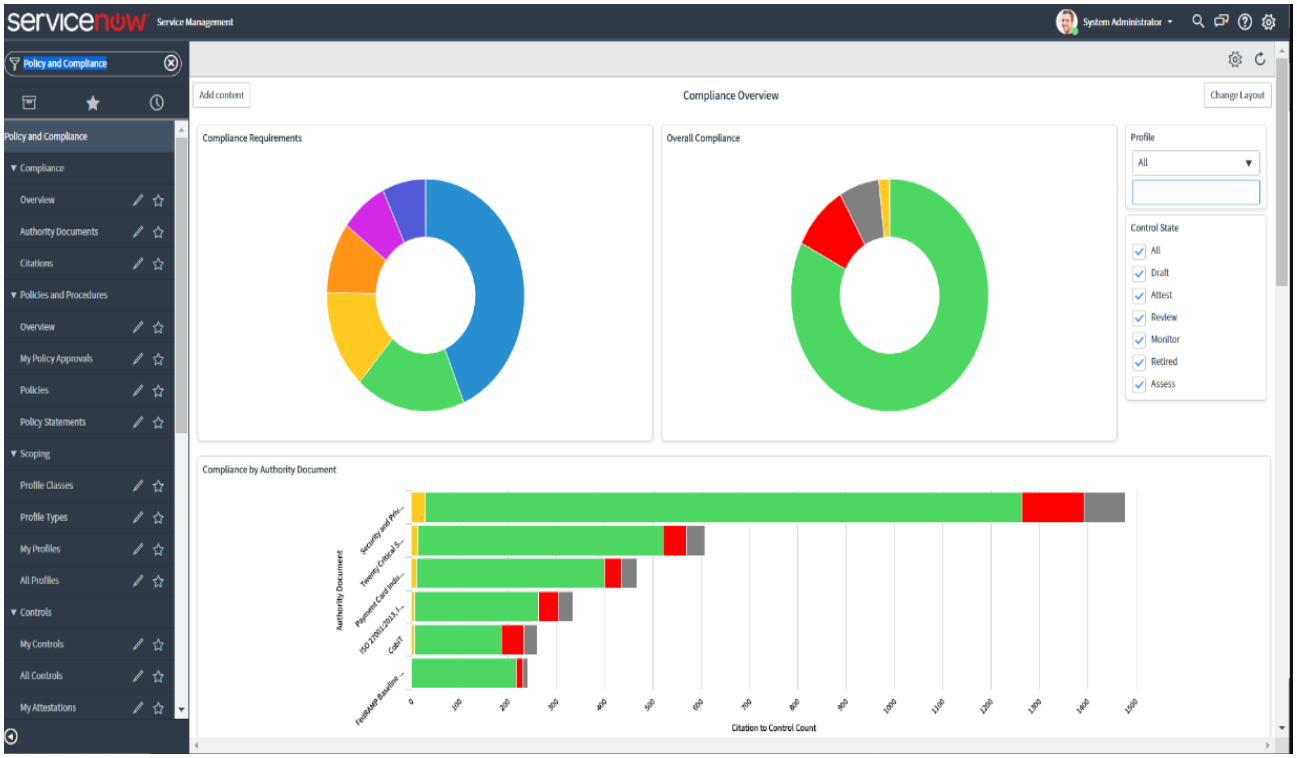

Рис. 3.12. Інтерфейс ServiceNow GRC

У питаннях вартості, обидві платформи знаходяться у високому ціновому діапазоні, але конкретні витрати залежать від масштабів впровадження та обраних модулів. RSA Archer може бути дорожчою через високу гнучкість та адаптивність, у той час як ServiceNow GRC пропонує більш зручну модель ціноутворення, особливо для організацій, які вже використовують інші сервіси ServiceNow.

Загалом, вибір між RSA Archer та ServiceNow GRC залежить від конкретних потреб організації. Якщо потрібна платформа з високим рівнем налаштування та можливістю інтеграції з різними системами, RSA Archer може бути кращим вибором. Якщо треба інтегроване рішення з інтуїтивно зрозумілим інтерфейсом та можливістю автоматизації процесів, ServiceNow GRC може бути більш підходящим варіантом.

