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: “МЕТОДИ ПЕРЕВІРКИ ЕФЕКТИВНОСТІ ЗАСОБІВ ПРОТИДІЇ ІНСАЙДЕРСЬКИМ ЗАГРОЗАМ ПІД ЧАС ВНУТРІШНЬОГО АУДИТУ ІНФОМАЦІЙНОЇ 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

_____ Нікіта МЕЛЬНИЧЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБДМ-61

Нікіта МЕЛЬНИЧЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Іван ОПІРСЬКИЙ
Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____ Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____” _____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мельниченку Нікіті Миколайовичу

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи перевірки ефективності засобів протидії інсайдерським загрозам під час внутрішнього аудиту інфомаційної безпеки”,
керівник кваліфікаційної роботи ОПІРСЬКИЙ Іван, д-р техн. наук, професор

(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. №467

2. Строк подання кваліфікаційної роботи “18” грудня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *система управління* протидії інсайдерським загрозам, *методика аудиту системи управління перевірки, інструменти аудиту, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
Проаналізувати методи та стандарти протидії інсайдерським загрозам під час внутрішнього аудиту, Дослідити структуру системи управління інформаційної безпеки, Проаналізувати методи й інструменти аудиту заходів внутрішнього аудиту інфомаційної безпеки, Розробити рекомендації щодо підвищення ефективності заходів із внутрішнього аудиту інфомаційної безпеки.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “02“ жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10. 2025	
3.	Аналіз теоретичних основ	27.10. 2025	
4.	Дослідження методів проведення аудиту	10.11. 2025	
5.	Розробка рекомендацій щодо підвищення ефективності	15.11. 2025	
6.	Формулювання висновків за результатами проведеного дослідження.	22.11. 2025	
7.	Оформлення роботи.	04.12. 2025	
8.	Оформлення презентації.	14.12. 2025	
9.	Отримання рецензії на роботу.	18.12. 2025	
10.	Захист в ЕК.	20.01. 2025	

Здобувач вищої освіти _____ Нікіта МЕЛЬНИЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Іван ОПІРСЬКИЙ
(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 Мельниченко Н.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи перевірки ефективності засобів протидії інсайдерським загрозам під час внутрішнього аудиту інфомаційної безпеки"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач МЕЛЬНИЧЕНКО Нікіта у кваліфікаційній роботі проаналізував методи та стандарти протидії інсайдерським загрозам під час внутрішнього аудиту; Дослідив структуру системи управління інформаційної безпеки; Проаналізував методи й інструменти аудиту заходів внутрішнього аудиту інфомаційної безпеки; розробив рекомендації щодо підвищення ефективності заходів із внутрішнього аудиту інфомаційної безпеки.

МЕЛЬНИЧЕНКО Нікіта 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 МЕЛЬНИЧЕНКА Нікіти на оцінку "_____" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Іван ОПІРСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Мельниченко Н.М. 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 Мельниченка Нікіти
на тему “ Методи перевірки ефективності засобів протидії інсайдерським загрозам під час внутрішнього аудиту інфомаційної безпеки ”

Актуальність. Методи протидії інсайдерським загрозам під час внутрішнього аудиту інфомаційної безпеки має важливе значення в контексті інформаційної безпеки через її роль у забезпеченні стійкості організації до збоїв. Заходи з протидії інссайдерським загрозам, такі як плани перевірки до появи катастроф та стратегії реагування на інциденти, мають вирішальне значення для підтримки цих цілей безпеки під час несприятливих подій. Ці заходи знижують ризики, забезпечуючи стійкість, мінімізуючи втрату даних, гарантуючи відповідність нормативним вимогам. З огляду на зазначене дослідження методика перевірки ефективності засобів протидії інсайдерським загрозам під час внутрішнього аудиту інфомаційної безпеки є актуальним науковим завданням.

Позитивні сторони.

1. У роботі детально проаналізовано методику перевірки ефективності засобів протидії інсайдерським загрозам в контексті внутрішнього аудиту, досліджено методи їх аудиту, інструменти та показники, які при цьому використовуються.

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: 40 публікацій, в тому числі англомовних.

4. За результатами дослідження запропоновано рекомендації щодо підвищення ефективності компонентів методики перевірки ефективності засобів протидії інсайдерським загрозам у контексті аудиту інфомаційної безпеки.

Недоліки.

1. Доцільно було б більш детально проаналізувати заходи, які мають бути реалізовані на кожному етапі 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 МЕЛЬНИЧЕНКО Нікіта заслуговує присвоєння кваліфікації магістра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____
_____ *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена методиці перевірки ефективності засобів протидії інсайдерським загрозам під час внутрішнього аудиту інфомаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 6 рисунків, висновків і списку використаних джерел із 25 найменувань. Загальний обсяг роботи становить 92 аркушів, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

Мета роботи є розробка методики перевірки ефективності засобів протидії інсайдерським загрозам у межах внутрішнього аудиту інформаційної безпеки.

Об'єктом дослідження є системи, процеси та організаційні механізми інформаційної безпеки, призначені для виявлення, запобігання та реагування на інсайдерські загрози в межах корпоративного середовища.

Предмет дослідження є методи, критерії та метрики оцінки ефективності технічних і процедурних засобів протидії інсайдерським загрозам у процесі внутрішнього аудиту інформаційної безпеки.

Методи дослідження. Вирішення поставлених завдань передбачає дослідження теоретичних засад інсайдерських ризиків, аналіз існуючих систем та методик оцінювання їх ефективності й створення комплексної та відтворюваної методики, що враховує сучасні стандарти, технологічні рішення та практичні потреби організацій.

Практичне значення одержаних результатів. Розроблена в роботі методика може бути використана під час планування та проведення внутрішнього аудиту інформаційної безпеки для оцінювання ефективності засобів протидії інсайдерським загрозам, завдяки DLP, SIEM, UEBA та системи контролю доступу.

Галузь застосування дослідження можуть бути використані для побудови систем управління інформаційною безпекою, розроблення політик та процедур протидії інсайдерам, удосконалення систем моніторингу подій безпеки та впровадження інструментів контролю доступу. Матеріали є актуальними для IT-підрозділів, служб інформаційної безпеки, внутрішніх аудиторів та керівництва

організацій, які прагнуть підвищити рівень кіберстійкості та мінімізувати операційні ризики, пов’язані з людським фактором.

Ключові слова: ЕФЕКТИВНІСТЬ ПРОТИДІЇ ІНСАЙДЕРСЬКИХ ЗАГРОЗ, ІНСАЙДЕРСЬКІ ЗАГРОЗИ, АУДИТ БЕЗПЕКИ.

Abstract

The qualification work is dedicated to the methodology for assessing the effectiveness of measures to counter insider threats during internal information security audits. The work consists of an introduction, three chapters containing six figures, conclusions, and a list of 25 references. The total volume of the work is 92 pages, of which 6 pages are occupied by a list of abbreviations and the bibliography.

The aim of the work is to develop a methodology for evaluating the effectiveness of measures against insider threats within the framework of internal information security audits.

The object of the study is the systems, processes, and organizational mechanisms of information security designed to detect, prevent, and respond to insider threats within a corporate environment.

The subject of the study is the methods, criteria, and metrics for evaluating the effectiveness of technical and procedural measures against insider threats during internal information security audits.

Research methods. The solution of the tasks involves studying the theoretical foundations of insider risks, analyzing existing systems and methodologies for assessing their effectiveness, and developing a comprehensive and reproducible methodology that takes into account current standards, technological solutions, and the practical needs of organizations.

Practical significance of the results. The methodology developed in this work can be used in planning and conducting internal information security audits to evaluate the effectiveness of countermeasures against insider threats, leveraging DLP, SIEM, UEBA, and access control systems.

Scope of application. The research findings can be applied to building information security management systems, developing policies and procedures to counter insider threats, improving security event monitoring systems, and implementing access control tools. The materials are relevant for IT departments, information security services,

internal auditors, and organizational management seeking to enhance cyber resilience and minimize operational risks related to human factors.

Keywords: Effectiveness of Countering Insider Threats, Insider Threats, Security Audit.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ - Інформаційна безпека

КБ - Кібербезпека

ІС - Інформаційна система

ISO - International Organization for Standardization / International

ІТ - Інформаційні технології

НСД - Несанкціонований доступ

ПЗ - Програмне забезпечення

СУІБ - Система управління інформаційною безпекою

УВІТ - Управління відновленням інформаційних технологій

NIST - National Institute of Standards and Technology

PIMS - Privacy Information Management System

SIEM - Security Information and Event Management

SOC - Security Operations Center

ВСТУП

Актуальність теми. Інсайдерські загрози є одним із найскладніших та найнебезпечніших типів ризиків у сфері інформаційної безпеки. На відміну від зовнішніх атак, вони здійснюються особами, які мають легітимний доступ до інформаційних ресурсів та добре обізнані з внутрішніми процесами організації. Через що значно ускладнюється виявлення таких інцидентів та потребує застосування спеціалізованих підходів до моніторингу, контролю та аудиту. У сучасних умовах цифровізації, розподілених робочих середовищ та широкого використання віддаленого доступу проблема інсайдерських загроз набуває ще більшої актуальності. Тому організації мають впроваджувати комплексні технічні й організаційні рішення, а також забезпечувати регулярний внутрішній аудит для перевірки їхньої ефективності.

Відповідність сучасни викликам вимагає аналізування та класифікацію інсайдерів, характерні сценарії інцидентів, фактори ризику й поведінкові особливості внутрішніх порушників. Для цього використовуються технологічні та організаційні засоби захисту, DLP, UEBA, SIEM, PAM та системи контролю доступу. Дуже важливо проводити огляд ключових міжнародних стандартів і нормативів, що визначають вимоги до контролю інсайдерських ризиків.

Ефективне реагування на інциденти є одним із ключових елементів інформаційної безпеки. Аудити оцінюють готовність команд реагування на інциденти, забезпечуючи швидкі дії для локалізації та усунення інцидентів безпеки, таким чином мінімізуючи вплив на операційну діяльність та захищаючи конфіденційну інформацію.

З точки зору аналізу сучасних методик аудиту та оцінки ефективності систем протидії інсайдерським атакам, які, зазвичай, засновані на стандартах ISO/IEC 19011, NIST Cybersecurity Framework, моделі ризикорієнтованого аудиту та метриках оцінювання роботи систем DLP, SIEM, UEBA. Й визначення ключових проблеми чинних підходів, зокрема неповноту оцінювання, високу кількість хибних спрацювань, недостатню інтеграцію з внутрішнім аудитом та відсутність єдиної стандартизованої методики для інсайдерських загроз.

З огляду на зазначене дослідження методики перевірки ефективності засобів протидії інсайдерським загрозам під час внутрішнього аудиту інфомаційної безпеки магістерська робота має важливе значення для захисту інформаційних активів, забезпечення дотримання нормативних вимог, підвищення стійкості та підтримки довіри зацікавлених і є актуальним науковим завданням.

Мета роботи є розробка методики перевірки ефективності засобів протидії інсайдерським загрозам у межах внутрішнього аудиту інформаційної безпеки.

Об'єктом дослідження є системи, процеси та організаційні механізми інформаційної безпеки, призначені для виявлення, запобігання та реагування на інсайдерські загрози в межах корпоративного середовища.

Предмет дослідження є методи, критерії та метрики оцінки ефективності технічних і процедурних засобів протидії інсайдерським загрозам у процесі внутрішнього аудиту інформаційної безпеки.

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

1.Проаналізувати природу інсайдерських загроз та сучасні підходи до їх виявлення, включаючи класифікацію внутрішніх порушень, фактори ризику та огляд технічних засобів контролю (DLP, SIEM, UEBA, IAM).

2.Визначити та систематизувати метрики, KPI та KRI, які застосовуються для вимірювання ефективності засобів протидії інсайдерським загрозам, а також критерії оцінки процесів виявлення, реагування та контролю доступу.

3.Розробити інтегровану методику та алгоритм проведення внутрішнього аудиту засобів захисту, що охоплює технічні системи, процеси SOC, політики безпеки та управління ризиками.

4.Провести практичну оцінку застосовності розробленої методики та сформувати рекомендації щодо оптимізації технічних, процедурних та організаційних заходів протидії інсайдерським загрозам.

Методи дослідження. Вирішення поставлених завдань передбачає дослідження теоретичних засад інсайдерських ризиків, аналіз існуючих систем та методик оцінювання їх ефективності й створення комплексної та відтворюваної

методики, що враховує сучасні стандарти, технологічні рішення та практичні потреби організацій.

Практичне значення одержаних результатів. Розроблена в роботі методика може бути використана під час планування та проведення внутрішнього аудиту інформаційної безпеки для оцінювання ефективності засобів протидії інсайдерським загрозам, завдяки DLP, SIEM, UEBA та системи контролю доступу.

Апробація результатів

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПРОТИДІЇ ІНСАЙДЕРСЬКИМ ЗАГРОЗАМ ТА ВНУТРІШНІЙ АУДИТ ІБ

Перед початком дослідження теми кваліфікаційної роботи необхідно ознайомитися з основними визначеннями у галузі інформаційної безпеки, регуляторними вимогами, стандартами, основними компонентами системи перевірки, застосованими методологіями у сфері перевірки ефективності засобів протидії інсайдерським загрозам під час внутрішнього аудиту інфомаційної безпеки.

1.1 Інсайдерські загрози: поняття, класифікація та характеристики

Інсайдерські загрози становлять одну з найскладніших і найнебезпечніших категорій ризиків для інформаційної безпеки, оскільки походять від осіб, які вже мають легітимний доступ до інформаційних ресурсів організації. Інсайдером мається на увазі співробітник, підрядник, партнер або будь-яка інша особа, що має дозволений доступ до внутрішніх систем і може свідомо або несвідомо завдати шкоди. За своєю природою інсайдерські інциденти важко виявити через те, що зловмисні дії часто виглядають як звичайна повсякденна діяльність користувача. Класифікація інсайдерів традиційно включає три основні типи: «Зловмисний інсайдер», «Недбалий інсайдер» та «Компрометований інсайдер». Зловмисний інсайдер — це особа, яка навмисно зловживає обліковими даними для крадіжки інформації у фінансових чи особистих цілях. Наприклад, це може бути людина, яка незадоволена попереднім роботодавцем і тому дає секретну конкуренту. Інсайдери мають перевагу перед іншими зловмисниками, тому що вони знайомі з політикою та процедурою організації та їх вразливістю [1]. Такий інсайдер зазвичай діє мотивовано чимось, або кимось - фінансово, ідеологічно або з особистих причин. Недбалий інсайдер не має наміру завдати шкоди, однак його помилки, необережність або недотримання політик безпеки створюють значні ризики для організації. Це може проявлятися в неправильному поводженні з конфіденційними

даними, використанні слабких паролів або відкриванні фішингових листів. Компрометований інсайдер — це користувач, обліковий запис або пристрій якого був захоплений стороннім зловмисником. Співробітники є не лише найціннішим активом організації, але часто також великим ризиком кібербезпеки. Відповідно до звіту про витоки даних за 2023 рік, 19% із приблизно 5200 витоків даних були спричинені діями персоналу. У іншому дослідженні за 2022 рік кількість цих подій перевищила 6800, а організації витратили близько 15,4 мільйона доларів на рік на усунення наслідків [2]. У такому випадку реальний нападник видає себе за легітимного співробітника, що ускладнює своєчасне виявлення атаки.

Сценарії інсайдерських інцидентів можуть значно відрізнятися за формою та масштабом. Якщо розглянути найбільш поширені то до них належать крадіжка конфіденційних даних, несанкціоноване копіювання або передача інформації третім сторонам, навмисне або випадкове видалення критично важливої інформації, саботаж роботи систем, витік даних через використання незахищених носіїв, фотографування екрану, злив журналів або конфігурацій, а також створення прихованих каналів зв’язку для подальших атак. Часто інсайдери діють поступово: збирають інформацію, тестують кордони безпеки, використовують час найменшого контролю або змінюють поведінку так, щоб мінімізувати підозри. Статистику зображенно на рис (1.1).

Рис. 1.1. Статистика робочого дня [3].

Існує ряд факторів, що сприяють виникненню інсайдерських атак. Серед внутрішніх факторів важливу роль відіграють відсутність контролю за доступами, надмірна кількість привілейованих облікових записів, слабкі або неактуальні політики інформаційної безпеки, недостатній рівень моніторингу та журналювання. Людський фактор також є вирішальним: низька обізнаність співробітників, стресові умови роботи, конфлікти всередині колективу або фінансові труднощі можуть підштовхнути до зловмисної поведінки або збільшити ризик недбалості. Зовнішні фактори — тиск кіберзлочинних груп, фішингові атаки або компрометація пристроїв співробітників — здатні перетворити звичайного користувача на інструмент атаки [4].

Опираючись на цю інформацію інсайдерські загрози становлять комплексну проблему, яка виникає на перетині технологій, людських взаємин та організаційних процесів. Їх ефективне розуміння та класифікація є ключовою передумовою для побудови надійної системи протидії, що охоплює як технічні засоби контролю, так і організаційні заходи, спрямовані на мінімізацію ризиків та своєчасне виявлення аномальної поведінки.

1.2Технологічні та організаційні засоби протидії інсайдерським загрозам

Технологічні та організаційні засоби протидії інсайдерським загрозам формують комплексну систему захисту, спрямовану на виявлення, запобігання та мінімізацію ризиків, що походять від осіб із легітимним доступом до інформаційних ресурсів. Оскільки інсайдери діють всередині периметра безпеки, ефективна протидія вимагає не лише впровадження сучасних технічних рішень, а й створення чіткої системи організаційних правил, політик та процедур.

Серед ключових технологічних засобів центральне місце займають системи DLP, UEBA, SIEM та PAM. DLP-системи забезпечують контроль за рухом конфіденційних даних, блокуючи або фіксуючи спроби їх незаконного копіювання, пересилання чи вивантаження. UEBA-технології аналізують поведінку користувачів та об’єктів у системі, виявляючи аномалії, що можуть свідчити про інсайдерську активність. Вони використовують машинне навчання, щоб створити «нормальні» профілі поведінки та знаходити відхилення, непомітні для традиційних засобів безпеки. SIEM-системи виконують роль центрального механізму кореляції та аналізу подій безпеки, поєднуючи дані з журналів, мережевих пристроїв, серверів та робочих станцій, що дозволяє виявляти складні та багатокрокові інциденти [5]. PAM-рішення забезпечують контроль за привілейованими обліковими записами, оскільки саме вони найчастіше стають інструментом або метою інсайдерських атак. Системи цього класу дозволяють керувати доступом адміністраторів, ізолювати критичні операції, вести відеозапис сесій та запобігати несанкціонованому використанню підвищених привілеїв. Порівння технологій зображенно на (табл. 1.1).

