Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«Допущено до захисту»
Завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття другого (магістерського)
рівня вищої освіти

Спеціальність 125 Кібербезпека та захист інформації

Тема роботи:
ТЕХНОЛОГІЯ ACCESS MANAGEMENT ДЛЯ ЗАХИСУ ВІД КІБЕРЗАГРОЗ

Виконав

студент групи БІКСм-1-25-1.4д

Білан Ярослав Олегович
(прізвище, ім'я, по батькові)

_____
(підпис)

Науковий керівник

Кандидат технічних наук, доцент
(науковий ступінь, наукове звання)

Складанний Павло Миколайович
(прізвище, ініціали)

_____
(підпис)

Київ – 2025

Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

Освітньо-кваліфікаційних рівень – магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітня програма 125.00.01 Безпека інформаційних і комунікаційних систем

«Затверджую»
Завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Білану Ярославу Олеговичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Технологія Access Management для захису від кіберзагроз;
керівник к.т.н., доц. Складанний Павло Миколайович
затверджені наказом ректора від «___»_____ 20___ року №__.
2. Термін подання студентом роботи «___»_____ 20___ р.
3. Вихідні дані до роботи:

3.1 науково-технічна та нормативна література з теми дослідження: науково-технічні праці - 55, ISO/IEC 27001:2022, ISO/IEC 27005:2022, ISO/IEC 22301:2019, NIST SP 800-61 Rev.2, NIST SP 800-207, NIST SP 800-137, Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про інформацію», Постанова КМУ №518 від 19.06.2019;

3.2 методи: системний аналіз, моделювання загроз (STRIDE, MITRE ATT&CK), структурне та функціональне проєктування, ризик-орієнтовані методи оцінювання загроз, експериментальні методи тестування механізмів автентифікації й авторизації;

3.3 технології: SIEM, SOAR, SOC, Zero Trust Architecture, Splunk Enterprise, Wazuh, Elastic Stack, Flask, REST API, Alert Manager, Dashboard Analytics;

3.4 алгоритми: кореляційні правила, евристичні пороги, статистичне виявлення аномалій;

3.5 мова програмування: Python;

3.6 математичні моделі та методи: моделі загроз STRIDE та MITRE ATT&CK, ризик-орієнтовані моделі оцінки загроз, моделі поведінкової аналітики UEBA, Zero Trust-модель контролю доступу, структурні та функціональні моделі Access Management.

4. Зміст текстової частини роботи (перелік питань, які потрібно розробити):

4.1. Проаналізувати теоретичні засади та сучасні підходи до технологій Access Management у сфері кібербезпеки.

4.2. Дослідити актуальні кіберзагрози, пов’язані з управлінням доступом, та визначити їх вплив на інформаційні системи.

4.3. Сформувати модель загроз і визначити вимоги до технології Access Management для забезпечення належного рівня захисту.

4.4. Обґрунтувати та розробити архітектурну модель системи Access Management для корпоративної інформаційної системи.

4.5. Розробити механізми автентифікації, авторизації та контролю доступу з урахуванням сучасних технічних і нормативних вимог.

4.6. Імплементувати елементи технології Access Management та провести їх налаштування у вибраному середовищі.

4.7. Оцінити ефективність запропонованої технології Access Management шляхом тестування, аналізу показників безпеки та порівняння з сучасними підходами.

5. Перелік графічного матеріалу:

5.1 Презентація доповіді, виконана в Microsoft PowerPoint.

5.2 Типові схеми: рисунків - 31.

6. Дата видачі завдання «___»_____ 20__ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1.	Уточнення постановки завдання		
2.	Аналіз літератури		
3.	Обґрунтування вибору рішення		
4.	Збір даних		
5.	Виконання та оформлення розділу 1.		
6.	Виконання та оформлення розділу 2.		
7.	Виконання та оформлення розділу 3.		
8.	Вступ, висновки, реферат		
9.	Апробація роботи на науково-методичному семінарі та/або науково-технічній конференції		
10.	Оформлення та друк текстової частини роботи		
11.	Оформлення презентацій		
12.	Отримання рецензій		
13.	Попередній захист роботи		
14.	Захист в ЕК		

Студент _____ Білан Ярослав Олегович
(підпис) (прізвище, ім’я, по батькові)

Науковий керівник _____ Складанний Павло Миколайович
(підпис) (прізвище, ім’я, по батькові)

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню теоретичних засад, моделей, методів та практичних механізмів управління доступом у сучасних інформаційних системах, а також розробці ефективної технології Access Management, здатної протидіяти актуальним кіберзагрозам, мінімізувати ризики несанкціонованого доступу та забезпечувати цілісність, конфіденційність і доступність критичних інформаційних ресурсів.

Робота складається зі вступу, трьох розділів, що містять 31 рисунків та 12 таблиць, висновків, списку використаних джерел, що містить 58 найменувань. Загальний обсяг роботи становить 115 аркушів, а також додатки, перелік умовних скорочень.