На рис. 3.13 зображена порівняльна діаграма розглянутих рішень. Ця діаграма ефективності демонструє порівняльні оцінки для RSA Archer та ServiceNow GRC за різними критеріями. Як видно, RSA Archer виграє у

гнучкості налаштування, тоді як ServiceNow GRC перевершує у зручності використання та інтеграції.

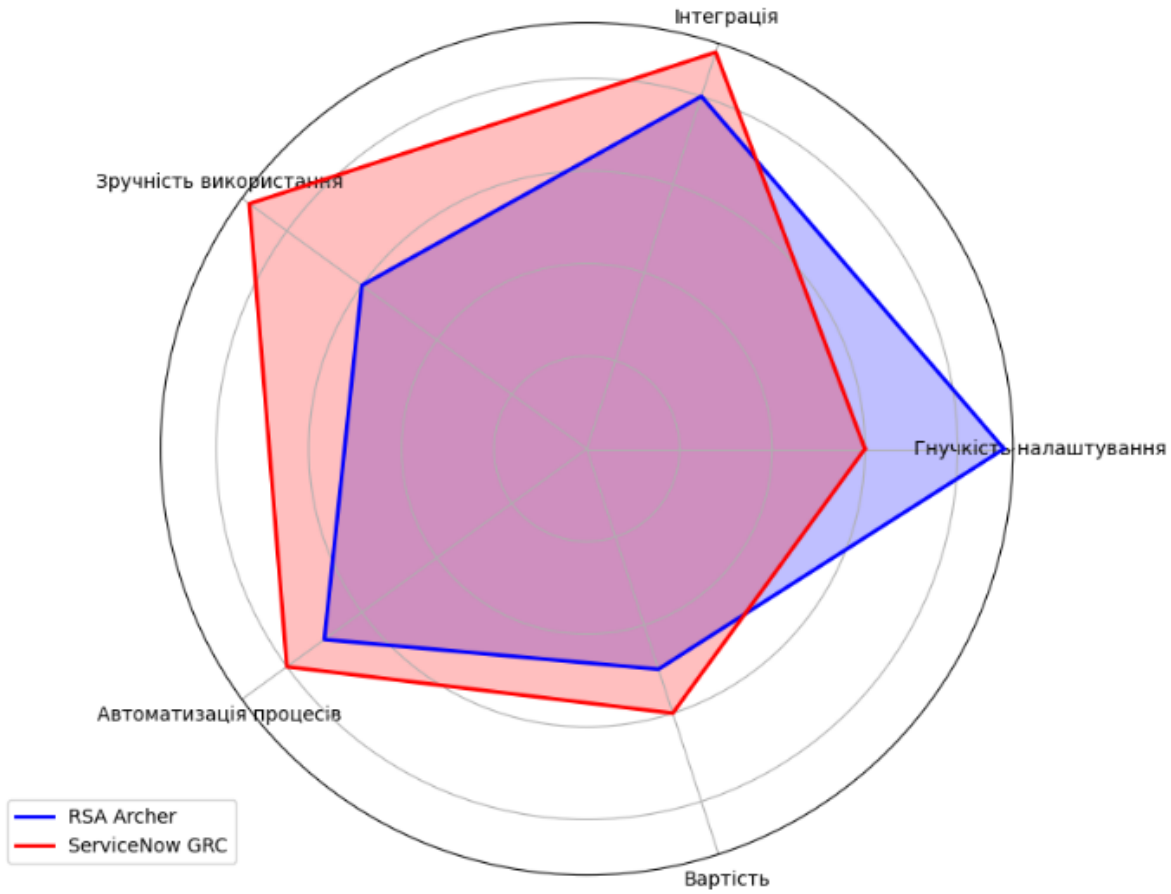

Рис. 3.13. Порівняльна діаграма RSA Archer та ServiceNow GRC

Також було додано узагальнені дані щодо вартості для всіх розглянутих інструментів аудиту ІБ. Ціни можуть значно варіюватися залежно від декількох факторів, включаючи кількість користувачів, обсяг даних, що обробляються, і рівень функціональності, який потрібен організації. Нижче наведені деякі загальні уявлення про те, як розраховуються ці ціни на місяць (рис. 3.14) та на рік (рис. 3.15).