Таблиця 1.1

Опис основних технологій

Технологія	**Повна назва**	**Основне призначення**	**Що саме контролює / аналізує**	**Користь для ІБ**
DLP	Data Loss Prevention	Запобігання витоку конфіденційних даних	Файли, документи, пошту, мережеві передачі, дії користувачів з даними	Зменшує ризик витоку, виявляє підозрілі операції з даними
UEBA	User and Entity Behavior Analytics	Аналітика поведінки користувачів і систем	Поведінкові патерни користувачів, пристроїв, акаунтів	Виявляє інсайдерів, скомпрометовані акаунти та аномалії
SIEM	Security Information and Event Management	Централізований збір, кореляція та аналіз логів	Логи з систем, серверів, мережевого обладнання, події безпеки	Дає цілісну картину безпеки, прискорює реагування на інциденти
PAM	Privileged Access Management	Контроль і управління привілейованими доступами	Дії адмінів, сесії з підвищеними правами, доступ до критичних систем	Зменшує ризики зловживання правами, забезпечує аудит адмінських дій

Складова технологічної захищеності є системи контролю доступу. Вони визначають, хто і до яких інформаційних ресурсів має право доступу, а до цього ще й встановлює механізми автентифікації та авторизації. Завдяки використанню багатоетапної автентифікації, гнучких моделей на основі ролей або атрибутів, регулярний перегляд прав доступу та сегментація мережі значно зменшують ймовірність того, що інсайдер зможе отримати доступ до даних, які не є необхідними для його посадових обов’язків. Контроль доступу забезпечує реалізацію принципу мінімальних привілеїв — фундаментального підходу, який зменшує площу атаки та ускладнює зловмисникам виконання критичних дій.

Дані перебувають під загрозою незалежно від того, де вони зберігаються, що робить їх захист пріоритетним завданням для будь-якої організації. Вартість

помилки може бути надвисокою. Останній звіт IBM® «Cost of a Data Breach Report» показав, що середня світова вартість витоку даних зросла на 10% порівняно з попереднім роком і досягла 4,88 млн доларів США — найбільший стрибок з часів пандемії [6]. Особливо цінною для злодіїв є персональна ідентифікаційна інформація (PII), яка часто стає об'єктом атак. Звіт також виявив, що майже половина всіх випадків витоку стосувалася PII клієнтів, яка може включати податкові ідентифікаційні номери, електронні адреси, номери телефонів та домашні адреси. На другому місці за поширеністю опинилася інформація про інтелектуальну власність (IP) — 43% випадків. Захищати дані стає дедалі складніше, оскільки дані організації можуть використовуватися або зберігатися у різних форматах, у різних місцях та різними зацікавленими сторонами в межах організації. Крім того, різні набори даних можуть підпадати під різні правила залежно від рівня конфіденційності або відповідних нормативів щодо захисту даних.

Політики та інструменти DLP допомагають організаціям захищати себе, відстежуючи кожен фрагмент даних у мережі в усіх трьох станах: у використанні, у русі та у спокої.

- **Дані у використанні (**коли дані доступні, обробляються, оновлюються або видаляються. Наприклад, дані організації, які використовуються для аналізу або обчислень, або текстовий документ, який редагує кінцевий користувач).
- **Дані у русі / дані в транзиті** (дані, що передаються мережею, наприклад, через сервер потокової події, додаток для обміну повідомленнями або переміщуються між мережами. Тому варто зазначити що дані у русі є найменш захищеними серед трьох станів і потребують особливої уваги).
- **Дані у спокої** (дані, що зберігаються, наприклад, у хмарному сховищі, на локальному жорсткому диску або в архіві. На відміну від даних у русі, дані у спокої навпаки є найбільш стійкими, але заходи безпеки все одно потрібні. Дані у спокої можуть бути скомпрометовані навіть через простий випадок, наприклад, якщо хтось забере USB-накопичувач із залишеного без нагляду столу).

Ідеальним варіантом буде, якщо рішення з попередження втрати даних організації здатне відстежувати всі дані у використанні, у русі та у спокої для всього спектра програмного забезпечення, що використовується. Наприклад, додавати захист DLP для архівування, застосунків бізнес-аналітики (BI), електронної пошти, платформ для командної роботи та операційних систем, таких як macOS і Microsoft Windows.

Не варто забувати, що технічні засоби не можуть функціонувати ефективно без належної організаційної підтримки, тому важливу роль відіграють політики безпеки та регламенти контролю користувачів. Вони визначають правила роботи з інформацією, порядок доступу до ресурсів, вимоги до паролів, правила використання зовнішніх носіїв, поведінку у випадку підозри на інцидент тощо. Чіткі політики задають рамки, у яких співробітники повинні діяти, і допомагають уникати недбалих дій, що часто стають причиною інсайдерських інцидентів. Регламенти контролю користувачів включають процедури моніторингу діяльності, аудиту журналів, перевірки прав доступу, управління привілеями та реагування на поведінкові аномалії. Поєднання технологічних та організаційних засобів створює багаторівневу систему захисту, здатну виявляти інсайдерські дії на ранніх етапах, запобігати критичним інцидентам та зменшувати можливі збитки. Такий підхід забезпечує не лише виявлення зловмисної активності, а й підвищує загальну культуру безпеки в організації, що є ключовим фактором у боротьбі з інсайдерськими загрозами.

1.3 Стандарти та нормативи щодо контролю інсайдерських ризиків

Стандарти та нормативи щодо контролю інсайдерських ризиків відіграють ключову роль у формуванні системи управління інформаційною безпекою, оскільки вони задають структурований підхід до виявлення, запобігання та реагування на загрози, що походять від внутрішніх користувачів. Інсайдерські ризики є складними для контролю, адже пов’язані з особами, які мають легітимний доступ до інформації, тому міжнародні стандарти й національні норми формують

фундамент, на який організації можуть спиратися при побудові ефективних заходів протидії.

Одним із найважливіших та найпопулярніших міжнародних стандартів є ISO/IEC 27001, який регламентує побудову, впровадження та підтримку системи управління інформаційною безпекою (СУІБ) (рис. 1.2.). ISO 27001 забезпечує систематичний, структурований та ризик-орієнтований підхід до управління та захисту конфіденційних інформаційних активів в організації будь-якого розміру, в будь-якій галузі чи секторі економіки [7].

Рис. 1.2. стандарт ISO 27001

Хоча сам стандарт не зосереджується виключно на інсайдерських загрозах, у його структурі наявні численні контролі, що безпосередньо впливають на здатність організації протидіяти інсайдерським ризикам: управління доступом, контроль

активів, моніторинг подій безпеки, управління привілейованими обліковими записами, проведення аудитів тощо, приклади наведено у (таб. 1.2).

Таблиця 1.2

Приклади застосування стандарту ISO 27001

Сфера / галузь	**Приклад застосування ISO 27001**
ІТ-компанії та розробка ПЗ	Захист вихідного коду, контроль доступу до репозиторіїв, управління вразливостями.
Банки та фінансові установи	Управління ризиками кібербезпеки, захист платіжних даних, аудит доступів співробітників.
Медичні заклади / eHealth	Захист персональних та медичних даних пацієнтів, безпечне зберігання електронних карток.
Державні органи	Класифікація інформації, контроль доступу до реєстрів, безпечне управління інцидентами.
Освітні установи	Захист персональних даних студентів, безпечне управління онлайн-платформами навчання.
E-commerce / онлайн-магазини	Захист даних клієнтів та транзакцій, контроль доступу до баз даних замовлень.
Телекомунікації	Управління інцидентами, безпека мережевої інфраструктури, моніторинг безпеки.
Хмарні провайдери	Ідентифікація та оцінка ризиків, ізоляція клієнтських середовищ, управління ключами шифрування.
Логістика та транспорт	Захист систем відстеження вантажів, контроль доступу до операційних центрів.
Виробництво / промисловість	Управління доступом до систем SCADA, захист технологічної інформації та креслень.

Доповнючий стандарт «ISO 27002» – Дуже важливо зазначити, є саме ДОДАТКОВИМ стандартом, що зосереджений на засобах контролю інформаційної безпеки, які організації можуть вирішити впровадити. Перелічені в Додатку А стандарту ISO 27001, саме на ці засоби контролю посилатимуться експерти з інформаційної безпеки, обговорюючи засоби контролю інформаційної безпеки. Однак, якщо в Додатку А кожен засіб контролю описано одним або двома

реченнями, то в ISO 27002 кожному засобу контролю присвячено в середньому одну сторінку. Стандарт пояснює, як працює кожен засіб контролю, його мету та як його можна впровадити [8]. Сукупно стандарти 27001/27002 формують фундаментальний підхід, який дозволяє організаціям системно знижувати інсайдерські ризики (рис.1.3).

Рис.1.3. Порівння ISO 27001 та ISO 27002

NIST 800-53 – це вичерпний посібник, розроблений Національним інститутом стандартів і технологій (NIST), нерегуляторним агентством Міністерства торгівлі США. Він надає організаціям основу для управління та захисту своїх інформаційних систем. NIST 800-53, широко визнаний провідним стандартом кібербезпеки, використовується в усьому світі для захисту конфіденційної інформації [9]. Його характеристика (рис. 1.4).

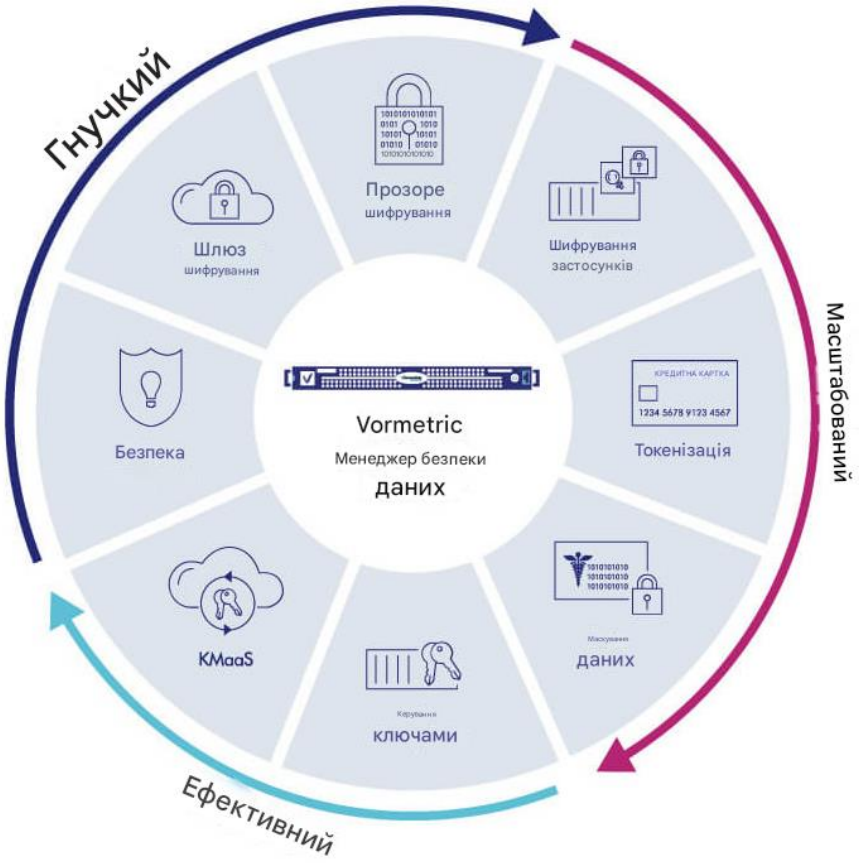

Рис. 1.4. Характеристика NIST 800-53

Американський стандарт NIST SP 800-53 пропонує більш технічний і детальний набір контролів, спрямованих на захист федеральних інформаційних систем США. Він містить широкий каталог вимог щодо управління доступом, аудиту, моніторингу та контролю поведінки користувачів, а також враховує як людський, так і технічний фактор. Важливою сучасною концепцією, пов’язаною з протидією інсайдерським загрозам, є модель Zero Trust, що стала ключовим елементом сучасної стратегії NIST. Zero Trust передбачає відмову від традиційного периметрового захисту і базується на принципах мінімальних привілеїв, постійної верифікації та недовіри до будь-якого користувача чи пристрою незалежно від його місцезнаходження [10]. У контексті інсайдерських ризиків це означає, що навіть легітимний користувач не отримує доступу без додаткової перевірки, а його дії постійно аналізуються. CIS Controls, у свою чергу, пропонує набір практичних і пріоритетних заходів, орієнтованих на швидке підвищення кіберстійкості організації. Серед них особливу увагу приділено контролю користувачів і доступів,

багатофакторній автентифікації, моніторингу журналів, контролю привілейованих дій та забезпеченню безпечної поведінки персоналу. CIS Controls є більш прикладним інструментом і часто використовується як базовий набір кроків для компаній, що тільки починають вибудовувати систему протидії інсайдерським загрозам (таб.1.3).

Таблиця 1.3

Порівння стандартів

Критерій	**ISO/IEC 27001**	**ISO/IEC 27002**	**NIST SP 800-53**
Тип стандарту	Міжнародний стандарт управління ІБ	Практичні рекомендації	Американський федеральний стандарт контролів
Призначення	Визначає вимоги до системи менеджменту інформаційної безпеки (ISMS)	Надає детальний опис контролів безпеки	Описує каталог контролів безпеки для федеральних систем США
Фокус	Процеси управління ІБ і вимоги	Практичні заходи, як реалізувати контролі	Глибокі технічні та організаційні контролі
Структура	11 розділів + Додаток А (114 контролів у версії 2013; 93 контролі у версії 2022)	4 тематичні розділи + детальний опис контролів	20+ контрольних сімейств (AC, AT, AU тощо), сотні контролів
Рівень деталізації	Високий рівень, орієнтований на менеджмент	Детальний опис для впровадження	Дуже детальний, технічно глибокий
Обов’язковість	Може бути сертифікований	Не сертифікується	Не сертифікується, але є обов’язковим для федеральних систем США
Для кого підходить	Будь-які організації, глобальний стандарт	Компанії, що впроваджують ISO 27001 або окремі контролі	Державні органи США, критична інфраструктура, великі компанії

Продовження таблиця 1.3

Критерій	**ISO/IEC 27001**	**ISO/IEC 27002**	**NIST SP 800-53**
Підхід до ризиків	Базується на управлінні ризиками	Підтримує ISO 27001	Присутній, але більш орієнтований на каталог контролів
Критерії відповідності	Виконання вимог ISMS	Впровадження рекомендацій	Відповідність вимогам контролів
Приклад використання	Побудова ISMS, отримання сертифікату	Опис того, як саме реалізувати заходи з ISO 27001	Побудова системи контролів в державних і критичних інфраструктурах

У багатьох країнах додатково діють національні нормативи, які встановлюють вимоги до захисту інформації. В Україні такими є НД ТЗІ від Держспецзв'язку, стандарти комплексної системи захисту інформації (КСЗІ), а також вимоги Національного банку України для банківського сектору [11]. Ці документи регламентують порядок управління доступами, ведення журналів подій, аудит безпеки, вимоги до персоналу та інші заходи, критично важливі для контролю інсайдерських ризиків. Національні норми найчастіше адаптовані під локальні правові вимоги та специфіку галузей, тому їх виконання є обов'язковим для організацій відповідної сфери.

Стандарти та нормативи створюють системний каркас, який дозволяє організаціям структурувати свою діяльність із протидії інсайдерським загрозам, впроваджувати зрозумілі процедури контролю та реагування, а також забезпечувати відповідність міжнародним практикам. Їх застосування сприяє зменшенню ризиків, підвищенню рівня довіри до IT-інфраструктури та формуванню стійкої культури інформаційної безпеки.

Внутрішній аудит відіграє ключову роль у забезпеченні протидії інсайдерським загрозам, оскільки він забезпечує незалежний та системний контроль за тим, наскільки ефективно організація управляє доступами, дотримується політик безпеки та реагує на потенційні ризики з боку своїх співробітників [12]. Інсайдерські загрози складні тим, що їх джерелом стають особи, які мають легальний доступ до критичних ресурсів, тому саме внутрішній аудит є тією функцією, що здатна виявити приховані слабкі місця, оцінити зрілість системи безпеки та забезпечити об'єктивний погляд на стан контролю в організації.

Функції внутрішнього аудиту в контексті протидії інсайдерським загрозам охоплюють оцінювання адекватності системи контролю доступів, перевірку відповідності політик та процедур вимогам стандартів, аналіз ефективності технічних рішень і виявлення порушень або аномалій у поведінці персоналу. Аудитори перевіряють, чи забезпечується принцип мінімальних привілеїв, чи існують механізми сегментації доступів, чи регулярно переглядаються права користувачів, а також чи впроваджені механізми моніторингу та журналювання. Основними принципами роботи внутрішнього аудиту є незалежність, об'єктивність, системність та ризик-орієнтований підхід. Ці принципи дозволяють сформувати всебічну оцінку стану внутрішнього контролю та знизити ризики отримання викривленої інформації про фактичний стан безпеки.

У загальній системі інформаційної безпеки внутрішній аудит займає роль контролюючого елемента, що забезпечує зворотний зв'язок для керівництва та підрозділів ІБ. Він не замінює технічні засоби захисту, але дозволяє перевірити їх ефективність, правильність налаштування, відповідність регламентам та здатність запобігати інсайдерським діям. Внутрішній аудит також координує діяльність із зовнішніми аудиторами, забезпечує відповідність стандартам ISO/IEC 27001, NIST та іншим нормативам, а також перевіряє, чи дотримуються вимоги національного законодавства у сфері захисту інформації. Особливо важливим є те, що внутрішній аудит сприяє підвищенню прозорості бізнес-процесів, формуванню культури безпеки та забезпеченню безперервного вдосконалення системи ІБ.