Об'єктом дослідження є процес організації, контролю та регулювання доступу користувачів і сервісів до інформаційних активів підприємства.

Предметом дослідження є моделі, політики та технічні засоби управління доступом, а також їх застосування для протидії несанкціонованому доступу та сучасним кіберзагрозам.

Метою роботи є дослідження, розробка та оцінювання комплексної технології управління доступом, що забезпечує підвищення стійкості інформаційно-комунікаційних систем до кіберзагроз на основі оптимізації політик доступу, сучасних методів автентифікації та інтегрованих механізмів моніторингу.

Для досягнення поставленої мети у роботі: проаналізувати теоретичні засади та сучасні підходи до технологій Access Management у сфері кібербезпеки; дослідити актуальні кіберзагрози, пов'язані з управлінням доступом, та визначити їх вплив на інформаційні системи; сформувати модель загроз і визначити вимоги до технології Access Management для забезпечення належного рівня захисту; обґрунтувати та розробити архітектурну модель системи Access Management для корпоративної інформаційної системи; розробити механізми автентифікації, авторизації та контролю доступу з урахуванням сучасних технічних і нормативних вимог; імплементувати елементи технології Access

Management та провести їх налаштування у вибраному середовищі; оцінити ефективність запропонованої технології Access Management шляхом тестування, аналізу показників безпеки та порівняння з сучасними підходами.

Крім того, у роботі обґрунтовано вибір оптимальної технологічної платформи для впровадження Access Management, з урахуванням архітектурних особливостей, підтримки протоколів автентифікації та авторизації, механізмів безпеки, масштабованості та сумісності з корпоративною інфраструктурою.

Наукова новизна одержаних результатів. Вперше запропоновано комплексну технологію Access Management, орієнтовану на протидію сучасним кіберзагрозам шляхом поєднання адаптивних механізмів автентифікації, гнучких моделей авторизації та інтегрованих засобів моніторингу доступу; уточнено підхід до формування моделі загроз для систем управління доступом з урахуванням векторів атак, характерних для сучасних корпоративних середовищ; удосконалено архітектурну модель системи Access Management, що забезпечує багаторівневий контроль доступу на основі Zero Trust та ризик-орієнтованого аналізу; дістало подальшого розвитку застосування поведінкової аналітики (UEBA) для виявлення аномальних дій користувачів у процесах автентифікації та авторизації; запропоновано авторський підхід до оцінювання ефективності технології Access Management, який включає сукупність показників стійкості, швидкодії та якості виявлення загроз.

Галузь застосування. Результати роботи можуть бути використані у процесі проєктування, модернізації та експлуатації корпоративних інформаційних систем для підвищення рівня їх кіберзахисту. Вони є корисними при впровадженні технологій управління доступом (Access Management) у державних установах, комерційних підприємствах та організаціях, що працюють із критичними інформаційними ресурсами. Одержані результати також можуть застосовуватися під час розроблення політик інформаційної безпеки, систем автентифікації та авторизації, а також при побудові Zero Trust-архітектур. Крім того, напрацьовані підходи можуть бути використані для створення або вдосконалення платформ IAM/PAM. Результати роботи є корисними й у

навчальному процесі закладів вищої освіти під час викладання дисциплін, пов’язаних із кібербезпекою та захистом інформації.

Ключові слова: ACCESS MANAGEMENT, УПРАВЛІННЯ ДОСТУПОМ, АВТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, IAM, PAM, ZERO TRUST, КІБЕРЗАГРОЗИ, МОДЕЛЬ ЗАГРОЗ, КОНТРОЛЬ ДОСТУПУ, MFA, OAUTH 2.0, OPENID CONNECT, МОНІТОРИНГ ДОСТУПУ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AM – Access Management — технологія управління доступом в інформаційних системах

IAM – Identity and Access Management — система управління ідентичностями та доступом

PAM – Configuration Management Database — система управління привілейованим доступом

IdP – Identity Provider — провайдер ідентичності; сервіс, що виконує автентифікацію користувачів

SP – Service Provider — система доменних імен

SSO – Single Sign-On — єдиний вхід, механізм одноразової автентифікації для доступу до кількох сервісів

MFA – Multi-Factor Authentication — багатофакторна автентифікація

2FA – wo-Factor Authentication — двофакторна автентифікація

FIDO2/WebAuthn – стандарти безпарольної автентифікації

OTP – One-Time Password — одноразовий пароль

TOTP – Time-Based One-Time Password — одноразовий пароль на основі часу

RBAC – Role-Based Access Control — модель контролю доступу на основі ролей

ABAC – Attribute-Based Access Control — модель контролю доступу на основі атрибутів

PBAC – Policy-Based Access Control — модель контролю доступу на основі політик

RBA – Risk-Based Authentication — ризик-орієнтована автентифікація

Zero Trust – модель «нульової довіри» для кібербезпеки

ZTNA – Zero Trust Network Access — мережевий доступ у моделі Zero Trust.