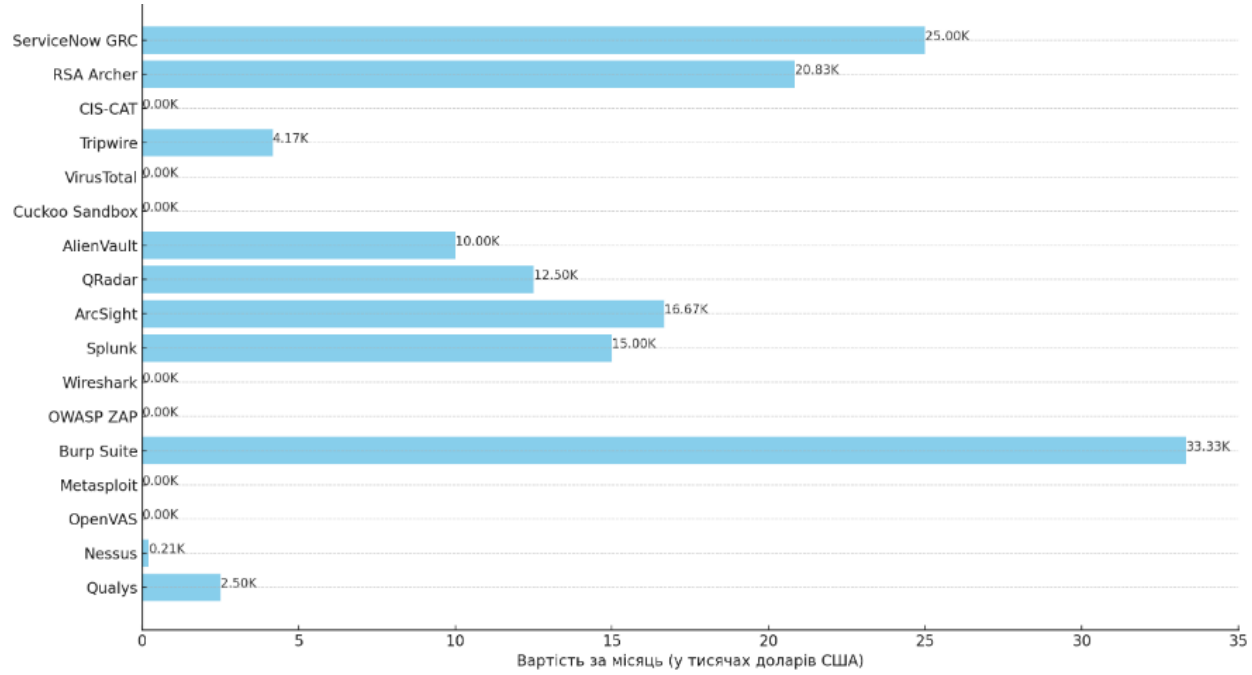

Рис. 3.14. Ціна інструментів за місяць користування

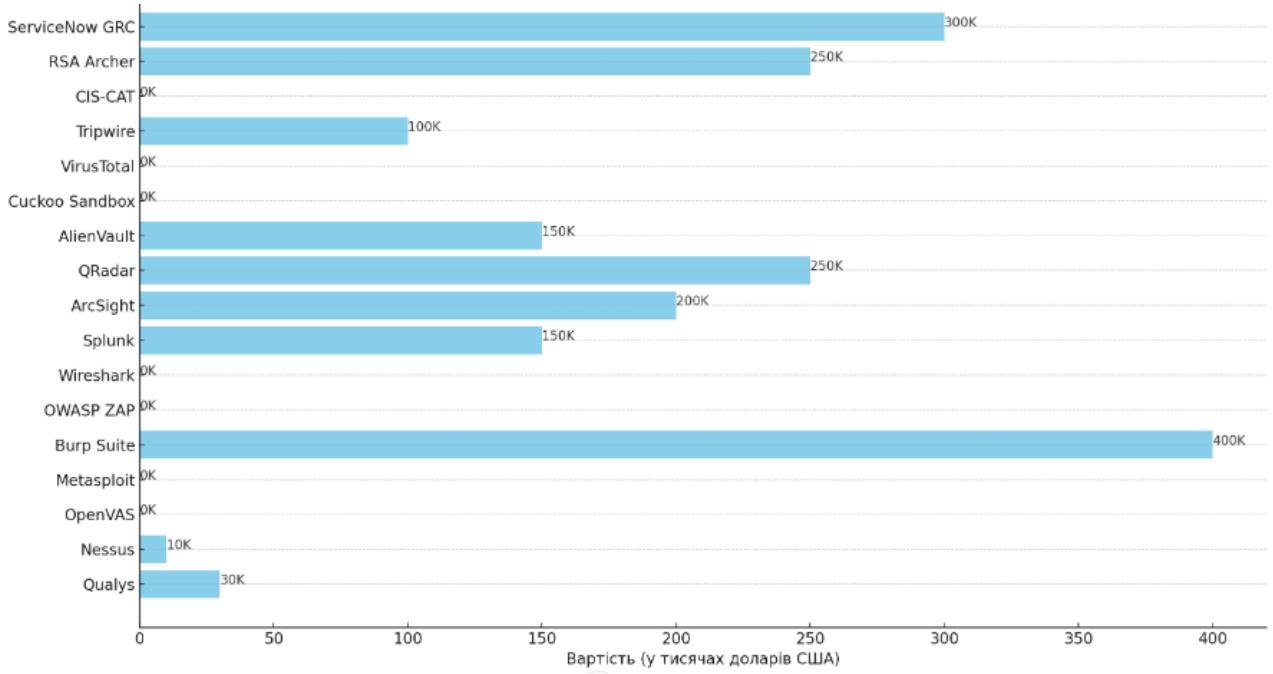

Рис. 3.15. Ціна інструментів за рік користування

- Qualys. Зазвичай ліцензія розрахована на кілька сотень до тисячі пристроїв. Вартість може змінюватись залежно від кількості сканів і пристроїв;

- Nessus (Tenable.io Vulnerability Management). Ліцензія може покривати від декількох десятків до кількох сотень пристроїв. Ціна може варіюватися в залежності від кількості IP-адрес або пристроїв;
- OpenVAS. Це безкоштовний інструмент, тому немає обмежень по кількості користувачів;
- Metasploit (Community Edition). Безкоштовна версія має обмежені можливості, але вона не обмежена за кількістю користувачів;
- Burp Suite (Enterprise Edition). Ліцензія зазвичай розрахована на певну кількість одночасних користувачів або інстанцій. Може включати від декількох до кількох десятків користувачів;
- OWASP ZAP. Безкоштовний інструмент, тому немає обмежень по кількості користувачів;
- Wireshark. Безкоштовний інструмент, тому немає обмежень по кількості користувачів;
- Splunk. Вартість залежить від обсягу даних, що індексуються, а не від кількості користувачів. Може підтримувати велику кількість користувачів;
- ArcSight.Вартість розраховується на основі обсягу даних та кількості джерел логів. Може підтримувати великі організації з великою кількістю користувачів;
- QRadar. Ліцензія залежить від обсягу даних, що обробляються, і може підтримувати багато користувачів;
- AlienVault (USM Anywhere).Ліцензія розрахована на кількість активів або пристроїв і може варіюватися від декількох десятків до декількох сотень пристроїв;
- Cuckoo Sandbox. Безкоштовний інструмент, тому немає обмежень по кількості користувачів;
- VirusTotal. Безкоштовний інструмент, тому немає обмежень по кількості користувачів;

- Tripwire. Вартість може залежати від кількості пристроїв або кінцевих точок, що моніторяться. Зазвичай розрахована на кілька сотень пристроїв;
- CIS-CAT. Безкоштовний інструмент, тому немає обмежень по кількості користувачів;
- RSA Archer.Ліцензія зазвичай розрахована на кількість користувачів і може варіюватися від десятків до сотень користувачів;
- ServiceNow GRC. Вартість залежить від кількості користувачів і функціональних модулів, які використовуються, і може покривати від десятків до сотень користувачів.