Процедури аудиту, які безпосередньо пов'язані з виявленням інсайдерських ризиків, включають аналіз журналів подій, оцінку роботи систем DLP, SIEM, UEBA та PAM, перевірку процесів управління доступами, аудит привілейованих облікових записів, аналіз інцидентів та тестування сценаріїв зловмисної чи недбалої поведінки користувачів. Аудитори проводять інтерв'ю з IT-персоналом та співробітниками ключових підрозділів, аналізують відповідність дій персоналу вимогам політик безпеки, перевіряють записи тренінгів і рівень обізнаності співробітників. Особлива увага приділяється виявленню нетипових аномалій: незвичайним діям із даними, доступам у неробочий час, змінам конфігурацій,

спробам приховування активності. У разі необхідності аудит може включати моделювання інсайдерських атак, що дозволяє оцінити реакцію систем захисту на реальні загрози.

Висновок до розділу 1

В розділі було проаналізовано теоретичні засади протидії інсайдерським загрозам та роль внутрішнього аудиту інформаційної безпеки у забезпеченні належного управління інсайдерськими ризиками. Аналіз показав, що інсайдерські загрози становлять одну з найскладніших категорій кіберризиків, оскільки походять від осіб, які мають легітимний доступ до інформаційних ресурсів і добре знайомі з внутрішніми процесами та вразливостями організації. Класифікація інсайдерів — зловмисних, недбалих та компрометованих — демонструє різноманітність сценаріїв їхніх дій та складність їх виявлення.

Було досліджено, що ефективна протидія інсайдерським загрозам можлива лише за умови поєднання технологічних та організаційних заходів.

Було визначено системи DLP, UEBA, SIEM та PAM формують технологічну основу багаторівневого контролю, дозволяючи відстежувати операції з даними, аналізувати поведінку користувачів, корелювати події безпеки та управляти привілейованими обліковими записами. Водночас їхня результативність значною мірою залежить від наявності чітких політик інформаційної безпеки, процедур доступу, правил реагування на інциденти та загальної культури безпеки в організації.

Було розглянуто роль міжнародних стандартів та нормативів у забезпеченні системного підходу до управління інсайдерськими ризиками. Стандарти ISO/IEC 27001 та ISO/IEC 27002 забезпечують фундамент для впровадження СУІБ та визначають ключові засоби контролю, що впливають на зниження інсайдерських загроз. Стандарт NIST SP 800-53 та концепція Zero Trust пропонують сучасні технічні та процедурні підходи до контролю доступу, моніторингу активності та

перевірки довіри, тоді як CIS Controls орієнтується на практичність і швидкість впровадження.

Було визначено, що інсайдерські загрози є комплексною проблемою, яка потребує інтегрованого, ризик-орієнтованого підходу, що поєднує сучасні технологічні рішення, належне регламентування та дотримання міжнародних стандартів..

РОЗДІЛ 2. АНАЛІЗ ІСНУЮЧИХ МЕТОДИК ТА ПРОБЛЕМ ОЦІНКИ ЕФЕКТИВНОСТІ ЗАСОБІВ ПРОТИДІЇ ІНСАЙДЕРСЬКИМ ЗАГРОЗАМ

Для досягнення мети дослідження необхідно провести аналіз кроків алгоритму проведення аудиту, визначити критерії, показники, інструменти та техніки, які при цьому застосовуються.

2.1 Огляд існуючих методик аудиту інформаційної безпеки

Аудит інформаційної безпеки є ключовим механізмом забезпечення належного рівня захисту інформаційних активів організації та формування об’єктивного уявлення про стан системи безпеки. Він дозволяє виявляти вразливості, оцінювати ефективність впроваджених заходів та відповідність вимогам нормативних документів і міжнародних стандартів. Сучасна практика аудиту базується на низці методик, що відрізняються глибиною аналізу, підходами до оцінювання та сферою застосування. Однією з найпоширеніших методик є аудит відповідності міжнародному стандарту ISO/IEC 27001, який визначає вимоги до створення, впровадження та підтримки системи управління інформаційною безпекою (СУІБ). Стандарт ISO/IEC 27002 доповнює його практичними рекомендаціями та наборами контролів, що дозволяють оцінювати ефективність політик та процедур безпеки, реалізацію технічних, організаційних і фізичних засобів контролю, процеси управління ризиками та відповідність вимогам сертифікації.

Перевагою цього підходу є його системність, структурованість і орієнтація на безперервне вдосконалення, яка реалізується через цикл PDCA (Plan–Do–Check–Act) (рис. 2.1). Такий підхід дозволяє організації не лише досягти необхідного рівня захисту, а й підтримувати та підвищувати його у відповідь на еволюцію загроз. Методика ISO/IEC 27001/27002 відзначається універсальністю: вона застосовується як у внутрішніх перевірках для самоконтролю організації, так і в рамках зовнішнього незалежного аудиту для підтвердження відповідності

міжнародним вимогам [13]. Забезпечується високий ступінь уніфікації, порівнянності результатів і формує довіру з боку партнерів, клієнтів та регуляторів. Недоліком методики може бути ресурсомісткість повноцінного аудиту, особливо для організацій із низьким рівнем зрілості процесів безпеки або обмеженими фінансовими та кадровими ресурсами, а також необхідність наявності компетентних фахівців для правильного аналізу і інтерпретації результатів.

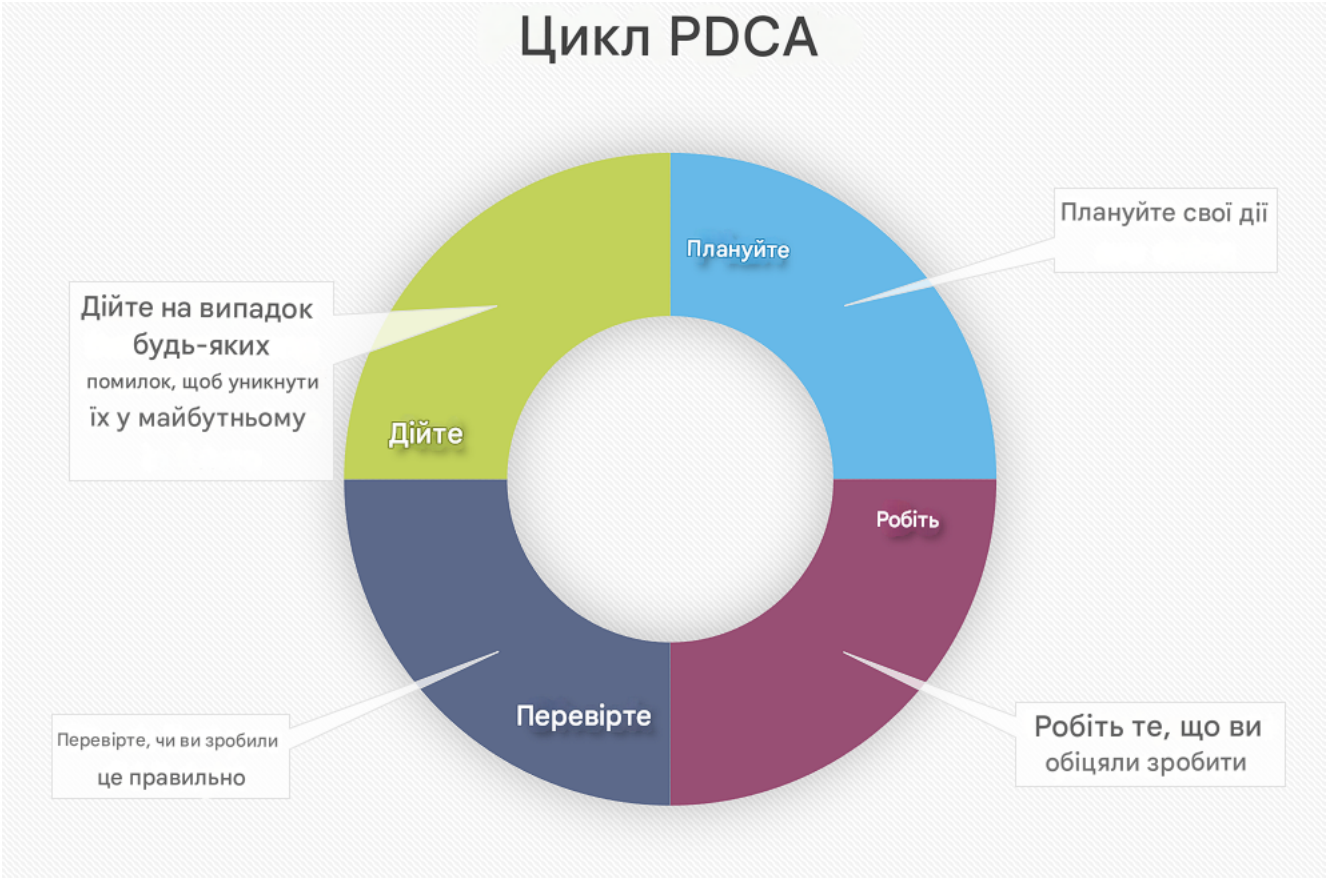

Рис. 2.1. Plan–Do–Check–Act

Методика ISO/IEC 27001/27002 широко застосовується у підприємствах різного масштабу та секторів економіки, де важлива відповідність міжнародним стандартам, ефективне управління ризиками та підвищення рівня інформаційної безпеки. Вона спрямована на створення структурованої системи управління безпекою, яка забезпечує контроль і моніторинг усіх критично важливих процесів, зниження ризиків і формування основи для подальшого вдосконалення заходів захисту інформаційних активів організації.

Аудит за цією методикою передбачає оцінювання:

- ефективності політик та процедур безпеки;
- реалізації технічних, організаційних та фізичних засобів контролю;
- процесів управління ризиками;
- відповідності вимогам сертифікації.

Національний інститут стандартів і технологій США (NIST) пропонує одну з найдеталізованіших методик аудиту інформаційної безпеки, основу якої становить стандарт NIST SP 800-53. Цей документ охоплює понад сто сімейств контролів безпеки, що включають управління доступом, моніторинг подій, реагування на кіберзагрози, адміністрування інцидентів, фізичну безпеку, захист мережевої інфраструктури та інші критично важливі домени. Аудит за NIST передбачає комплексний аналіз внутрішніх політик і процедур, оцінювання організаційних та технічних заходів, інтерв'ювання відповідальних співробітників, тестування ефективності впроваджених технічних контролів та перевірку узгодженості чинної системи захисту з моделлю управління ризиками RMF. Методика вирізняється високим рівнем деталізації, стандартизованим підходом і можливістю побудови аудиту будь-якої складності, що робить її придатною для великих організацій та структур із високими вимогами до безпеки.

Перевагою стандарту NIST SP 800-53 є його системність і глибина охоплення всіх аспектів інформаційної безпеки — від технічних контролів до організаційних процесів і управління ризиками. Методика забезпечує уніфікований, чітко структурований підхід, який можна масштабувати для організацій різного типу, а також гарантує узгодженість заходів безпеки з міжнародно визнаною моделлю управління ризиками RMF [14]. Водночас її впровадження є ресурсомістким: повноцінна оцінка потребує значних часових, людських і фінансових витрат, що може бути обмежувальним фактором для невеликих організацій або структур із низьким рівнем зрілості процесів інформаційної безпеки. Методика широко застосовується у державних установах, великих корпораціях, фінансовому секторі та будь-яких організаціях, де критично важлива висока надійність систем безпеки та відповідність регуляторним вимогам. Основна спрямованість NIST SP 800-53

полягає на комплексній оцінці ефективності всіх заходів безпеки, забезпеченні відповідності політик і процесів управлінню ризиками, а також на створенні структурованої та масштабованої системи захисту інформаційних активів організації.

Аудит за NIST включає:

- аналіз політик та процедур;
- інтерв'ювання персоналу;
- тестування технічних контролів;
- оцінювання відповідності ризик-менеджменту моделі RMF.

Фреймворк CIS Controls (раніше відомий як CIS 20) є практичним, уніфікованим та пріоритетним набором заходів кіберзахисту, спрямованим на швидке та ефективне підвищення рівня інформаційної безпеки організації [15]. Методика аудиту на основі CIS Controls фокусується на перевірці базових конфігурацій систем, аналізі процесів управління активами, оцінюванні ефективності контролів доступу, журналювання, резервного копіювання та здатності організації реагувати на інциденти. Особливістю фреймворку є чітка пріоритизація заходів, поділених на три рівні важливості, що дозволяє організаціям поступово нарощувати зрілість безпеки відповідно до наявних ресурсів і потреб. Основною перевагою цього підходу є його практичність, простота та висока швидкість впровадження, що робить його надзвичайно зручним для компаній із середнім або початковим рівнем зрілості процесів інформаційної безпеки, які прагнуть швидко підвищити базовий рівень захисту без надмірних ресурсних витрат.

Недоліком методики є її орієнтація переважно на базові заходи, що може залишати поза увагою складні чи специфічні загрози та інциденти високого рівня, а також потреба у регулярному оновленні пріоритетів та контрольних заходів, щоб вони відповідали поточним загрозам. Методика CIS Controls широко використовується для оцінки поточного стану безпеки в організаціях різного розміру, у тому числі у малому та середньому бізнесі, при підготовці до сертифікацій або внутрішніх аудитів, а також для створення дорожньої карти

поступового підвищення зрілості безпеки. Спрямованість цього фреймворку полягає на забезпеченні практичного, поетапного підходу до підвищення кіберзахисту, оптимізації базових контролів і формуванні надійної основи для подальшого розвитку систем управління інформаційною безпекою.

Методика аудиту на основі CIS зазвичай включає:

- перевірку базових налаштувань систем;
- аналіз керування активами;
- оцінювання контролів доступу, журналювання та резервного копіювання;
- перевірку реагування на інциденти.

COBIT 2019 як методика аудиту IT-процесів охоплює не лише питання інформаційної безпеки, а й весь спектр управління IT у організації. У межах цього підходу аудит розглядається як комплексний аналіз зрілості та ефективності ключових процесів, включаючи управління ризиками, інцидентами, змінами, сервісами, ресурсами та загальним IT-керуванням. У сфері безпеки оцінюються наявність контрольних точок, рівень формалізації та документування процедур, відповідність фактичного виконання встановленим політикам, а також показники результативності, які демонструють, наскільки ефективно функціонує система контролів. Методика дозволяє організаціям не лише виявляти слабкі місця та потенційні ризики, а й формувати рекомендації щодо підвищення зрілості процесів, оптимізації управління IT-ресурсами та забезпечення інтегрованого підходу до інформаційної безпеки.

Серед переваг COBIT 2019 варто зазначити його комплексність і здатність узгоджувати IT-ініціативи з бізнес-цілями, що забезпечує прозорість процесів і ефективне управління ризиками. Методика дозволяє стандартизовано оцінювати процеси незалежно від специфіки організації, що робить її придатною для великих та регульованих підприємств. Вона підтримує формування чіткої дорожньої карти вдосконалення IT-процесів, що підвищує керованість і контрольованість систем безпеки. До недоліків цього підходу належить значна складність впровадження, яка вимагає залучення висококваліфікованих фахівців, ресурсомісткість аудиту та

можливі труднощі при адаптації методики до малих або швидко змінюваних організацій, де процеси ще не достатньо формалізовані.

COBIT 2019 широко використовується у великих корпоративних структурах, фінансових та державних установах, де важлива відповідність вимогам регуляторів, а також у проєктах цифрової трансформації, де необхідно забезпечити інтеграцію безпеки та управління IT на всіх рівнях. Методика спрямована на підвищення зрілості IT-процесів, оптимізацію ресурсів, забезпечення узгодженості діяльності IT з бізнес-цілями, зниження ризиків і посилення контролю за виконанням політик безпеки. Вона дозволяє організаціям системно підходити до управління IT та інформаційною безпекою, забезпечуючи не лише відповідність нормативам, а й довгострокову ефективність і надійність IT-середовища [16].

У контексті безпеки дані процеси оцінюються за критеріями:

- наявність контрольних точок;
- ступінь формалізації та документування;
- виконання процедур;
- показники ефективності (KPI).

Для аудиту Інформаційної безпеки застосовуються спеціалізовані методики, серед яких однією з найпоширеніших є OWASP SAMM. Модель дає змогу комплексно оцінити зрілість процесів розробки, визначити рівень інтеграції безпеки на всіх етапах життєвого циклу програмного забезпечення та сформувати чітке уявлення про здатність організації запобігати вразливостям у створюваних продуктах. Під час аудиту аналізується якість архітектурних рішень і повнота моделювання загроз, стан і безпечність кодової бази, ефективність процедур управління вразливостями та оперативність їх усунення, а також результати різних типів тестування, включно зі статичним і динамічним аналізом та етичним зламом. Методика є особливо цінною для компаній, що здійснюють активну розробку власних продуктів, оскільки допомагає систематизувати практики безпечної розробки, підвищити їхню зрілість і забезпечити стабільний рівень безпеки на всіх етапах створення та підтримки програмного забезпечення.

Перевагою OWASP SAMM є те, що вона забезпечує комплексне охоплення всіх етапів SDLC та дозволяє оцінити зрілість процесів, а не лише наявність технічних вразливостей. Методика надає можливість виявляти системні недоліки в організації процесів, підтримує безперервне вдосконалення завдяки чітким рівням зрілості та рекомендаціям, а також сприяє зниженню витрат на усунення дефектів на пізніх етапах, оскільки дозволяє виявляти проблеми ще під час розробки [17]. Разом із тим вона має і певні недоліки: її впровадження може вимагати значних ресурсів, особливо якщо організація має низьку зрілість розробки; успішне застосування потребує участі кваліфікованих фахівців із безпечної розробки, а інтеграція підходів SAMM у швидкі, гнучкі чи малодокументовані процеси може бути ускладненою. У ситуаціях, коли внутрішні процеси непрозорі або недостатньо формалізовані, результати оцінювання можуть бути неповними. На практиці методику OWASP SAMM застосовують під час оцінювання стану безпеки внутрішніх команд розробки, підготовки до випуску нових продуктів, аналізу готовності організації до переходу на DevSecOps, а також під час аудиту зовнішніх постачальників програмного забезпечення з метою визначення рівня їхньої компетентності у сфері безпечної розробки. Основна спрямованість SAMM полягає у визначенні зрілості процесів, виявленні прогалин у практиках безпеки, підвищенні узгодженості та контрольованості процесів створення програмного забезпечення, а також у формуванні довгострокової стратегії інтеграції безпеки в SDLC, що забезпечує стабільний рівень захисту продуктів і знижує ризики появи критичних вразливостей.