Таким чином, ціни, наведені вище, можуть сильно варіюватися в залежності від конкретних умов і потреб організації.

3.2 Вибір оптимального рішення щодо використовуваних інструментів аудиту ІБ

При виборі оптимального рішення щодо використовуваних інструментів аудиту ІБ важливо враховувати низку факторів, включаючи вартість, функціональні можливості, сумісність з існуючою інфраструктурою, технічну підтримку та можливість масштабування [35]. Вартість є одним з основних факторів, оскільки бюджет може суттєво обмежити доступні варіанти. Наприклад, інструменти, такі як OpenVAS, OWASP ZAP, Wireshark, Cuckoo Sandbox та VirusTotal, є безкоштовними та можуть бути дуже привабливими для організацій з обмеженими фінансовими ресурсами. Водночас, безкоштовні інструменти можуть вимагати більше часу на налаштування та технічну підтримку, що потрібно враховувати при їх виборі [36].

З іншого боку, комерційні рішення, такі як Qualys, Nessus, Burp Suite, Splunk, ArcSight, QRadar, AlienVault, Tripwire, RSA Archer та ServiceNow GRC, пропонують більш широкий спектр можливостей, технічну підтримку та регулярні оновлення, що може виправдовувати їх високу вартість. Наприклад, Qualys і Nessus забезпечують високий рівень автоматизації та точність виявлення

вразливостей, що значно спрощує процес управління ризиками. Burp Suite є потужним інструментом для тестування безпеки веб-додатків, що дозволяє виявляти та виправляти вразливості на ранніх етапах розробки. Splunk та інші SIEM-системи, такі як ArcSight і QRadar, забезпечують ефективний збір та аналіз логів, що дозволяє виявляти аномалії та реагувати на інциденти безпеки в реальному часі [37].

Сумісність з існуючою інфраструктурою також є важливим фактором при виборі інструментів. Наприклад, якщо організація вже використовує певні системи управління подіями безпеки або інші інструменти, важливо переконатися, що нові інструменти будуть інтегруватися з ними без проблем. Наприклад, інструменти, такі як RSA Archer та ServiceNow GRC, можуть бути легко інтегровані з іншими системами управління та забезпечити централізоване управління ризиками та відповідністю нормативним вимогам.

Технічна підтримка і можливість масштабування є ключовими аспектами, особливо для великих організацій, які потребують стабільної роботи інструментів і можливості їх розширення в міру зростання організації. Комерційні рішення зазвичай пропонують різні рівні технічної підтримки, що може бути критично важливим у разі виникнення проблем або необхідності у швидкому оновленні. Наприклад, Splunk та QRadar відомі своєю масштабованістю та можливістю обробляти великі обсяги даних, що робить їх підходящими для великих корпоративних мереж [38].

Таким чином, вибір оптимального рішення щодо використовуваних інструментів аудиту ІБ залежить від конкретних потреб та можливостей організації. Безкоштовні інструменти можуть бути ефективними для малих організацій або окремих проектів, тоді як комерційні рішення надають більш широкі можливості та підтримку, що може бути необхідним для великих компаній з складними ІС. У будь-якому випадку, важливо ретельно аналізувати можливості кожного інструменту та враховувати всі фактори, щоб забезпечити максимально ефективний захист ІБ [39].

3.3 Розробка рекомендацій щодо вдосконалення методів аудиту ІБ

У світлі сучасних викликів і зростаючих загроз ІБ, вдосконалення методів аудиту ІБ стає критично важливим для забезпечення надійного захисту ІС і даних. Представляю вам рекомендації, спрямовані на підвищення ефективності аудиту ІБ, які базуються на сучасних тенденціях та кращих практиках у цій галузі [40].