Основними компонентами аудиту є:

- аналіз архітектури та моделювання загроз;
- рев’ю кодової бази;
- перевірка практик керування вразливостями;
- тестування безпеки (SAST, DAST, PenTest).

Методика аудитів відповідності регуляторним вимогам має чітко визначену спрямованість — забезпечити, щоб організація виконувала мінімальні вимоги, встановлені законодавством або галузевими стандартами. Її головна мета полягає в

підтвердженні того, що процеси обробки даних, механізми контролю та засоби захисту відповідають нормам, необхідним для легальної діяльності та уникнення штрафів. Такий підхід широко застосовується в секторах, де регулятор встановлює обов'язкові правила, як-от обробка платіжних карток за PCI DSS, захист медичної інформації за HIPAA чи робота з персональними даними громадян ЄС у контексті GDPR. У практичному використанні це передбачає аналіз політик, технічних налаштувань, логів, процедур доступу та інцидент-менеджменту, а також перевірку того, чи відповідають вони вимогам стандарту.

Основною перевагою таких аудитів є їхня прозорість і однозначність: регуляторні стандарти містять чіткі критерії, яких потрібно дотримуватись, тому організація точно знає, які вимоги виконати. Це спрощує підготовку, а також дозволяє продемонструвати партнерам і клієнтам відповідність визнаним нормам, підвищуючи рівень довіри. Крім того, такі аудити знижують юридичні та фінансові ризики, оскільки виконання стандартів допомагає уникати штрафів, заборони на роботу з певними даними або репутаційних втрат. Для багатьох компаній регуляторний аудит є рушійною силою покращення внутрішніх процесів, адже змушує впорядковувати документацію, структурувати політики та забезпечувати контрольованість IT-середовища. Втім, цей підхід має й певні недоліки. Регуляторні вимоги часто зосереджені на мінімально необхідному рівні безпеки, тому виконання стандарту не гарантує повного захисту від сучасних загроз. Організації, що обмежуються лише відповідністю, ризикують залишити поза увагою нові ризики та вразливості, які не охоплені нормативами. Крім того, такі аудити можуть бути ресурсомісткими, вимагати значних фінансових вкладень та утримання окремих команд, що займаються відповідністю. Для деяких компаній значною проблемою є бюрократичний характер перевірок, коли акцент робиться більше на документацію, ніж на реальний рівень безпеки.

На практиці аудит відповідності використовується під час щорічної сертифікації за PCI DSS, при підготовці до перевірок регуляторів у фінансовому або медичному секторі, у рамках впровадження GDPR-процедур щодо обробки персональних даних. Він сприяє не лише формальному підтвердженню

відповідності, а й забезпечує чітку дорожню карту заходів, які організація повинна виконати для підтримання законності та стабільної роботи [18]. Такий аудит спрямований насамперед на забезпечення виконання норм і захист організації від регуляторних ризиків, а також на підвищення базового рівня інформаційної безпеки через дотримання встановлених вимог.

- **PCI DSS** - для компаній, що працюють із платіжними картками;
- **HIPAA** - для медичних установ;
- **GDPR** - для організацій, які обробляють персональні дані громадян ЄС.

Ризик-орієнтований аудит спрямований на виявлення та оцінку саме тих факторів, які становлять найбільшу загрозу для стабільної роботи організації, тому він допомагає формувати реалістичне бачення стану безпеки та раціонально визначати пріоритети захисту. На відміну від формальних перевірок відповідності, цей підхід орієнтується на практичні ризики, що можуть вплинути на бізнес, тому розпочинається з ідентифікації критичних активів, аналізу загроз і вразливостей, а також оцінювання ризиків за стандартизованими методиками на кшталт ISO 31000 чи OCTAVE. Далі оцінюється ефективність наявних контролів і визначається, наскільки вони справді знижують ризики та чи відповідають політикам і потребам організації.

Перевагою цього підходу є його гнучкість і сфокусованість на реальних проблемах, що дозволяє отримати найбільш релевантну інформацію про слабкі місця та не витрачати ресурси на малозначущі аспекти. Він забезпечує краще стратегічне планування, адже дає змогу прив’язати заходи безпеки до конкретних бізнес-ризиків і прогнозованих збитків. Крім того, ризик-орієнтований аудит стимулює проактивність, допомагає підвищувати зрілість процесів безпеки та адаптувати контролі до нових загроз [19].

Недоліком цього підходу є те, що він потребує високої кваліфікації фахівців, які здатні правильно оцінити загрози та ймовірності, а також неповних або неточних даних, що можуть вплинути на кінцеві висновки. У деяких випадках ризик-орієнтований аудит вимагає більше часу й ресурсів, ніж нормативні

перевірки, а також може викликати складнощі під час узгодження з керівництвом, якщо ризики важко кількісно оцінити.

Цей підхід використовується під час побудови систем управління безпекою, підготовки до впровадження технологічних змін, проведення внутрішніх аудитів ІБ, аналізу готовності до нових загроз чи при оцінці ефективності впроваджених технічних та організаційних контролів. Його ключова спрямованість полягає в тому, щоб забезпечити максимально ефективне застосування ресурсів безпеки, концентруючи зусилля на тих сферах, де можливі інциденти спричинили б найбільші збитки або перерву в роботі. Таким чином, ризик-орієнтований аудит стає основою для формування довгострокової стратегії захисту, що орієнтується на реальні загрози та потреби бізнесу.

Він включає:

- визначення критичних активів;
- аналіз загроз та вразливостей;
- оцінювання ризиків за методиками ISO 31000 або OCTAVE;
- перевірку ефективності контролів щодо зниження ризику.

2.2. Поточні підходи до оцінки ефективності систем захисту

Оцінювання ефективності систем захисту від інсайдерських загроз є важливим елементом управління інформаційною безпекою, оскільки дозволяє визначити реальний рівень захищеності та здатність організації своєчасно виявляти й реагувати на потенційно небезпечні дії внутрішніх користувачів. У сучасній практиці застосовуються різні групи метрик, що охоплюють технічні показники роботи систем моніторингу, поведінкові індикатори ризику та результати процесів реагування. Найважливіше значення при цьому мають дані, які генеруються системами DLP, SIEM та UEBA, доповнені KPI та KRI, що відображають якість функціонування процесів безпеки (таб. 2.1)

Таблиця 2.1

Головні засоби та їх характеристики

Засіб	**Що відбувається на етапі перевірки**	**Переваги**	**Недоліки / обмеження**
DLP (Data Loss Prevention)	Перевіряється контроль каналів витоку даних, правильність політик, сповіщення про порушення, блокування небезпечних дій користувачів.	Забезпечує захист конфіденційних даних; дозволяє виявляти ненавмисні та свідомі спроби витоку; інтегрується з іншими системами.	Можливі хибнопозитивні спрацювання; складність налаштування тонких правил; потребує постійного оновлення політик.
SIEM (Security Information and Event Management)	Оцінюється збір журналів подій, кореляція інцидентів, сповіщення в реальному часі, аналітика та формування звітів.	Центральне управління безпековими подіями; швидке виявлення інцидентів; аналітика на основі історичних даних; інтеграція з іншими системами.	Висока складність конфігурації; велика кількість даних, що потребують обробки; можливість пропуску нових типів аномалій без оновлення правил.
UEBA (User and Entity Behavior Analytics)	Перевіряється аналіз поведінки користувачів, моделювання нормальної активності, виявлення аномалій та відхилень від звичних патернів.	Дозволяє виявляти приховані або складні інсайдерські загрози; прогнозування потенційно небезпечної поведінки; зменшення кількості хибних спрацювань.	Потребує достатньої історії даних для навчання моделей; складність інтерпретації результатів; не завжди ефективно при нових, нетипових сценаріях.
PAM (Privileged Access Management)	Перевіряється облікові записами, контроль доступу до критичних систем, реєстрація дій користувачів з високими правами.	Захист від ескалації привілеїв; контроль та аудит критичних дій; зменшення ризику компрометації систем.	Складність впровадження; потребує регулярного оновлення; обмежена ефективність без підтримки поведінкових аналітик.

Системи DLP оцінюються за показниками, що характеризують точність, повноту та оперативність виявлення потенційних витоків інформації**.** Метрики дозволяють оцінити ефективність політик безпеки та продуктивність аналітиків SOC при роботі з інцидентами.

1. Precision (точність виявлення)

Визначає частку коректно ідентифікованих інцидентів серед усіх сповіщень DLP. Висока точність дозволяє зменшити навантаження на аналітиків SOC, запобігаючи відволіканню на помилкові спрацьовування, та підвищує довіру до системи.

2. Recall (повнота виявлення)

Показує, яку частину реальних інцидентів DLP здатна виявити. Низький показник recall свідчить про наявність «сліпих зон», де потенційні витоки даних можуть залишатися непоміченими. Високий recall забезпечує більш повний контроль над ризиками витоку інформації.

3. False Positive Rate (рівень помилкових спрацювань)

Цей показник відображає частку помилкових сповіщень від усіх подій, зафіксованих DLP. Високий FPR призводить до ігнорування сповіщень аналітиками та зниження ефективності контролю. Оптимізація FPR дозволяє балансувати точність і повноту виявлення інцидентів.

4. Time to Detect (TTD)

Час, необхідний для виявлення порушення політики доступу або спроби ексфільтрації даних. Швидке виявлення критично важливе для зменшення потенційного збитку від інсайдерських загроз [20].

5. Time to Block / Time to Prevent

Вимірює час від виявлення до автоматичного блокування передачі конфіденційної інформації. Ця метрика відображає ефективність автоматизованих засобів захисту і дозволяє оперативно запобігати витокам даних.

6. Policy Coverage (охоплення політиками)

Визначає частку бізнес-процесів і типів даних, покритих актуальними DLP-політиками. Високий рівень охоплення дозволяє організації забезпечити комплексний контроль над конфіденційною інформацією та виявляти прогалини у захисті.

Порівняння та приклад використання цих метрик зображенно у (таб. 2.2).

Таблиця 2.2

Опис метрик

Метрика	**Використання**	**Переваги**	**Недоліки**
Precision (точність виявлення)	Оцінка частки коректно ідентифікованих інцидентів серед усіх сповіщень	Зменшує навантаження на аналітиків SOC; підвищує довіру до системи	Може занижувати загальні ризики, якщо система налаштована занадто консервативно
Recall (повнота виявлення)	Визначає, яку частину реальних інцидентів система здатна виявити	Забезпечує контроль над усіма потенційними витоками	Високий recall може збільшувати кількість помилкових спрацьовувань
False Positive Rate (рівень помилкових спрацювань)	Вимірює частку помилкових сповіщень від усіх подій	Допомагає оптимізувати роботу аналітиків SOC; зменшує «втому від сповіщень»	Не відображає всієї повноти захисту; не показує пропущені інциденти
Time to Detect (TTD)	Час від початку інциденту до його виявлення	Дозволяє оцінити оперативність системи; швидше реагування зменшує збитки	Може не враховувати складність інциденту та ресурсів SOC
Time to Block / Time to Prevent	Час від виявлення до блокування передачі даних	Ключова метрика для автоматизованого реагування; зменшує ризик витоку	Не завжди можливий повний автоматичний контроль; може створювати помилкові блокування
Policy Coverage (охоплення політиками)	Частка бізнес-процесів і типів даних під контролем політик DLP	Дозволяє оцінити комплексність захисту; виявляє прогалини	Не відображає ефективність окремих політик; висока охопленість не гарантує якісного контролю

SIEM-системи є центральним механізмом моніторингу подій інформаційної безпеки, що дозволяє збирати, агрегувати та аналізувати лог-дані з усіх підсистем організації у реальному часі. Ефективність SIEM визначається якістю кореляції подій, охопленням логування та здатністю швидко і точно повідомляти про інциденти.

1. Log Coverage (охоплення логування)

Цей показник відображає відсоток систем, підсистем та бізнес-процесів**,** інтегрованих у SIEM. Високе охоплення забезпечує повну видимість подій у корпоративній мережі та дозволяє виявляти інциденти на ранньому етапі. У

великих мережах значення нижче 80% свідчить про ризик неповної видимості та потенційні «сліпі зони».

2. Correlation Rule Accuracy

Метрика оцінює якість та релевантність налаштованих кореляційних правил**.** Вимірюється через precision та recall, аналогічно до DLP. Висока точність кореляційних правил дозволяє зменшити кількість помилкових сповіщень та підвищити ефективність реагування SOC.

3. Event Volume per Second (EPS)

Цей технічний показник вимірює кількість подій, оброблених SIEM за секунду. Високий EPS критично важливий для запобігання втраті подій або їх несвоєчасній обробці, особливо у великих корпоративних мережах з великим потоком логів.

4. Mean Time to Correlate (MTTC)

Показник визначає середній час, необхідний для аналізу подій та спрацювання кореляційного правила**.** Зменшення MTTC дозволяє оперативніше реагувати на інциденти**,** знижуючи потенційний вплив загроз [21].

5. Alert Fatigue Index

Цей KRI оцінює рівень «втоми від сповіщень» аналітиків SOC. Надмірні або нерелевантні сповіщення можуть призводити до ігнорування важливих інцидентів. Контроль цього показника допомагає оптимізувати правила кореляції та зменшити навантаження на аналітиків, підвищуючи ефективність реагування на загрози.

Порівняння та приклад використання метрик SIEM зображенно у (таб. 2.3).

Таблиця 2.3

Опис метрик

Метрика	**Використання**	**Переваги**	**Недоліки**
Log Coverage (охоплення логування)	Відсоток систем, підсистем та бізнес-процесів, інтегрованих у SIEM	Забезпечує повну видимість подій; дозволяє виявляти інциденти в усіх критичних точках	Низьке охоплення (<80%) створює «сліпі зони»; потребує значних ресурсів для інтеграції всіх джерел
Correlation Rule Accuracy	Якість і релевантність налаштованих правил кореляції подій	Збільшує точність сповіщень; допомагає виявляти складні інциденти	Погано налаштовані правила можуть генерувати багато помилкових спрацювань або пропускати інциденти
Event Volume per Second (EPS)	Вимірює пропускну здатність SIEM; кількість подій, оброблених за секунду	Дозволяє оцінити технічну здатність системи; запобігає втраті подій	Не відображає якість обробки та кореляції; високі значення потребують потужної інфраструктури
Mean Time to Correlate (MTTC)	Час, необхідний для аналізу подій та спрацювання кореляційного правила	Швидке корелювання забезпечує оперативне реагування на загрози	Може не враховувати складність інциденту; залежить від навантаження на систему
Alert Fatigue Index	Оцінка рівня «втоми від сповіщень» аналітиків SOC	Допомагає оптимізувати правила та скоротити кількість нерелевантних сповіщень	Високий індекс свідчить про перевантаження аналітиків; потребує постійного моніторингу та корекції правил

Рішення UEBA призначені для аналізу поведінкових моделей користувачів та сутностей з метою виявлення аномальних дій, які можуть свідчити про інсайдерські загрози, зловживання доступом або витік інформації. Метрики UEBA дозволяють оцінити ефективність аналітичних моделей та швидкість адаптації системи до динамічних змін у поведінці користувачів.

1. Anomaly Detection Rate (рівень виявлення аномалій)

Цей показник характеризує здатність системи UEBA виявляти нетипові патерни поведінки користувачів та сутностей. Високий рівень виявлення аномалій дозволяє своєчасно ідентифікувати підозрілі дії та зменшити ризик інсайдерських інцидентів.

2. Model Accuracy / Drift Resistance

Вимірює точність моделей поведінки та їх стійкість до “зсуву даних” (data drift), що виникає внаслідок зміни звичайної активності користувачів. Стійкі моделі забезпечують довгострокову ефективність системи UEBA та зменшують потребу у частому перенавчанні моделей.

3. Risk Score Reliability (надійність ризикових оцінок)

Показник відображає, наскільки стабільно та обґрунтовано система присвоює ризикові бали користувачам і сутностям. Надійна оцінка ризику дозволяє пріоритизувати інциденти, концентрувати ресурси SOC на найбільш критичних загрозах і ухвалювати обґрунтовані рішення щодо реагування.

4. Time to Behavioral Profile Update

Цей показник вимірює швидкість, з якою система адаптує поведінкові профілі користувачів. У динамічних корпоративних середовищах швидке оновлення профілів критично важливе для підтримки актуальності ризикових оцінок і точності виявлення аномалій.

Метрики порівняно у (таб. 2.4)

Таблиця 2.4

Характеристика метрик

Метрика	**Використання**	**Переваги**	**Недоліки**
Anomaly Detection Rate (рівень виявлення аномалій)	Оцінка здатності моделі UEBA виявляти нетипові патерни поведінки користувачів	Допомагає своєчасно ідентифікувати підозрілі дії; підвищує безпеку від інсайдерських загроз	Високий показник може створювати багато помилкових спрацювань, якщо моделі недостатньо адаптовані
Model Accuracy / Drift Resistance	Стійкість моделей до змін поведінки користувачів (data drift)	Забезпечує довгострокову ефективність UEBA; зменшує потребу в частих перенавчаннях моделей	Вразливість до раптових змін поведінки або нових сценаріїв атак
Risk Score Reliability	Наскільки стабільно й обґрунтовано система присвоює ризикові бали	Дозволяє пріоритизувати користувачів і події за ризиком; підвищує ефективність реагування	Недостатньо точні оцінки можуть призводити до помилкових підозр
Time to Behavioral Profile Update	Швидкість, із якою система оновлює поведінкові профілі користувачів	Дозволяє швидко реагувати на зміни в поведінці; підвищує релевантність оцінки ризику	Повільне оновлення профілів може призводити до затримки виявлення аномалій

Окрім технічних метрик, інструментом оцінки ефективності захисту є KPI (ключові показники ефективності) та KRI (ключові індикатори ризику). KPI використовуються для оцінювання рівня виконання процесів безпеки, таких як своєчасність розслідування інцидентів, дотримання політик доступу та рівень покриття системами моніторингу критичних активів. KRI дозволяють виміряти рівень загроз, пов'язаних із поведінкою користувачів: зростання кількості аномальних дій, частота спроб доступу до критичних ресурсів, різке збільшення операцій копіювання даних тощо. Разом ці індикатори формують інтегральне уявлення про реальний стан інсайдерських ризиків.

Основні KPI дозволяють оцінити поточний рівень контролю, ефективність реагування та продуктивність процесів розслідування інцидентів.

1. Частка покриття інсайдерських ризиків системами контролю

Цей показник відображає долю співробітників, пристроїв та бізнес-процесів, що контролюються системами безпеки, такими як DLP, UEBA та IAM. Високе охоплення дозволяє організації забезпечити повну видимість потенційних інсайдерських загроз та виявляти ризики на ранньому етапі.

2. KPI відповідності політикам безпеки

Цей показник включає відстеження порушень політик доступу, накладних переміщень даних та заборонених операцій. Моніторинг допомагає оцінити ступінь дотримання співробітниками правил безпеки та вчасно виявляти порушення, що можуть привести до інцидентів.

3. Скорочення часу реагування на інсайдерські інциденти

- MTTA (Mean Time to Acknowledge) – середній час до підтвердження інциденту аналітиками SOC.
- MTTI (Mean Time to Investigate) – середній час на повне розслідування інциденту.

Ці показники дозволяють оцінити операційну ефективність процесів реагування та забезпечують своєчасне зменшення потенційних збитків від інсайдерських дій.

4. Показник завершених розслідувань

Доля інцидентів, що пройшли повний цикл розслідування та класифікації, дозволяє оцінити якість процесу управління інцидентами. Високий показник демонструє ефективну роботу аналітиків SOC та здатність організації закривати випадки інсайдерських порушень повністю.

5. Кількість співробітників у групі високого ризику

Сегментація персоналу за рівнем ризику, визначеним UEBA або службою безпеки, дозволяє концентрувати ресурси на потенційно ризикових користувачах. Показник допомагає пріоритизувати контроль, навчання та моніторинг для зменшення ймовірності інсайдерських інцидентів (таб. 2.5).

Таблиця 2.5

Важливість KPI

KPI	**Опис**	**Важливість**	**Переваги**	**Недоліки**
Частка покриття інсайдерських ризиків системами контролю	Доля співробітників, пристроїв та бізнес-процесів, що контролюються DLP, UEBA, IAM	Дозволяє оцінити, наскільки комплексно організація контролює інсайдерські загрози	Виявляє прогалини в контролі; допомагає планувати додаткові заходи безпеки	Високе охоплення не гарантує ефективність контролю; потребує постійного оновлення
KPI відповідності політикам безпеки	Відстеження порушень політик доступу, заборонених операцій та накладних переміщень даних	Важливо для забезпечення відповідності нормативам та внутрішнім правилам	Допомагає підтримувати дисципліну серед співробітників; мінімізує ризик порушень	Не завжди відображає приховані порушення; потребує регулярного моніторингу
Скорочення часу реагування на інсайдерські інциденти (MTTA, MTTI)	MTTA – середній час до підтвердження інциденту; MTTI – середній час на розслідування	Критично для швидкого реагування на загрози та мінімізації збитків	Забезпечує оперативне реагування та ефективність SOC	Може бути складно скоротити у великих організаціях з високим навантаженням
Показник завершених розслідувань	Доля інцидентів, що пройшли повний цикл розслідування та класифікації	Дозволяє оцінити якість процесу розслідування та управління ризиком	Підвищує ефективність аналізу інцидентів; покращує управління ризиками	Не завжди враховує складність та серйозність інцидентів

Продовження таблиці 2.5

KPI	Опис	Важливість	Переваги	Недоліки
Кількість співробітників у групі високого ризику	Сегментація персоналу за рівнем ризику, визначеним UEBA або службою безпеки	Важливо для пріоритизації контролю та запобігання інсайдерським загрозам	Дозволяє концентрувати ресурси на потенційно ризикових користувачах	Може створювати стигму серед співробітників; ризик помилкових класифікацій

KRI (Key Risk Indicators) — це показники, що дозволяють оцінювати майбутні ризики та прогнозувати ймовірність внутрішніх порушень безпеки. Вони орієнтовані на виявлення потенційно ризикової поведінки користувачів, слабких місць у процесах та передумов для інсайдерських загроз [22]. Основні KRI включають:

1. Аномальна активність високоризикових користувачів

Цей показник відображає різке збільшення активності співробітників, яка відхиляється від типової поведінки для їхньої ролі. Під аномальною активністю мається на увазі збільшення кількості доступів до систем, нестандартні запити до критичних ресурсів або часті повторні спроби виконати дії, що виходять за межі звичайних операцій. Високий рівень аномальної активності може сигналізувати про потенційні спроби витоку інформації або зловживання доступом.

2. Рівень обхідних дій (policy bypass attempts)

Цей KRI відображає кількість спроб користувачів оминути технічні або організаційні засоби контролю, наприклад DLP, IAM або правила корпоративної політики безпеки. Часті спроби обходу політик можуть свідчити про наміри порушити правила або знайти лазівки у внутрішніх процесах. Моніторинг цього показника дозволяє оперативно реагувати на потенційні загрози та посилювати контроль уразливих точок.

3. Зростання кількості доступів до критичних даних

Цей показник фіксує збільшення звернень користувачів до конфіденційних або критично важливих даних, особливо поза робочим часом або з нетипових пристроїв. Нестандартний доступ до ресурсів може бути ознакою підготовки до

несанкціонованого використання даних або внутрішнього витоку. Моніторинг дозволяє швидко виявляти ризикову активність і запобігати інцидентам.

4. Очікуваний ризиковий вплив (Expected Loss Metric)

Цей показник дозволяє оцінити потенційні збитки у випадку реалізації інсайдерської загрози. Враховуються такі фактори, як тип інформації, роль користувача, рівень доступу та важливість бізнес-процесів. Критично важливим є те, що Expected Loss Metric допомагає пріоритизувати заходи безпеки та ресурсні витрати на захист даних з високим потенційним збитком.

5. Соціальні та організаційні фактори ризику

Ці показники дозволяють враховувати людський та організаційний аспект ризиків:

- Зміна посади - нові обов'язки або перехід на іншу роль можуть збільшувати ризик неправильного використання доступу.
- Передзвільний період - співробітники, які планують залишити компанію, можуть мати підвищений ризик витоку або саботажу.
- Конфлікти або негативні оцінки - проблемні відносини з керівництвом чи колегами можуть стимулювати ризикову поведінку.
- Різке падіння продуктивності - різка зміна робочих показників може свідчити про демотивацію або приховані наміри порушення політик безпеки.

Характеристика KRI нада у (таб. 2.6)

Таблиця 2.6

Характеристика KRI

KRI	**Опис**	**Важливість**	**Переваги**	**Недоліки**
Аномальна активність високоризикових користувачів	Різке зростання кількості дій, нетипових для певної ролі	Дозволяє виявляти потенційні загрози до їх реалізації	Своєчасне попередження про ризики; допомагає сконцентрувати увагу SOC на ключових користувачах	Може генерувати багато помилкових спрацьовувань; потребує налаштування порогів
Рівень обхідних дій (policy bypass attempts)	Кількість спроб оминання технічних та організаційних засобів контролю	Вказує на слабкі місця в політиках та процесах контролю	Дозволяє вчасно усунути вразливості; зменшує ймовірність порушень	Не завжди відображає мотиви користувача; потребує детального аналізу контексту

Продовження таблиці 2.6

Зростання кількості доступів до критичних даних	Особливо поза робочим часом або з нетипових пристроїв	Важливо для контролю над витоком інформації	Дозволяє виявляти потенційні інсайдерські загрози	Може створювати помилкові тривоги, якщо немає контексту роботи
Очікуваний ризиковий вплив (Expected Loss Metric)	Оцінка потенційних збитків залежно від типу інформації та ролі користувача	Дозволяє пріоритизувати заходи безпеки	Допомагає оцінювати економічний вплив загроз	Може бути складно точно розрахувати; залежить від достовірності вихідних даних
Соціальні та організаційні фактори ризику	Зміна посади, передзвільний період, конфлікти, різке падіння продуктивності	Допомагає прогнозувати ймовірність інсайдерських порушень	Дає комплексний огляд ризиків, що не видно в технічних метриках	Суб'єктивні фактори; складно формалізувати та виміряти

Значну увагу приділяють також метрикам виявлення та реакції, що характеризують ефективність процесу реагування на інциденти. До основних таких показників належать середній час виявлення інциденту (MTTD), середній час реагування (MTTR), тривалість фази ескалації та частка інцидентів, що були вирішені без повторного виникнення. Саме ці метрики дозволяють оцінити, наскільки швидко організація може ідентифікувати та нейтралізувати внутрішню загрозу до того, як вона спричинить значні збитки.

У контексті Security Operations Center (SOC) та корпоративних систем захисту інформації особливо критичними є метрики швидкості та якості реагування на інциденти. Вони дозволяють оцінювати ефективність виявлення загроз, правильність класифікації інцидентів і швидкість нейтралізації інцидентів.

Метрики виявлення

1. MTTD (Mean Time to Detect). Середній час від початку інциденту до його виявлення. Ключовий показник для SOC, оскільки зменшення MTTD дозволяє оперативніше реагувати на загрози та знижувати потенційний збиток.

2. Detection Coverage. Частка інцидентів, які система здатна виявити згідно з моделлю загроз (Threat Model). Високе охоплення забезпечує повну видимість активності та виявлення більшості потенційних інцидентів.

3. Incident Classification Accuracy. Якість класифікації інцидентів, тобто правильність визначення критичності та типу загрози. Висока точність класифікації дозволяє SOC ефективніше пріоритизувати реагування та ресурси.

4. Detection Depth. Глибина виявлення інциденту: наскільки система здатна визначити першопричину інциденту, а не лише поверхневі симптоми. Глибокий аналіз сприяє ефективнішому усуненню причин загроз та запобіганню повторним інцидентам.

Метрики реакції

1. MTTR (Mean Time to Response / Remediation)

Час, необхідний для нейтралізації загрози або відновлення нормального функціонування системи. Зменшення MTTR є критично важливим для зниження негативного впливу інцидентів на бізнес-процеси.

2. Containment Time

Інтервал між підтвердженням інциденту та обмеженням його впливу. Швидке обмеження дозволяє мінімізувати шкоду від порушення безпеки та витоку даних.

3. Response Workflow Efficiency

Оцінка автоматизації процесів реагування (SOAR), включаючи частку інцидентів, які відпрацьовано без участі людини. Підвищення ефективності workflow дозволяє скорочувати час реагування та навантаження на аналітиків SOC.

4. Post-Incident Review Completion Rate

Доля інцидентів, що пройшли повний аудит, аналіз причин та оновлення політик. Показник важливий для постійного вдосконалення процесів безпеки та навчання SOC.

5. Cost of Response per Incident

Враховує всі витрати на реагування: персонал, простій систем, SOAR-

інфраструктуру, юридичні та іміджеві наслідки. Показник дозволяє оцінити економічну ефективність процесів реагування та оптимізувати ресурси (таб. 2.7).

Таблиця 2.7

Метрики та їх порівняння

Метрика	**Опис**	**Взаємозв'язок з іншими метриками**	**Переваги**	**Недоліки**
MTTD (Mean Time to Detect)	Середній час від початку інциденту до його виявлення	Впливає на MTTR і Containment Time: чим швидше виявлено, тим швидше реагують	Швидке виявлення зменшує збитки; дозволяє раннє втручання	Не враховує глибину або точність класифікації; залежить від охоплення Detection Coverage
Detection Coverage	Частка інцидентів, які система здатна виявити згідно з моделлю загроз	Підвищує точність MTTD та Incident Classification Accuracy	Забезпечує повну видимість; зменшує «сліпі зони»	Високе охоплення потребує ресурсів; можливе зростання помилкових спрацьовувань
Incident Classification Accuracy	Якість визначення критичності та типу загрози	Впливає на MTTR, Containment Time та Response Workflow Efficiency	Дозволяє пріоритизувати інциденти; ефективніше використання ресурсів SOC	Помилки у класифікації можуть призвести до неправильного реагування
Detection Depth	Наскільки система визначає першопричину інциденту	Підвищує ефективність MTTR і Post-Incident Review Completion Rate	Глибокий аналіз допомагає запобігти повторним інцидентам	Вимагає складних аналітичних моделей; збільшує час на обробку
MTTR (Mean Time to Response / Remediation)	Час до нейтралізації загрози або відновлення нормальної роботи	Залежить від MTTD, Containment Time, Response Workflow Efficiency	Мінімізує збитки; оцінює ефективність реагування	Може бути довгим у великих мережах; залежить від автоматизації та ресурсів
Containment Time	Інтервал між підтвердженням інциденту та обмеженням його впливу	Впливає на MTTR та Cost of Response	Швидке обмеження мінімізує шкоду; знижує ризик поширення інциденту	Не завжди враховує довгострокові наслідки; залежить від готовності процесів

Продовження таблиці 2.7

Метрика	**Опис**	**Взаємозв'язок з іншими метриками**	**Переваги**	**Недоліки**
Response Workflow Efficiency	Оцінка автоматизації процесів реагування (SOAR)	Зменшує MTTR та Containment Time; впливає на Cost of Response	Знижує навантаження на аналітиків; прискорює реагування	Вимагає налаштування та підтримки автоматизації; ризик помилкових автоматичних дій
Post-Incident Review Completion Rate	Доля інцидентів, що пройшли повний аудит та оновлення політик	Підвищує ефективність Detection Depth і майбутнього реагування	Сприяє навчанням SOC; удосконалює процеси безпеки	Може бути ресурсомістким; час проведення рев'ю може відкладати оновлення політик
Cost of Response per Incident	Витрати на персонал, SOAR, простій систем, юридичні та іміджеві наслідки	Залежить від MTTR, Containment Time та Response Workflow Efficiency	Дозволяє оцінити економічну ефективність; оптимізує ресурси	Не враховує непередбачувані наслідки; складно точно оцінити комплексні витрати

Проаналізувавши все вище сказане можна дійти висновку, що сучасні підходи до оцінки ефективності систем захисту від інсайдерських загроз ґрунтуються на комплексному аналізі технічних, процесних і поведінкових показників. Поєднання метрик роботи DLP, SIEM та UEBA із KPI та KRI забезпечує системне бачення рівня безпеки та дозволяє приймати обґрунтовані управлінські рішення щодо вдосконалення архітектури інформаційного захисту.

2.3. Основні проблеми наявних підходів

Попри значний розвиток систем моніторингу та аудиту інформаційної безпеки, наявні підходи до оцінки ефективності протидії інсайдерським загрозам залишаються неповними та недостатньо узгодженими з реальними потребами організацій. Однією з ключових проблем є неповнота оцінювання, що зумовлена складністю і багатовимірністю інсайдерських ризиків. Більшість методик фокусуються переважно на технічних аспектах, зокрема на роботі DLP, SIEM чи UEBA, проте не охоплюють організаційні, психологічні та поведінкові фактори, які мають вирішальне значення для правильного визначення намірів користувача. У

результаті перевірка часто не дозволяє сформувати цілісну картину інцидентів і може пропустити критичні прояви неналежної поведінки співробітників. Важлива проблема є в тому, що є високий рівень хибних спрацювань у сучасних системах захисту. DLP та SIEM нерідко генерують надмірну кількість попереджень, які не мають реального зв'язку з інсайдерською активністю. UEBA, що базується на поведінкових моделях, також може створювати аномальні сповіщення через зміну робочих навичок користувачів або неякісне налаштування алгоритмів. Велика кількість хибнопозитивних подій суттєво перевантажує аналітиків безпеки, знижує ефективність реагування та може призвести до ігнорування справді небезпечних інцидентів. Крім того, це ускладнює проведення аудиту, оскільки аудитори змушені витрачати час на аналіз малозначущих записів, що знижує якість оцінювання [24].

Проблемою залишається й обмежена інтеграція наявних підходів з процесами внутрішнього аудиту. Переважна більшість методик створювалися для оперативної роботи підрозділів інформаційної безпеки, а не для аудиторської перевірки. Унаслідок цього аудитори часто не отримують повного доступу до даних або ж інформація подається у форматі, який недостатньо придатний для формальної оцінки відповідності. Крім того, процеси аудиту не завжди включають глибоку перевірку налаштувань систем моніторингу, ефективності кореляційних правил чи якості журналювання. Замість цього акцент робиться на документуванні процесів, що не дозволяє комплексно оцінити реальний функціонал технічних засобів та їхню ефективність у протидії інсайдерам.

Фундаментальною проблемою є відсутність стандартизованої методики, яка була б присвячена саме інсайдерським загрозам. Попри наявність численних стандартів з управління інформаційною безпекою, жоден із них не пропонує єдиного алгоритму оцінювання рівня захисту від внутрішніх порушників. Це створює значну варіативність у підходах різних організацій, що утруднює порівняння результатів аудиту та впровадження узгоджених критеріїв ефективності. Відсутність стандартизованої методики також призводить до того,

що оцінювання часто залежить від досвіду аудиторів, суб'єктивності їхніх висновків та обмеженості наявних інструментів (таб. 2.8).