Перш за все, необхідно впровадити ризик-орієнтований підхід до аудиту ІБ. Це означає, що аудитори повинні зосереджуватися на тих областях, де існує найбільший ризик для безпеки інформації. Аналіз ризиків допоможе визначити пріоритетні зони перевірок і відповідно планувати аудит. Використання сучасних інструментів і методологій для оцінки ризиків, таких як ISO/IEC 27005, дозволить більш точно ідентифікувати і оцінювати ризики [41].

Другим важливим аспектом є автоматизація процесів аудиту. Використання спеціалізованих програмних засобів для моніторингу та аналізу ІС дозволить скоротити час на проведення аудиту та підвищити його точність. Автоматизовані інструменти можуть збирати і аналізувати великі обсяги даних у реальному часі, що дозволить швидко виявляти аномалії і потенційні загрози [42].

Важливо також звернути увагу на постійне навчання і підвищення кваліфікації аудиторів. ІБ є динамічною сферою, яка постійно розвивається. Тому аудитори повинні бути в курсі новітніх технологій, методів атак і захисту. Регулярні тренінги та участь у професійних конференціях сприятимуть зростанню професійних знань та навичок.

Окремо слід зазначити необхідність інтеграції аудиту ІБ у загальну систему управління організацією. Аудитори повинні тісно співпрацювати з іншими підрозділами, такими як ІТ-відділ, відділ ризик-менеджменту та юридичний відділ. Така співпраця дозволить більш ефективно ідентифікувати вразливі місця і розробляти комплексні заходи з їх усунення [43].

Рекомендується також використовувати стандарти і кращі практики у галузі ІБ, такі як ISO/IEC 27001, NIST SP 800-53 та інші. Використання визнаних стандартів дозволяє забезпечити системний підхід до забезпечення безпеки і підвищити довіру до результатів аудиту [44].

Нарешті, важливо впровадити регулярні внутрішні та зовнішні аудити для оцінки ефективності заходів ІБ. Постійний моніторинг та оцінка дозволять своєчасно виявляти недоліки і впроваджувати необхідні покращення.

Отже, вдосконалення методів аудиту ІБ є багатогранним процесом, що включає ризик-орієнтований підхід, автоматизацію, постійне навчання, інтеграцію з іншими підрозділами, використання стандартів та регулярний моніторинг. Лише комплексний підхід дозволить забезпечити надійний захист інформаційних активів організації та своєчасно реагувати на нові виклики і загрози [45].

Висновки до розділу 3

У розділі було проведено порівняльний аналіз інструментів аудиту ІБ. Отримані результати оцінювання ефективності інструментів аудиту ІБ свідчать про те, що ефективність інструменту залежить від його здатності відповідати конкретним потребам організації, а також від його вартості, функціональних можливостей, сумісності з існуючими системами, наявності технічної підтримки та можливості масштабування. Вартість інструменту є критичним аспектом, оскільки бюджетні обмеження можуть суттєво впливати на рішення.

Таким чином, вибір конкретного інструменту залежить від потреб організації, її бюджету та технічних вимог. Комерційні рішення пропонують розширені функціональні можливості та технічну підтримку, тоді як безкоштовні інструменти можуть бути ефективними для малих організацій або окремих проєктів. Виходячи з отриманих результатів, можна сказати, що кожен інструмент має свої переваги та недоліки, і їхній вибір повинен базуватися на ретельному аналізі можливостей та вимог до безпеки.

Також було розроблено рекомендації щодо вдосконалення методів аудиту ІБ. Було запропоновано ризик-орієнтований підхід до аудиту ІБ, постійне навчання і підвищення кваліфікації аудиторів, автоматизацію та інтеграцію для покращення ефективності ІБ.

ВИСНОВКИ

У ході роботи був проведений аналіз та оцінка ефективності методів та інструментів аудиту ІБ. Були охарактеризовані сутність та принципи, основні методи та інструменти аудиту ІБ, було проведено їх порівняльний аналіз.

В першому розділі було проаналізовано теоретичні основи проведення аудиту. Було визначено принципи аудиту, основними з яких є об’єктивність та незалежність, які гарантують неупередженість аудиторів. Згідно цих принципів аудитори повинні діяти незалежно від організаційних впливів і особистих інтересів, щоб забезпечити точну та чесну оцінку стану ІБ. Комплексність є важливим принципом, що передбачає всебічне охоплення всіх аспектів ІБ, дотримуючись якого аудитори перевіряють всі рівні захисту, включаючи технічні, організаційні та адміністративні заходи. Дотримання систематичності передбачає виконання чітко визначеного плану аудиту, що включає конкретні етапи та методи перевірки. Це допомагає забезпечити послідовність і повноту аудиту, мінімізуючи ризик пропуску важливих аспектів. Було проаналізовано регуляторне середовище у сфері аудиту ІБ, яке представлене такими стандартами як ISO/IEC 27001:2022 , ISO/IEC 27002:2022, NIST SP 800-53 та COBIT.

В другому розділі увагу було приділено аналізу методів та інструментів аудиту ІБ. Було досліджено особливості застосування інструментів аудиту ІБ, до яких належать сканери вразливостей, які автоматично перевіряють системи на наявність відомих вразливостей, інструменти для тестування на проникнення, що імітують атаки зловмисників з метою виявлення слабких місць, системи управління подіями та інформацією про безпеку (SIEM), які збирають та аналізують логи для виявлення аномальних дій, інструменти для аналізу конфігурацій, що перевіряють правильність налаштувань програмного та апаратного забезпечення, ПЗ для моніторингу мережевого трафіку, яке дозволяє виявляти підозрілі дії у режимі реального часу, інструменти для управління політиками безпеки, що допомагають забезпечувати відповідність встановленим стандартам та вимогам, а також інструменти управління ризиками. Було

проаналізовано методи та техніки, які застосовують для проведення аудиту, а саме: тестування на проникнення, аудит конфігурацій, аналіз логів, опитування та інтерв'ю, оцінку відповідності стандартам.

В третьому розділі було проведено порівняльний аналіз досліджуваних інструментів аудиту ІБ, що дозволило сформувати такі висновки: більшість інструментів не мають вагомої переваги над аналогами, вибір інструменту залежить від ресурсів, обсягів, мети організації. На основі проведеного аналізу було розроблено рекомендації щодо вдосконалення методів аудиту ІБ: ризик-орієнтований підхід, автоматизація процесів аудиту, інтеграція аудиту ІБ у загальну систему управління організацією а також постійне підвищення кваліфікації аудиторів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 27001. Information security, cybersecurity and privacy protection – Information security management systems. Effective from 2022-10-25. Official edition. 2022. С. 10-40.

2. General Data Protection Regulation : Постанова від 27.04.2016 р. : станом на 25 трав. 2018 р. С. 10-56 .URL: https://gdpr-info.eu/.

3. Health Insurance Portability and Accountability Act : Закон від 21.08.1996 р. Ст.21-39.URL: https://biz.ligazakon.net/analitycs/225344_hipaa-compliance-v-ukranskomu-kontekst-yak-pratsyuvati-vtchiznyany-kompan.

4. Control objectives for information and related technologies. Effective from 2019-01-01. Official edition. Шаумбург, США, 2018. С.19-31

5. Special publication 800-53. Effective from 2005-02-28. Official edition. Гейтерсберг, Меріленд ,США.С. 56-124.

6. International association of privacy professionals. International association of privacy professionals. 07.06.2024 . С. 2-5. URL: https://iapp.org/

7. Stuttard D., Pinto M. Web application hacker's handbook: discovering and exploiting security flaws. Wiley & Sons, Incorporated, John, 2011. С. 32-57.

8. Collins R. Network security monitoring: basics for beginners. a practical guide. USA : CreateSpace independent publishing platform, 2017. С. 16-43.

9. Kennedy D. Metasploit: the penetration tester's guide. San Francisco, Calif : No Starch Press, 2011. С. 15-28.

10. Champlain J. J. Auditing information systems. Wiley & Sons, Incorporated, John, 2003. С. 230-255.

11. Calder A. A business guide to information security. Kogan Page, 2006. С. 147-161.

12. Protzman R. Speaking their language: the non-techie's guide to managing IT & cybersecurity for your organization. Standard 3.1 Publishing, 2021. С. 2-7.