Таблиця 2.8

Головні проблеми та їх важливість

Проблема	**Опис**	**Важливість**	**Приклад наслідків ігнорування**
Помилкові спрацювання (False Positives)	Надмірна кількість некоректних сповіщень від DLP, SIEM або UEBA	Висока – перевантажує аналітиків SOC, знижує довіру до систем	Аналітики можуть ігнорувати реальні загрози, що призводить до витоку даних
Пропущені інциденти (False Negatives)	Інциденти, які залишаються непоміченими через обмеження системи	Критична – «сліпі зони» дозволяють загрозам залишатися непоміченими	Несанкціонований доступ до конфіденційних даних або витік інформації
Обмежене охоплення (Coverage)	Не всі бізнес-процеси, пристрої та користувачі інтегровані у системи контролю	Висока – обмежує видимість і контроль над інсайдерськими ризиками	Частина інцидентів залишається поза увагою SOC, знижується ефективність захисту
Затримки в детекції та реагуванні (MTTD, MTTR)	Пізнє виявлення інцидентів та уповільнене реагування	Критична – збільшує потенційні збитки	Інциденти встигають поширитися по мережі, збільшуються втрати та простій систем
Повільне оновлення моделей поведінки (Behavioral Profile Update)	UEBA не встигає адаптуватися до змін активності користувачів	Висока – зниження точності виявлення аномалій	Аномальні дії користувачів залишаються непоміченими, збільшується ризик внутрішніх порушень
Недосконалі правила кореляції (Correlation Rule Accuracy)	Низька якість правил у SIEM, що призводить до нерелевантних сповіщень	Висока – знижує точність і ефективність SOC	Втрата критичних подій або перевантаження аналітиків SOC непотрібними сповіщеннями
Обмежена глибина аналізу (Detection Depth)	Системи не завжди визначають першопричину інциденту	Висока – складно запобігти повторним інцидентам	Усунуті лише симптоми загрози, повторні інциденти виникають повторно
Розрізнені рішення та слабка інтеграція	DLP, SIEM, UEBA, IAM працюють окремо, без централізованого управління	Висока – ускладнює побудову повної картини інсайдерських ризиків	Втрата узгодженості при реагуванні, дублювання зусиль, повільне реагування

Продовження таблиці 2.8

Проблема	**Опис**	**Важливість**	**Приклад наслідків ігнорування**
Відсутність єдиних метрик ефективності	Немає уніфікованої системи KPI та KRI для оцінки ефективності	Середня – складно порівнювати та оптимізувати системи	Неможливо визначити слабкі місця, важко обґрунтувати інвестиції у безпеку
Складність оцінки економічної ефективності	Витрати на реагування важко формалізувати	Середня – ускладнює планування бюджету	Перевитрати на інфраструктуру та персонал, неефективне використання ресурсів

Враховуючи сучасні підходи до оцінки ефективності засобів протидії інсайдерським загрозам мають низку суттєвих недоліків: неповноту охоплення ризиків, надмірну кількість хибних спрацювань, слабку інтеграцію з внутрішнім аудитом та відсутність стандарту, присвяченого саме інсайдерським атакам. Вирішення цих проблем потребує розробки комплексної, відтворюваної та ризикорієнтованої методики, яка забезпечить системність та об’єктивність аудиторської перевірки і ляже в основу підвищення рівня інформаційної безпеки організацій.

Висновок до розділу 2

У розділі проведено комплексний аналіз сучасних методик аудиту інформаційної безпеки та підходів до оцінювання ефективності засобів протидії інсайдерським загрозам. Розглянуті стандарти та фреймворки — ISO/IEC 27001/27002, NIST SP 800-53, CIS Controls, COBIT 2019, OWASP SAMM, регуляторні підходи та ризик-орієнтований аудит — демонструють значну різноманітність існуючих моделей, що дає змогу будувати як комплексні, так і цільові перевірки залежно від потреб організації. Кожна методика має власні переваги, зокрема системність, масштабованість, практичність або глибину охоплення, а також певні обмеження, пов’язані з ресурсозатратністю, необхідністю високої кваліфікації персоналу чи складністю адаптації до різних моделей управління.

Узагальнення результатів аналізу засвідчило, що для оцінки ефективності систем захисту від інсайдерських загроз критичним є поєднання технічних та

організаційних підходів. Системи DLP, SIEM, UEBA та PAM забезпечують різні аспекти контролю та моніторингу, формуючи комплексне середовище виявлення відхилень і попередження потенційно небезпечних дій внутрішніх користувачів. Разом із тим їх результативність значною мірою залежить від коректності налаштувань, якості зібраних даних та інтеграції в загальну систему управління ризиками.

Проведений аналіз показав, що сучасні методики аудиту та показники ефективності дають змогу всебічно оцінювати зрілість систем безпеки, проте не забезпечують універсального рішення для всіх типів організацій. Виявлені проблеми, зокрема відсутність стандартизованих метрик саме для інсайдерських загроз, складність інтерпретації поведінкової аналітики та залежність від кваліфікації фахівців, підкреслюють потребу в розробленні інтегрованого підходу, який враховуватиме специфіку корпоративних середовищ та особливості моделей користувацької поведінки.

Результати аналізу формують теоретичне підґрунтя для подальшої розробки та обґрунтування багаторівневої системи оцінювання ефективності захисту від інсайдерських загроз, яка стане основою для практичної частини дослідження та створення оптимізованої моделі аудиту корпоративної безпеки.

РОЗДІЛ 3. РОЗРОБКА ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДИКИ ПЕРЕВІРКИ ЕФЕКТИВНОСТІ ЗАСОБІВ ПРОТИДІЇ ІНСАЙДЕРСЬКИМ ЗАГРОЗАМ

Для досягнення мети буде проведенна розробка та реалізація методики перевірки ефективності засобів протидії інсайдерським загрозам: буде сформовано покроковий алгоритм аудиту, визначено ключові етапи перевірки технічних засобів (DLP, SIEM, UEBA, IAM), оцінки політик і процесів, проведення практичних тестів та симуляцій інсайдерських дій, визначення KPI/KRI, аналізу отриманих результатів і формування рекомендацій щодо підвищення ефективності захисту від внутрішніх загроз.

3.1. Концепція та принципи методики

Методика перевірки ефективності засобів протидії інсайдерським загрозам ґрунтується на поєднанні сучасних підходів до оцінювання безпеки, принципів ризикорієнтованого управління та стандартів аудиту інформаційних систем. Її мета полягає у створенні відтворюваної, структурованої та практично орієнтованої процедури оцінювання, яка дає можливість визначити реальний рівень готовності організації до протидії діям зловмисних або недбалих внутрішніх користувачів. Комплексність методики визначається поєднанням організаційних, процедурних та технологічних аспектів оцінювання. У процесі перевірки враховуються внутрішні нормативні документи, чинні політики інформаційної безпеки, структури доступів, практика управління привілейованими обліковими записами, а також реальний стан технічних систем контролю — зокрема DLP, SIEM, UEBA та PAM. Таке багатовимірне охоплення дозволяє отримати інтегральне уявлення про те, наскільки збалансовано функціонують елементи системи захисту та чи здатні вони спільно протистояти інсайдерським активностям (таб. 3.1).

Таблиця 3.1

Засоби та приклади використання

Засіб	Приклад використання у тестових сценаріях	Рекомендовані метрики ефективності	Взаємодія у комплексній системі
DLP (Data Loss Prevention)	Блокування копіювання конфіденційних документів на зовнішній носій або пересилання через e-mail; контроль доступу до критичних файлів.	- Частка спроб витоку, виявлених системою (%)- Кількість хибнопозитивних спрацювань- Час реакції на інцидент	Передає події до SIEM для кореляції; разом з UEBA аналізує аномальну поведінку користувачів; PAM обмежує доступ до критичних ресурсів.
SIEM (Security Information and Event Management)	Кореляція подій із DLP, UEBA та PAM; сповіщення про підозрілу активність користувачів; формування централізованих звітів.	- Час виявлення інциденту (MTTD)- Час реагування (MTTR)- Точність виявлення інцидентів	Центральний вузол збору даних: отримує події від DLP, UEBA, PAM; забезпечує аналітику та сповіщення; передає результати в автоматизовані системи реагування.
UEBA (User and Entity Behavior Analytics)	Виявлення нетипової поведінки: доступ до файлів у незвичний час, масове завантаження даних, спроби обходу політик.	- Коефіцієнт виявлення аномалій (%)- Частка хибних спрацьовувань- Відсоток виявлених раніше непомічених інцидентів	Спільно з DLP визначає потенційні загрози; події передає до SIEM для кореляції; взаємодіє з PAM для відстеження привілейованих дій.
PAM (Privileged Access Management)	Контроль дій адміністраторів: записи команд у критичних системах, обмеження сесій, відстеження ескалації привілеїв.	- Кількість несанкціонованих привілейованих дій- Час виявлення зловживань- Відсоток дотримання політик доступу	Додає контекст до подій UEBA і DLP; передає журнали у SIEM для кореляції; забезпечує контроль критичних ресурсів у комплексі системи.

Розроблена схема:

1. **DLP** захищає самі дані, а UEBA визначає аномальну поведінку користувачів.
2. **SIEM** централізує всі події, корелює їх і формує аналітику.
3. **PAM** контролює привілейовані доступи і надає додатковий контекст для аналізу аномалій.

Схему зображено на (рис 3.1).

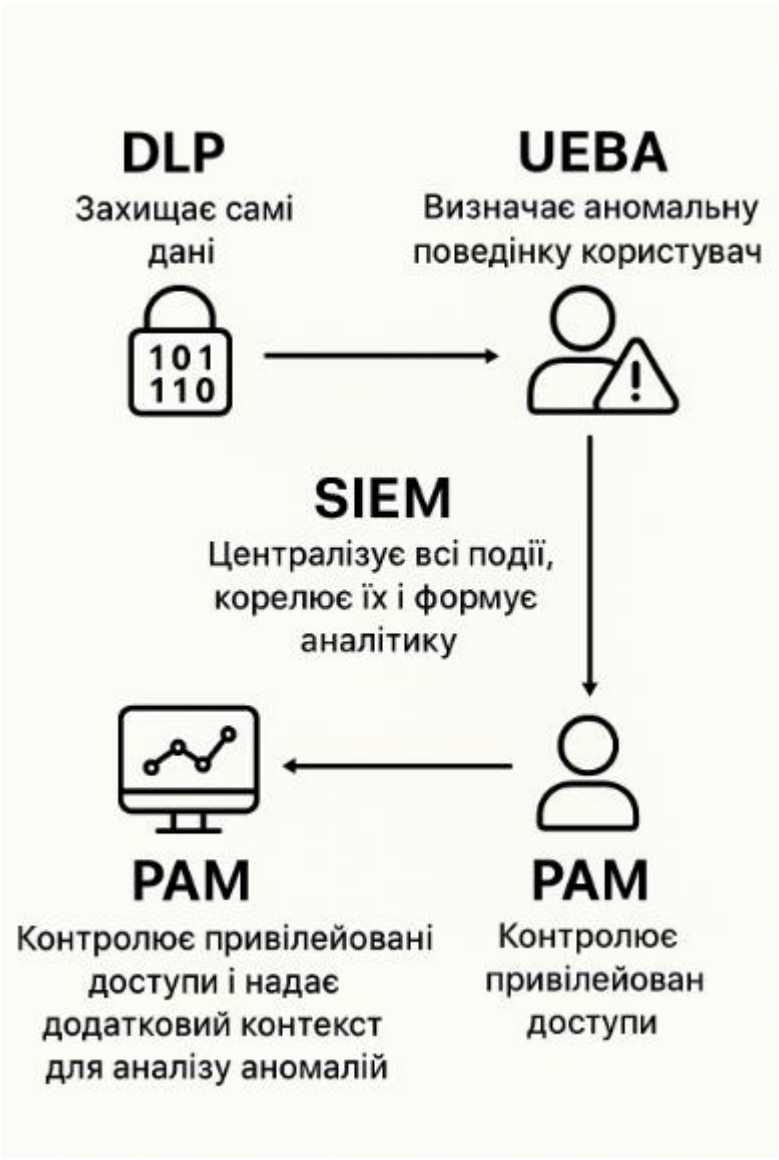

Рис. 3.1. Розроблена схема

Як ми бачимо разом вони формують інтегровану багаторівневу систему, здатну виявляти, блокувати та аналізувати інсайдерські загрози, а також вимірювати ефективність захисту за допомогою конкретних метрик.

Важливою складовою методики є оцінювання стану журналювання подій і можливостей систем моніторингу. Аналізується повнота, цілісність та доступність логів, оскільки вони є основою для виявлення підозрілих дій та подальшого розслідування інцидентів. Значна увага приділяється поведінковій аналітиці, що дозволяє виявляти непрямі та приховані ознаки інсайдерських порушень, які не завжди можна зафіксувати на основі простих технічних тригерів. Методика передбачає практичне моделювання інсайдерських сценаріїв, що дозволяє оцінити

здатність організації виявляти та запобігати реальним загрозам. Імітація дій зловмисного співробітника, тестування обходу систем контролю чи аналіз реакції на нетипові поведінкові патерни забезпечують реалістичність оцінювання та дозволяють перевірити ефективність засобів безпеки в умовах, наближених до реальних.

Враховуючи все вище сказанне, методика не обмежується формальним аналізом документів чи конфігурацій, а формує багаторівневу, адаптивну систему аудиту, що поєднує стратегічне бачення та практичні механізми виявлення загроз. Її застосування сприяє підвищенню загального рівня кіберстійкості організації, дозволяє своєчасно виявляти слабкі місця та формувати рекомендації щодо вдосконалення системи захисту від інсайдерських дій. Ризикорієнтованість у контексті методики перевірки ефективності засобів протидії інсайдерським загрозам передбачає зосередження уваги на тих елементах організаційної та технічної структури, де ймовірність виникнення інсайдерської активності є найвищою, а можливі наслідки — найбільш критичними. Такий підхід дозволяє оптимально розподілити ресурси аудиту, зменшити обсяг непотрібних перевірок і забезпечити глибший аналіз саме тих сегментів, які становлять найбільшу загрозу для безпеки інформаційних активів.

У межах ризикорієнтованого підходу ключовою категорією аналізуються працівники з підвищеним рівнем доступу, а також ті, чия діяльність пов’язана з обробкою конфіденційної інформації: адміністратори систем, співробітники фінансових підрозділів, оператори баз даних, науковий персонал, що працює з чутливими розробками тощо. Вивчається характер їхніх повноважень, історія змін доступів, наявність привілейованих облікових записів і відповідність ролей їхнім посадовим обов’язкам.

Одночасно аналізу підлягають критичні бізнес-процеси, які можуть зазнати шкоди внаслідок інсайдерських дій. Це може включати обробку персональних даних, фінансову звітність, доступ до дослідницьких матеріалів, управління серверною інфраструктурою тощо. У рамках оцінювання визначається важливість цих процесів для загальної діяльності організації, ступінь їх автоматизації та

залежність від конкретних користувачів або служб. Вивчення чутливості інформаційних активів, а саме оцінювання даних з погляду їх конфіденційності, цілісності та доступності. Дані поділяються на категорії — від загальнодоступних до строго конфіденційних — що дозволяє визначити потенційні наслідки компрометації та пріоритетність перевірки відповідних систем.

Аналіз здійснюється з урахуванням реальних умов діяльності організації: структури взаємодії між підрозділами, типових робочих навантажень, сезонності бізнес-процесів, особливостей використання інформаційних систем. Важливе місце займає моделювання ймовірних сценаріїв загроз, включно з діями зловмисного інсайдера, помилками користувачів, неправомірним використанням доступів або компрометацією облікових записів.

Відтворюваність методики досягається завдяки використанню стандартизованої структури, чіткому визначенню послідовності дій та фіксації вимог до кожного етапу оцінювання. Детальний опис процедур, критеріїв, форм документування та способів аналізу результатів забезпечує можливість проводити аудит незалежно від складу команди, часових рамок або особливостей конкретного середовища. Це робить методику універсальною та придатною для використання у різних організаціях і сценаріях.

Чітко структурована послідовність етапів - від підготовки, аналізу політик та технологічних засобів до тестування інсайдерських сценаріїв і формування підсумкового звіту - дозволяє багаторазово повторювати процедуру з отриманням зіставних та об’єктивних результатів. Стає можливе відстеження динаміки змін, порівняння показників ефективності за різні періоди та оцінювання впливу впроваджених заходів на рівень безпеки. Важливою перевагою відтворюваності є можливість застосовувати методику в різних підрозділах організації, з урахуванням їх функціональної специфіки. Це дає змогу проводити порівняльний аналіз, визначати слабкі ланки, а також формувати уніфіковані рекомендації, релевантні всіх структурним одиницям. Вона сприяє інтеграції методики у регулярні процеси управління інформаційною безпекою. Перевірка може бути включена до плану внутрішніх аудитів, слугувати інструментом контролю після

впровадження оновлень або змін у політиках, а також виконувати функцію періодичної оцінки зрілості системи захисту від інсайдерських загроз. Завдяки цьому методика стає не разовою процедурою, а постійним механізмом підтримання та підвищення рівня кіберстійкості організації.

Ключовим елементом концепції методики є модель інсайдерських загроз, яка становить основу для формування сценаріїв перевірки, вибору метрик оцінювання та аналізу ефективності наявних засобів захисту. Модель визначає типові ролі внутрішніх користувачів, їх можливі дії, мотиви та наслідки порушень, що дає змогу структурувати аудит і забезпечити релевантність тестування реальним ризикам.

У межах дослідження виділяються три категорії інсайдерів, кожна з яких характеризується специфічною поведінкою та векторами впливу на інформаційну безпеку організації.

1. Недбалий співробітник, що порушує правила безпеки ненавмисно; (це користувач, який ненавмисно порушує правила безпеки внаслідок недостатньої обізнаності, неуважності або нехтування вимогами політик. Для цієї категорії характерні ризики випадкових витоків, неправильного поводження з конфіденційною інформацією, некоректного налаштування засобів доступу або передачі даних третім сторонам. Перевірка спрямована на визначення того, наскільки система здатна виявляти і блокувати такі помилки до того, як вони спричинять шкоду).

2. Зловмисний співробітник, мотивований особистою вигодою або шкодою організації; **(**діє свідомо й цілеспрямовано, мотивований матеріальною вигодою, особистим конфліктом або бажанням завдати репутаційних чи фінансових збитків. Для таких сценаріїв характерні спроби обходу технічних засобів контролю, збір і непомітне виведення даних, ескалація привілеїв або маніпулювання системами обліку. Модель інсайдерів цього типу дає змогу перевірити, чи спроможні засоби безпеки протидіяти навмисним, добре прихованим діям).

3. Компрометований співробітник, дані якого потрапили у руки сторонніх осіб. **(** становить окрему категорію, коли внутрішні облікові дані потрапляють до сторонніх осіб унаслідок фішингу, зловмисного ПЗ або соціальної інженерії. Формально такі дії можуть виглядати як легітимна активність, що ускладнює їх виявлення. Перевірка за цим напрямом спрямована на визначення того, наскільки ефективно працюють поведінкові аналізатори, системи виявлення аномалій та засоби контролю доступу).

Беручи до уваги все вище сказане, побудована модель інсайдерських загроз забезпечує логічну й методологічну основу всієї методики, дозволяючи здійснювати оцінку не лише технічних можливостей, але й готовності організації протистояти різним типам внутрішніх ризиків. Вона формує структуру сценаріїв тестування, визначає фокус аудиту та сприяє точності й релевантності отриманих результатів.