13. The Institute of Internal Auditors. Auditing cybersecurity operations: prevention and detection. Institute of Internal Auditors, 2022. С. 1-2.

14. Touhill G. J., Touhill C. J. Cybersecurity for executives: a practical guide. Wiley & Sons, Incorporated, John, 2014. C. 20-38.

15. Davis R. E. Auditing information and cyber security governance. Taylor & Francis Group, 2021. C. 13-16.

16. Blokdyk G. Compliance audit a complete guide - 2020 edition. Emereo Pty Limited, 2020. C. 150-201.

17. Das R. Assessing and insuring cybersecurity risk. Auerbach Publishers, Incorporated, 2021. C. 97-141.

18. Qualys. URL: https://www.trustradius.com/products/qualys-trurisk-platform/reviews?qs=pros-and-cons#product-details

19. Nessus. URL: https://www.g2.com/products/tenable-nessus/reviews

20. OpenVAS. URL: https://www.techradar.com/reviews/openvas

21. Metasploit. URL: https://www.gartner.com/reviews/market/penetration-testing-tools/vendor/rapid7/product/metasploit

22. Burp Suite. URL: https://www.itpro.com/security/burp-suite-review-a-highly-functional-tool-your-business-should-learn-about#:~:text=Burp%20Suite%20is%20a%20highly,developed%20for%20this%20extensive%20product.

23. OWASP ZAP. URL: https://www.capterra.com/p/246914/OWASP-ZAP/

24. Wireshark, URL: https://www.techradar.com/reviews/wireshark

25. Splunk. URL: https://www.g2.com/products/splunk-enterprise/reviews

26. ArcSight. URL: https://www.gartner.com/reviews/market/security-information-event-management/vendor/opentext/product/arcsight-enterprise-security-manager-esm

27. QRadar URL: https://www.g2.com/products/ibm-security-qradar-siem/reviews

28. AlienVault.URL: https://www.trustradius.com/products/alienvault/reviews

29. Cuckoo Sandbox.URL: https://www.g2.com/products/cuckoo-sandbox/reviews

30. VirusTotal.URL: https://www.trustradius.com/products/virustotal/reviews

31. Tripwire. URL: https://www.g2.com/products/tripwire-enterprise/reviews

32. CIS-CAT. URL: https://its.gmu.edu/knowledge-base/what-are-cis-security-benchmark-tools/

33. RSA Archer. URL: https://www.trustradius.com/products/archer-integrated-risk-management-platform/reviews?qs=pros-and-cons

34. ServiceNow GRC. URL: https://www.g2.com/products/servicenow-servicenow-integrated-risk-management/reviews

35. G2 Crowd. URL: https://www.g2.com/

36. Capterra. URL:https://www.capterra.com/

37. TrustRadius URL: https://www.trustradius.com/

38. Reddit. URL: https://www.reddit.com/

39. Stack Overflow. URL: https://stackoverflow.com/

40. Bundesamt für Sicherheit in der Informationstechnik. Standard 100-1, Information Security Management Systems (ISMS), 2008. С.8-36.

41. Vasileiou I., Furnell S. Cybersecurity education for awareness and compliance. IGI Global, 2019. С.18-35.

42. Champlain J. J. Auditing information systems. Wiley & Sons, Incorporated, John, 2008. С. 169-201.

43. The Role of Auditors in Company-Prepared Cybersecurity Information: Present and Future.URL: https://www.thecaq.org/the-role-of-auditors-in-company-prepared-cybersecurity-information-present-and-future

44. “Network Traffic Analysis: A Powerful Tool for Security and Performance – Journal of Computer Networks and Communications”,URL: https://www.zenarmor.com/docs/network-security-tutorials/what-is-network-traffic-analysis-nta

45. Sergeja Slapnicar ,Marko Čular , Tina Vuko. International Journal of Accounting Information Systems .Effectiveness of cybersecurity audit .2022. С.9-23.URL:https://www.researchgate.net/publication/357861875_Effectiveness_of_cybersecurity_audit