Визначення меж аудиту (scope), необхідно враховувати оскільки саме від чіткої фіксації об’єкта перевірки залежить коректність оцінювання та валідність отриманих результатів. Межі аудиту задають конкретні системи, сервіси, інфраструктурні компоненти, підрозділи та бізнес-процеси, у рамках яких здійснюється аналіз засобів протидії інсайдерським загрозам. До них також входить деталізований перелік категорій даних, що підлягають захисту, рівнів доступу користувачів, каналів обміну інформацією, а також конкретних механізмів моніторингу, журналювання та контролю.

Визначення scope передбачає створення повної карти інформаційних активів, визначення критичних точок, у яких можливе втручання інсайдера, та окреслення технологічних і організаційних меж, у яких буде здійснюватися тестування. Сюди входять:

- системи управління доступами та автентифікацією;
- платформи моніторингу та журналювання (DLP, SIEM, UEBA, інші);
- сегменти мережі з підвищеним ризиком;
- підрозділи чи групи співробітників, які працюють із конфіденційними даними;

- процеси обробки, передачі та зберігання інформації.

Коректно визначений scope гарантує, що перевірку буде проведено всебічно, без пропуску важливих компонентів, а отримані дані матимуть чіткий контекст для інтерпретації. Це також дозволяє узгодити очікування замовника, визначити обмеження щодо доступу аудиторів до певних систем і забезпечити повторюваність процедури у майбутніх аудитах. Таким чином, межі аудиту виступають фундаментальною передумовою повноцінності, точності та прозорості методики оцінювання ефективності засобів протидії інсайдерським загрозам.

Таблиця 3.2

Етапи та опис

Етап методики	**Що відбувається на цьому етапі**	**Переваги**	**Недоліки / Обмеження**
Підготовчий етап	Визначення цілей, меж аудиту, відповідальних осіб; збір базової інформації про інфраструктуру та політики.	Створює чітке бачення перевірки; мінімізує ризик пропуску важливих компонентів.	Потребує часу; можливі неточності через неповні дані від замовника.
Вивчення політик та регламентів	Аналіз внутрішніх документів, що регламентують безпеку, доступи, поведінку персоналу.	Дає змогу оцінити формальну готовність організації; виявляє прогалини в нормативній базі.	Політики можуть бути застарілими; документи не завжди відповідають реальній практиці.
Аналіз технологічних засобів (DLP, SIEM, UEBA, PAM)	Перевірка налаштувань, роботи, інтеграції та покриття технічних систем.	Забезпечує реальну оцінку можливостей виявлення та реагування; дозволяє виявити неефективні конфігурації.	Великий обсяг технічних деталей; залежність від доступу до систем; можливість упущення прихованих проблем.
Аналіз управління доступами	Оцінка розподілу ролей, політик доступу, принципів мінімальних привілеїв, процедури надання/відкликання доступів.	Сприяє зменшенню ризику ескалації привілеїв і помилок у доступах; виявляє надлишкові права.	Може займати багато часу, особливо в великих організаціях; потребує точних даних про користувачів.
Верифікація журналів безпеки	Аналіз повноти, структурованості та доступності логів; оцінка коректності кореляції подій.	Дозволяє оцінити здатність систем до ретроспективного аналізу; виявляє прогалини в моніторингу.	Логи можуть бути неповними, перезаписаними або неправильно збереженими; потребує доступу до великих обсягів даних.

Продовження таблиці 3.2

Етап методики	**Що відбувається на цьому етапі**	**Переваги**	**Недоліки / Обмеження**
Проведення тестових інсайдерських сценаріїв	Виконання контрольованих дій, що імітують поведінку інсайдера: копіювання, видалення, передавання даних, ескалація доступів тощо.	Найбільш інформативний етап; дозволяє оцінити реальну роботу засобів у дії; формує доказову базу.	Потребує високої компетентності виконавців; може бути ризик впливу на продуктивні системи; складно моделювати всі можливі сценарії.
Узагальнення результатів	Формування звіту, визначення рівня ефективності, виявлення недоліків, рекомендацій та плану покращення.	Дає комплексну картину стану захищеності; дозволяє формувати чіткі кроки щодо підвищення безпеки.	Якість висновків залежить від повноти даних на попередніх етапах; можливість суб’єктивності.

3.2. Алгоритм проведення перевірки

Розроблений алгоритм проведення перевірки складається з семи послідовних етапів, що охоплюють підготовку, збір інформації, технічний та організаційний аналіз, а також виконання контрольованих тестових сценаріїв.

1. Підготовчий етап

На цьому етапі визначаються цілі перевірки, формуються робоча група та графік аудиту. Проводиться збір попередньої інформації про структуру підприємства, категорії персоналу, перелік систем і набори критичних даних. Визначаються доступи для аудиторів, формуються технічні засоби для тестування та узгоджуються умови проведення імітаційних інсайдерських сценаріїв.

2. Вивчення політик та регламентів

Аналізуються локальні політики інформаційної безпеки, внутрішні нормативні документи, процедури управління доступами, регламенти моніторингу та реагування на інциденти. Метою є оцінити формальну базу протидії інсайдерським загрозам: наскільки чітко визначено відповідальність працівників, чи є вимоги до захисту інформації, чи передбачені санкції за порушення.

3. Аналіз технологічних засобів контролю (DLP, SIEM, UEBA, PAM)

На цьому етапі здійснюється детальна перевірка функціональних можливостей технічних рішень:

– DLP-системи аналізуються на предмет контролю каналів витоку, відповідності політик, ефективності сповіщень;

– SIEM-платформи оцінюються щодо повноти збору журналів, наявності кореляційних правил і здатності виявляти інциденти в реальному часі;

– UEBA-рішення аналізуються на предмет побудови моделей поведінки користувачів та виявлення відхилень;

– PAM-системи перевіряються щодо управління привілейованими обліковими записами, запису дій та контролю доступу до критичних ресурсів [25].

4. Аналіз управління доступами

На цьому етапі перевіряється відповідність призначених доступів посадовим обов'язкам, оцінюється наявність надлишкових прав, правильність сегментації ролей, регулярність ревізії доступів та наявність контролю над критичними обліковими записами. Також аналізуються механізми багатофакторної автентифікації та процедури надання/відкликання доступів [26].

5. Верифікація журналів безпеки

Виконується перевірка повноти, цілісності та доступності журналів подій. Визначається, чи покривають журнали весь необхідний спектр активностей користувачів, чи налаштовано централізоване збирання, чи ведеться кореляція подій. Оцінюється можливість відтворити реальну картину інциденту на основі журналів.

6. Проведення тестових інсайдерських сценаріїв

Виконуються практичні імітації типових дій потенційного інсайдера, наприклад:

– несанкціоноване копіювання конфіденційних даних;
– спроби обходу DLP-контролю;
– маніпуляції з привілейованими доступами;
– видалення або модифікація журналів;
– виконання нетипових операцій у робочий час або поза ним.

Метою є перевірити, чи здатні наявні засоби виявити та блокувати ці дії, а також наскільки швидко реагують системи й персонал [27].

7. Узагальнення результатів

Після проходження всіх етапів формується комплексний звіт. У ньому відображаються виявлені інциденти, статистика реагування, стан політик, відповідність доступів, ефективність технічних засобів та рівень дотримання регламентів. Розраховуються метрики ефективності та формується підсумковий висновок.

3.3. Практичне застосування методики та система метрик для оцінювання ефективності

Для кількісного та якісного оцінювання ефективності застосовується система метрик, яка дозволяє об’єктивно порівнювати результати перевірок та оцінювати динаміку рівня захищеності.

Метрика точності виявлення

Визначає частку коректно виявлених інцидентів порівняно з їх реальною кількістю. Охоплює показники:

– кількість виявлених інсайдерських активностей;

– частка хибнопозитивних спрацьовувань;

– частка хибнонегативних інцидентів.

Метрика швидкості реакції

Оцінює, наскільки оперативно система або персонал реагує на подію. Включає час між:

– моментом виникнення інциденту і його виявленням;

– сповіщенням і початком реагування;

– початком реагування і локалізацією інциденту.

Інтегральний показник ефективності

Це комплексна оцінка, що поєднує точність, швидкість, повноту виявлення, якість журналів та здатність систем до аналізу поведінки користувачів.

Інтегральний показник дозволяє визначити загальний рівень протидії інсайдерським загрозам у конкретній організації [28].

Рівні зрілості (maturity levels)

Методика передбачає класифікацію системи безпеки за п’ятьма рівнями зрілості:

1. Низький рівень — мінімальний набір засобів, відсутність політик.
2. Базовий рівень — частковий контроль та окремі технічні рішення.
3. Середній рівень — наявність регламентів, інтегрованих засобів.
4. Високий рівень — комплексний моніторинг, аналітика поведінки.
5. Просунутий рівень — адаптивні системи, автоматизоване реагування.

Методика перевірки ефективності засобів протидії інсайдерським загрозам передбачає комплексну оцінку технічних, організаційних та процесних компонентів безпеки. Практичне застосування методики під час внутрішнього аудиту включає кілька ключових етапів:

1. Підготовчий етап

Підготовчий етап є критично важливим для успішного проведення внутрішнього аудиту, оскільки від нього залежить точність, повнота та коректність подальших оцінок. На цьому етапі здійснюється чітке визначення об’єкта аудиту, збір вихідної інформації та встановлення критеріїв оцінки ефективності систем захисту**.**

1.1. Визначення об’єкта аудиту

На даному підетапі аудитори визначають конкретні елементи інфраструктури та процесів, які будуть перевірятися**.** Це включає:

- Технічні системи контролю та моніторингу:
  - DLP (Data Loss Prevention),
  - SIEM (Security Information and Event Management),
  - UEBA (User and Entity Behavior Analytics),
  - IAM (Identity and Access Management) [29].
- Політики безпеки**:**
  - правила доступу до інформаційних ресурсів,

- обмеження прав користувачів,
- процедури обробки конфіденційних даних.
- Процеси реагування SOC (Security Operations Center)**:**
- реєстрація, класифікація,
- ескалація та завершення інцидентів, а також автоматизовані механізми реагування через SOAR.

Коротко кажучи визначення об’єкта аудиту дозволяє обмежити рамки перевірки, забезпечити системність та уникнути пропусків критично важливих компонентів безпеки [30].

1.2. Збір первинної інформації

На цьому підетапі здійснюється детальний збір даних про поточний стан систем та процесів безпеки. Основні дії включають:

- Формування переліку користувачів та ролей
- визначення, які співробітники мають доступ до критичних даних та систем.
- Оцінка рівнів доступу та прав привілеїв
- контроль над адміністративними та службовими акаунтами.
- Ідентифікація критичних даних
- класифікація інформаційних ресурсів, визначення об’єктів з підвищеним ризиком витоку.
- Аналіз наявних політик безпеки
- перевірка актуальності правил доступу, DLP-політик, процедур реагування SOC.
- Огляд логів та журналів подій
- вивчення історичних даних для виявлення аномалій та оцінки ефективності наявних систем моніторингу.

Він дозволяє отримати повне уявлення про інфраструктуру, поточні загрози та рівень контролю, що є основою для коректної оцінки ефективності засобів захисту.

1.3. Визначення критеріїв оцінки

Наступний етап підготовки полягає у встановленні конкретних показників ефективності, на основі яких буде проводитися аудит:

KPI (Key Performance Indicators) – ключові показники ефективності:

- Швидкість та точність виявлення інцидентів (MTTD, Detection Accuracy).
- Покриття бізнес-процесів та критичних даних системами контролю (Policy Coverage, Detection Coverage).
- Час реагування на інциденти та ефективність SOC-процесів (MTTR, Containment Time, Workflow Efficiency) [31].

KRI (Key Risk Indicators) – показники ризику, що дозволяють прогнозувати потенційні внутрішні загрози:

- Аномальна активність користувачів та сутностей.
- Спроби обходу політик безпеки (Policy Bypass Attempts).
- Доступ до критичних даних поза робочим часом або з нетипових пристроїв.
- Соціальні та організаційні фактори ризику (зміна посади, передзвільний період, конфлікти, падіння продуктивності) [32].

2. Етап перевірки технічних засобів

На цьому етапі аудитори здійснюють практичну перевірку ефективності технічних засобів захисту інформації. Мета — оцінити, наскільки наявні системи здатні виявляти, сигналізувати та протидіяти інсайдерським загрозам. Для цього застосовуються як технічні тести, так і аналіз історичних даних та процесів реагування.

2.1. Оцінка DLP-систем

Data Loss Prevention (DLP) — основний інструмент контролю витоку конфіденційної інформації [34]. Під час аудиту перевіряються наступні параметри:

- Precision (точність виявлення) – оцінюється частка коректно ідентифікованих інцидентів серед усіх сповіщень системи. Висока точність зменшує навантаження на аналітиків та запобігає ігноруванню сигналів.
- Recall (повнота виявлення) – показник здатності системи виявляти всі реальні інциденти. Низька повнота свідчить про наявність «сліпих зон».

- Time to Detect (TTD) та Time to Block / Time to Prevent – оцінюється швидкість виявлення та блокування спроб ексфільтрації даних [35].
- Policy Coverage (охоплення політиками) – перевіряється, яка частка бізнес-процесів і типів даних контролюється актуальними DLP-політиками.

2.2. Оцінка SIEM-систем

Security Information and Event Management (SIEM) забезпечує централізований моніторинг та кореляцію подій безпеки. Під час перевірки оцінюються:

- Log Coverage (охоплення логування) – частка систем та підсистем, інтегрованих у SIEM. Низьке охоплення знижує видимість загроз.
- Correlation Rule Accuracy (точність правил кореляції) – якість та релевантність налаштованих правил, оцінюється за метриками Precision та Recall.
- Mean Time to Correlate (MTTC) – час, необхідний для обробки подій та спрацювання кореляційного правила.
- Alert Fatigue – рівень «втоми від сповіщень» аналітиків SOC, який визначає ефективність обробки великого потоку подій.
- Event Volume per Second (EPS) – пропускна здатність системи для запобігання втраті або несвоєчасній обробці подій [36].

2.3. Оцінка UEBA

User and Entity Behavior Analytics (UEBA) дозволяє виявляти аномальні дії користувачів та сутностей. Під час аудиту перевіряються:

- Anomaly Detection Rate (рівень виявлення аномалій)
    - здатність системи ідентифікувати нетипові патерни поведінки.
- Risk Score Reliability (надійність ризикових оцінок)
    - наскільки стабільно та обґрунтовано система присвоює ризикові бали.
- Time to Behavioral Profile Update
    - швидкість оновлення профілів користувачів у динамічному середовищі, що впливає на актуальність аналізу [37].
- Model Accuracy / Drift Resistance

- стійкість моделей до зміни звичайної активності користувачів (data drift).

2.4. Тестування реакції SOC

Security Operations Center (SOC) відповідає за оперативне реагування на інциденти безпеки**.** Під час перевірки оцінюються:

- MTTR (Mean Time to Response / Remediation) – час нейтралізації загрози або відновлення нормальної роботи.
- Containment Time – інтервал між підтвердженням інциденту та обмеженням його впливу.
- Response Workflow Efficiency – ефективність автоматизованих процесів реагування (SOAR) та частка інцидентів, оброблених без участі людини [33].
- Post-Incident Review Completion Rate – доля інцидентів, що пройшли повний аудит та аналіз причин.
- Cost of Response per Incident – економічна ефективність реагування, включаючи витрати на персонал, SOAR, юридичні та репутаційні наслідки [38].

3. Етап оцінки процесів та політик

На цьому етапі аудитори зосереджуються на оцінці організаційних аспектів безпеки**,** перевіряючи відповідність політик, процедур та контролю над доступом до критичних ресурсів. Ефективність технічних засобів безпосередньо залежить від правильності та послідовності реалізації процесів, а також від дисципліни користувачів.

3.1. Перевірка дотримання політик доступу

- Сегментація прав користувачів
  - оцінюється, чи співробітники мають доступ лише до ресурсів, необхідних для виконання своїх обов’язків (принцип найменших привілеїв).
- Контроль доступу до критичних даних
  - перевіряється ефективність DLP та IAM у запобіганні несанкціонованого доступу.

- Актуальність та повнота політик безпеки
    - оцінюється, чи відповідають правила доступу сучасним загрозам та регуляторним вимогам.

3.2. Аналіз процесів інцидент-менеджменту

- Реєстрація інцидентів
    - перевіряється, чи фіксуються всі події, що можуть свідчити про інсайдерську загрозу.
- Класифікація та пріоритезація
    - оцінюється точність визначення критичності інцидентів та типу загрози.
- Ескалація подій
    - перевіряється, наскільки ефективно інциденти передаються на відповідні рівні SOC або керівництва для оперативного реагування.
- Документування та аудит
    - перевіряється наявність журналів, протоколів та звітів для подальшого аналізу та вдосконалення процесів.

3.3. Оцінка внутрішнього контролю над інсайдерськими ризиками

- Моніторинг співробітників групи високого ризику
    - аналізуються дії користувачів із підвищеним ризиком на основі UEBA, історичних даних та поведінкових патернів.
- Контроль виконання політик
    - оцінюється, наскільки співробітники дотримуються встановлених правил і процедур безпеки.
- Виявлення «сліпих зон»
    - визначаються області, де контроль недостатній або відсутній, що може призвести до витоків даних чи несанкціонованого доступу.

4. Використання метрик KPI та KRI

Метрики KPI та KRI є ключовими інструментами оцінки ефективності та прогнозування ризиків під час аудиту засобів протидії інсайдерським загрозам.

Вони дозволяють аудиторам не лише оцінити поточний стан безпеки, але й передбачити потенційні загрози, що можуть виникнути в майбутньому [39].

4.1. KPI (Key Performance Indicators)

KPI дозволяють оцінити поточну ефективність систем захисту, а саме:

- Скорочення часу виявлення та реагування на інциденти**:**
  - MTTD (Mean Time to Detect) – середній час від початку інциденту до його виявлення.
  - MTTR (Mean Time to Response / Remediation) – час, необхідний для нейтралізації загрози або відновлення нормальної роботи системи. Високі показники MTTD та MTTR можуть свідчити про недостатню ефективність SOC або слабке налаштування технічних систем.
- Покриття інсайдерських ризиків системами контролю
  - оцінюється частка співробітників, пристроїв та бізнес-процесів, що контролюються DLP, UEBA та IAM. Недостатнє покриття створює «сліпі зони», де інциденти можуть залишатися непоміченими.
- Завершення розслідувань та класифікація інцидентів
  - оцінюється доля інцидентів, які пройшли повний цикл розслідування та правильно класифіковані за критичністю. Це дозволяє аналізувати якість роботи SOC та ефективність процесів реагування.

4.2. KRI (Key Risk Indicators)

KRI дозволяють прогнозувати потенційні загрози та виявляти ранні сигнали ризику внутрішніх порушень:

- Аномальна активність користувачів
  - різке зростання кількості дій або нетипових дій для певної ролі. Виявлення таких патернів дозволяє заздалегідь реагувати на потенційні інсайдерські загрози.
- Рівень спроб обходу політик (Policy Bypass Attempts)
  - кількість спроб оминання технічних та організаційних засобів контролю. Підвищена активність свідчить про спроби несанкціонованого доступу або порушення політик безпеки.

- Зростання доступу до критичних даних поза робочим часом або з нетипових пристроїв
    - сигналізує про потенційні внутрішні загрози або підготовку до витоку інформації.

4.3. Важливість комплексного використання KPI та KRI

- KPI дозволяють оцінити ефективність наявних систем і процесів у режимі реального часу.
- KRI допомагають виявляти ранні ознаки потенційних загроз, навіть до того, як вони перетворяться на інциденти.
- Разом вони забезпечують комплексний підхід до контролю інсайдерських ризиків**,** дозволяючи аудиторам формувати обґрунтовані рекомендації щодо покращення захисту та мінімізації ризиків.

5. Практичне тестування та аудит

Практичне тестування є критично важливим етапом методики перевірки, оскільки дозволяє не лише оцінити наявність засобів захисту, а й перевірити їхню ефективність у реальних або наближених до реальних сценаріях інсайдерських загроз**.**

5.1. Проведення симуляцій інсайдерських інцидентів

- Моделювання типових сценаріїв загроз:
    - Спроби несанкціонованого доступу до критичних систем або даних.
    - Спроби передачі конфіденційної інформації поза межі організації, включно з електронною поштою, зовнішніми носіями або хмарними сервісами.
    - Зміни привілеїв користувачів або спроби використання адміністративних прав без відповідних повноважень.
- Симуляції дозволяють перевірити швидкість виявлення (MTTD), час реагування (MTTR) та коректність класифікації інцидентів.

5.2. Аналіз логів та сповіщень

- Перевіряється точність та повнота виявлення інцидентів технічними системами: DLP, SIEM, UEBA.

- Оцінюється кількість помилкових спрацювань (False Positive Rate) та пропущених інцидентів (False Negative Rate).
- Аналіз логів дозволяє ідентифікувати сліпі зони, слабкі налаштування кореляційних правил SIEM або неточності у поведінкових моделях UEBA.

5.3. Перевірка операційної відповідності політикам безпеки

- Оцінюється дотримання встановлених правил доступу, сегментація прав користувачів та контроль над критичними даними.
- Перевіряється ефективність процесів SOC, включно з реєстрацією, класифікацією, ескалацією та завершенням розслідувань.
- Проводиться оцінка взаємодії технічних засобів та організаційних процесів, що дозволяє визначити слабкі місця та оптимізувати процедури реагування.

5.4. Результати практичного тестування

- Виявлення реальних проблем та прогалин у системах захисту та процесах.
- Формування рекомендацій щодо підвищення ефективності технічних засобів, політик та процедур.
- Оцінка готовності організації до управління інсайдерськими загрозами у реальних умовах.

6. Формування висновків та рекомендацій

Нарешті на фінальному етапі аудиту здійснюється аналітичне підбиття підсумків перевірки технічних засобів, політик та процесів, а також розробка практичних рекомендацій для підвищення ефективності захисту від інсайдерських загроз.

6.1. Виявлення слабких місць

- Сліпі зони DLP
    - непокриті політиками бізнес-процеси або типи даних, де можливий витік інформації.
- Низька точність правил SIEM
    - надмірні помилкові спрацювання або пропущені інциденти через некоректні кореляційні правила.
- Повільне оновлення профілів UEBA

- зниження актуальності поведінкових моделей у динамічному середовищі та ризик пропуску аномальної активності.

- Недостатня операційна ефективність SOC
  - повільне реагування на інциденти, низький рівень автоматизації, часті помилки у класифікації інцидентів [40].

6.2. Розробка рекомендацій

На основі виявлених проблем формуються конкретні заходи для підвищення ефективності контролю та реагування**:**

- Підвищення охоплення логування та політик DLP
  - розширення об’єктів контролю, актуалізація правил та політик доступу.
- Удосконалення кореляційних правил SIEM
  - оптимізація сценаріїв, підвищення точності та релевантності сповіщень.
- Автоматизація процесів реагування через SOAR
  - зменшення часу реагування, зниження навантаження на аналітиків та підвищення якості виконання процедур.

- Постійне навчання SOC та оновлення поведінкових профілів UEBA
  - підвищення професійного рівня аналітиків, актуалізація моделей для точного виявлення аномалій.

6.3. Підсумкова оцінка

- Формується комплексний висновок про ефективність засобів протидії інсайдерським загрозам, включно з оцінкою технічних систем, політик та процесів.
- Визначаються пріоритетні напрями вдосконалення**,** що дозволяє організації знизити ризики витоку даних, підвищити швидкість реагування та оптимізувати використання ресурсів SOC**.**

Висновок до розділу 3

Було сформуванню, обґрунтуванню та практично реалізовано методики перевірки ефективності засобів протидії інсайдерським загрозам, що поєднує ризикорієнтований підхід, сучасні технічні інструменти та стандартизовані процедури аудиту інформаційної безпеки. Запропонована методика має комплексний характер і охоплює як організаційні, так і технологічні аспекти захисту, що забезпечує можливість всебічної та об’єктивної оцінки здатності організації протистояти внутрішнім загрозам.

У було визначено концепцію та принципи методики, побудовано модель інсайдерських загроз, сформовано чіткі межі аудиту та створено структуровану послідовність етапів, що включають аналіз політик, оцінку технічних засобів (DLP, SIEM, UEBA, PAM), перевірку систем управління доступами, верифікацію журналів безпеки та проведення практичних тестових сценаріїв. Такий підхід дозволяє не лише виявити слабкі місця у налаштуваннях та інтеграції інструментів захисту, а й оцінити їхню реальну ефективність у контексті дій недбалих, зловмисних чи компрометованих інсайдерів.

Була розроблена інтегрована схема взаємодії DLP, UEBA, SIEM та PAM демонструє, що у комплексі ці системи формують багаторівневий механізм виявлення, блокування та аналізу підозрілих дій, забезпечуючи можливість вимірювання ефективності захисту за визначеними KPI та KRI. Значна увага приділена критичному аспекту повноті та якісному стану журналів подій, оскільки саме вони є основою для кореляції, ретроспективного аналізу та розслідування інцидентів.

Особливістю розробленої методики є її відтворюваність та адаптивність: стандартизована структура, чітко визначені критерії, деталізований опис процедур та можливість застосування у різних підрозділах забезпечують сталість результатів, порівнюваність оцінок у часі та зручність інтеграції у регулярні процеси управління інформаційною безпекою.

ВИСНОВКИ

У кваліфікаційній роботі було комплексно проаналізовано теоретичні засади протидії інсайдерським загрозам, сучасні підходи до внутрішнього аудиту інформаційної безпеки та практичні методики оцінювання ефективності систем захисту. Проведений аналіз підтвердив, що інсайдерські загрози становлять одну з найскладніших категорій кіберризиків, оскільки походять від осіб з легітимним доступом до інформаційних активів і глибоким розумінням внутрішніх процесів організації. Різноманітність типів інсайдерів: зловмисних, недбалих і компрометованих, зумовлює багатоваріантність можливих сценаріїв порушень та складність їх виявлення.

Було доведено, що ефективна протидія інсайдерським загрозам вимагає поєднання технологічних, організаційних та процедурних заходів. Було встановлено, що системи DLP, UEBA, SIEM та PAM формують технологічний фундамент багаторівневого контролю: від захисту даних і моніторингу поведінки користувачів до централізованої кореляції подій та управління привілейованими доступами. Разом із тим їх результативність напряму залежить від наявності чітких політик інформаційної безпеки, регламентів доступу, культури безпеки та зрілості процесів реагування на інциденти. Важливе значення у формуванні системного підходу до управління інсайдерськими ризиками мають міжнародні стандарти та фреймворки. Зокрема, стандарти ISO/IEC 27001 і ISO/IEC 27002 задають фундамент для побудови СУІБ, NIST SP 800-53 та Zero Trust пропонують сучасні технічні моделі контролю та перевірки довіри, а CIS Controls орієнтується на практичну реалізацію швидких заходів безпеки. Разом вони забезпечують методологічне підґрунтя для розроблення, впровадження та удосконалення систем протидії інсайдерським загрозам.

У межах кваліфікаційної роботи було здійснено всебічний огляд сучасних методик аудиту інформаційної безпеки — ISO/IEC 27001/27002, NIST SP 800-53, CIS Controls, COBIT 2019, OWASP SAMM, ризик-орієнтованого аудиту та регуляторних моделей. Аналіз показав, що попри значну різноманітність існуючих підходів, не існує універсального рішення, яке однаково ефективно відповідало б

потребам усіх організацій. Основними викликами залишаються відсутність стандартизованих метрик інсайдерських загроз, складність інтерпретації поведінкової аналітики та висока залежність якості аудиту від компетентності фахівців.

Практична частина дослідження була спрямована на формування та обґрунтування комплексної методики оцінювання ефективності засобів протидії інсайдерським загрозам. Розроблена методика поєднує ризик-орієнтований підхід, стандартизовані аудиторські процедури та аналіз технічних засобів (DLP, SIEM, UEBA, PAM). Створена модель інсайдерських загроз, визначені межі аудиту та послідовність перевірок дозволяють оцінювати не лише наявність інструментів, але й реальну ефективність їхнього застосування у сценаріях дій різних типів інсайдерів.

Враховуючи все вище сказане розроблена методика є масштабованою, відтворюваною та здатною до адаптації в різних організаційних середовищах, що забезпечує сталість результатів і можливість інтеграції у регулярні процеси управління інформаційною безпекою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 4 приклади інсайдерських загроз та як їх запобігти | ESKA Блог. ESKA - Провайдер послуг з кібербезпеки та IT рішень. URL: https://eska.global/blog/4-prikladi-insajderskih-zagroz-ta-yak-yih-zapobigti
2. Небезпека ближче, ніж ви думаєте: як компанії захиститися від інсайдерських загроз. ESET. URL: https://www.eset.com/ua/about/newsroom/blog/business-security/nebezpeka-blyzhche-nizh-vy-vvazhayete-yak-kompaniyi-zakhystytsya-vid-insayderskykh-zahroz/?srsltid=AfmBOooUAnxiQL31YRLU3fRLnj0zI4JLnmPmVSz6_CGMkxSkCqZ82Khn
3. Kontrolle und Disziplinen або як позбавитися інсайдерських загроз - IT-Solutions, Україна. IT-Solutions, Україна. URL: https://it-solutions.ua/blog/kontrolle-und-disziplinen-abo-yak-pozbavitisya-insajderskih-zagroz/
4. What Is Cybersecurity? Why It Matters & Core Concepts. Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security
5. ROI4CIO. Обзор решений SIEM (Security information and event management). Хабр. URL: https://habr.com/ru/companies/roi4cio/articles/528770/
6. Звіт про витік даних: Вперше падіння витрат на втрату даних. B2B Cyber Security. URL: https://b2b-cyber-security.de/uk/звіт-про-витік-даних-спочатку-зменшує-витрати-на-втрату-даних/
7. ISO/IEC 27001:2022 ISMS Awareness. Libero Services. URL: https://eshop.liberoservices.org/list-of-seminar/iso-management-systems/awareness/product/iso-iec-27001-2022-isms-awareness?gad_source=1&gad_campaignid=21803307303&gclid=CjwKCAiA0eTJBhBaEiwA-Pa-hduQhDjub2HV0f_VAktptJtYzrhjTb0T1JNrJCBWxAkuHV623D-OFhoCkKIQAvD_BwE
8. Kirvan P., Cole B. What is ISO 27002? | Definition from TechTarget. Search Security. URL: https://www.techtarget.com/searchsecurity/definition/ISO-27002-International-Organization-for-Standardization-27002
9. What is NIST 800-53? | Fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/nist-800-53
10. What Is Zero Trust Architecture? Key Elements and Use Cases. Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
11. What Is Zero Trust?. Coursera. URL: https://www.google.com/aclk?sa=L&ai=DChsSEwjCjMLV97ORAxVW8XkEHd0mI24YACICCAEQARoCd2Y&co=1&gclid=CjwKCAiA0

eTJBhBaEiwA-Pa-hdWyF5YiqoLed3ZGmskluQu6UEFgGFpaHfdCKhJ87arAfZO2zIJsuBoCLvUQAvD_BwE&cce=2&sig=AOD64_194tg_QZkRXtpvq0FBkZOq7a5Xqw&q&adurl&ved=2ahUKEwio4brV97ORAxWVXvEDHdc6HuAQ0Qx6BAgbEAE

12. Про затвердження Інструкції про порядок регулювання діяльності банків в Україні : Постанова Нац. банку України від 28.08.2001 № 368 : станом на 31 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/z0841-01#Text (дата звернення: 10.12.2025).
13. Термін «Внутрішній аудит» // Термінологія законодавства / Законодавство України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/term/4407
14. Atlassian. Collaboration software for software, IT and business teams | Atlassian. URL: https://www.atlassian.com/work-management/project-management/pdca-cycle
15. Rumiantsev I. ИБ по-американски. Часть 1. Что такое NIST 800-53 и как выглядят контроли безопасности?. Хабр. URL: https://habr.com/ru/articles/238245/
16. The 18 CIS Controls. CIS. URL: https://www.cisecurity.org/controls/cis-controls-list
17. COBIT 2019: IT governance framework - ITLawCo. ITLawCo. URL: https://itlawco.com/cobit-2019-it-governance-framework/
18. WASP SAMM | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-samm/
19. Barney N. What is PCI DSS? Requirements and Compliance | TechTarget. Search Security. URL: https://www.techtarget.com/searchsecurity/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard
20. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. SEI Digital Library. URL: https://www.sei.cmu.edu/library/introducing-octave-allegro-improving-the-information-security-risk-assessment-process/
21. Courtemanche M. What is mean time to detect (MTTD)? | Definition from TechTarget. Search IT Operations. URL: https://www.techtarget.com/searchitoperations/definition/mean-time-to-detect-MTTD
22. IBM. What is Mean Time to Repair (MTTR)? | IBM. IBM. URL: https://www.ibm.com/think/topics/mttr
23. Kirvan P., Tucci L. What is a Key Risk Indicator (KRI) and Why is it Important? | Definition from TechTarget. Search CIO. URL: https://www.techtarget.com/searchcio/definition/key-risk-indicator-KRI

24. Gillis A. S., Rosencrance L. What is SIEM (Security Information and Event Management)? | Definition from TechTarget. Search Security. URL: https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM
25. Privileged Access Management (PAM) Demystified. One Identity | Unified Identity Security. URL: https://www.oneidentity.com/what-is-privileged-access-management/
26. OTUS. Что такое управление доступом и как его протестировать?. Хабр. URL: https://habr.com/ru/companies/otus/articles/726846/
27. Довідник з рішень кібербезпеки - H-X Technologies. H-X Technologies. URL: https://www.h-x.technology/ua/security-solutions-full-review-ua
28. СУКУПНІСТЬ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ЗБРОЙНИХ СИЛ УКРАЇНИ | Сучасні інформаційні технології у сфері безпеки та оборони. Сучасні інформаційні технології у сфері безпеки та оборони. URL: https://sit.nuou.org.ua/article/view/212647
29. Системи моніторингу та керування - IT-Solutions, Україна. IT-Solutions, Україна. URL: https://it-solutions.ua/servisi/sistemi-monitoringu-ta-keruvannya/
30. Що таке операційний центр безпеки (SOC)? | Захисний комплекс Microsoft. Your request has been blocked. This could be due to several reasons. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-security-operations-center-soc
31. What is a Key Performance Indicator (KPI)? - KPI.org. KPI.org. URL: https://www.kpi.org/kpi-basics/
32. What are Key Risk Indicators (KRIs) in Enterprise Risk Management (ERM)?. Metricstream. URL: https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm
33. rackWise Digital | Honeywell. Honeywell - The Future Is What We Make It. URL: https://hcenews.honeywell.com/QMS.html?utm_source=google&utm_medium=cpc&utm_campaign=cpc-google-MD-nonbrand-qms-emea-english&utm_content=website&gad_source=1&gad_campaignid=

22803604514&gclid=Cj0KCQiAprLLBhCMARIsAEDhdPcLOeBNO90mo80JmHXgGooU9rRb8YEzKjxeAEpl2ZpcMPX7MAEfGo8aAqJPEALw_wcB

34. What is DLP (Data Loss Prevention)? | Fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/dlp (date of access: 18.01.2026).
35. Cymulate. Mean Time to Detect (MTTD). Cymulate. URL: https://cymulate.com/cybersecurity-glossary/mean-time-to-detect/
36. QRadar: Understanding EPS Average, EPS PEAK, and License Threshold. IBM. URL: https://www.ibm.com/support/pages/qradar-understanding-eps-average-eps-peak-and-license-threshold
37. Scapicchio M., Downie A., Finio M. What Is a Security Operations Center (SOC)? | IBM. IBM. URL: https://www.ibm.com/think/topics/security-operations-center
38. Understanding the Costs of Incident Response: Investigation Costs. MOXFIVE Technical Advisory Services. URL: https://www.moxfive.com/blog/understanding-the-costs-of-incident-response-investigation-costs
39. KRI против KPI: основные различия, которые нужно знать. Блог про HR-аналитику. URL: https://edwvb.blogspot.com/2024/10/kri-kpi.html
40. Контроль кіберризиків: Що це таке і що він охоплює? - Synchron. Synchron. URL: https://synchron.ua/cyber-risk-management-uk/