OAuth 2.0 – протокол авторизації

OIDC – OpenID Connect — протокол автентифікації на базі OAuth 2.0

SAML – Security Assertion Markup Language — стандарт обміну даними автентифікації між IdP та SP

SIEM – Security Information and Event Management — система управління подіями та інформацією безпеки

SOC – Security Operations Center — центр моніторингу безпеки

UEBA – User and Entity Behavior Analytics — поведінковий аналіз користувачів та сутностей

API – Application Programming Interface — інтерфейс програмування застосунків

HTTPS – захищений протокол передачі гіпертексту

TLS – ransport Layer Security — протокол безпечного транспортного рівня

CIA triad – Confidentiality, Integrity, Availability — триада конфіденційності, цілісності та доступності

ВСТУП

Стрімке зростання кількості кіберзагроз, спрямованих на компрометацію облікових записів, несанкціоноване отримання доступу до інформаційних ресурсів та використання привілейованих прав, визначає управління доступом як один із ключових елементів систем кібербезпеки сучасних підприємств. Значна частина успішних атак починається саме з порушення механізмів автентифікації або авторизації, зловживання привілеями, атак на сесії доступу або викрадення облікових даних. У цих умовах традиційні підходи до контролю доступу, що базуються на статичних правилах або ролях, дедалі частіше виявляються недостатньо ефективними через складність, динамічність та мультивекторність сучасних кіберзагроз.

Проблема посилюється тим, що корпоративні інформаційні системи стають розподіленими, інтегрують хмарні сервіси, мобільні додатки та сторонні платформи, що збільшує площину атаки та кількість точок доступу. Відсутність комплексної технології Access Management, здатної забезпечити багаторівневу перевірку користувача, аналіз контексту доступу, динамічну авторизацію та моніторинг поведінки, створює передумови для успішної реалізації атак на критично важливі інформаційні активи.

Таким чином, постає науково-практична задача розроблення технології Access Management, яка дозволяє підвищити стійкість інформаційних систем до сучасних кіберзагроз, забезпечує контроль і регламентацію доступу на основі сучасних моделей і стандартів, а також забезпечує можливість адаптивного реагування на аномалії та неправомірні дії в режимі реального часу.

Актуальність роботи полягає в тому, що сучасні інформаційні системи функціонують у середовищі постійно зростаючих кіберзагроз, значна частина яких спрямована на компрометацію механізмів автентифікації, викрадення облікових даних, отримання несанкціонованого доступу та зловживання привілейованими правами. У таких умовах традиційні системи контролю доступу вже не забезпечують належного рівня захисту, оскільки не враховують

динамічність атак, багатовекторність засобів проникнення та необхідність контекстного аналізу поведінки користувачів. Це зумовлює потребу у впровадженні сучасних технологій Access Management, які поєднують адаптивну автентифікацію, гнучкі політики авторизації, інструменти моніторингу доступу та модель Zero Trust для підвищення стійкості інформаційних систем до кібератак.

Метою роботи є дослідження, розробка та оцінювання комплексної технології управління доступом, що забезпечує підвищення стійкості інформаційно-комунікаційних систем до кіберзагроз на основі оптимізації політик доступу, сучасних методів автентифікації та інтегрованих механізмів моніторингу.

Для досягнення поставленої мети були поставлені та вирішенні такі **завдання**:

1. Проаналізувати теоретичні засади та сучасні підходи до технологій Access Management у сфері кібербезпеки.

2. Дослідити актуальні кіберзагрози, пов’язані з управлінням доступом, та визначити їх вплив на інформаційні системи.

3. Сформувати модель загроз і визначити вимоги до технології Access Management для забезпечення належного рівня захисту.

4. Обґрунтувати та розробити архітектурну модель системи Access Management для корпоративної інформаційної системи.

5. Розробити механізми автентифікації, авторизації та контролю доступу з урахуванням сучасних технічних і нормативних вимог.

6. Імплементувати елементи технології Access Management та провести їх налаштування у вибраному середовищі.

7. Оцінити ефективність запропонованої технології Access Management шляхом тестування, аналізу показників безпеки та порівняння з сучасними підходами.

Об’єктом дослідження є процес організації, контролю та регулювання доступу користувачів і сервісів до інформаційних активів підприємства.

Предметом дослідження є моделі, політики та технічні засоби управління доступом, а також їх застосування для протидії несанкціонованому доступу та сучасним кіберзагрозам.

Методи дослідження. Для вирішення означених вище наукових завдань в роботі використано методи системного аналізу, моделювання загроз (STRIDE, MITRE ATT&CK), структурного та функціонального проєктування, ризик-орієнтовані методи оцінювання загроз, а також експериментальні методи тестування механізмів автентифікації й авторизації.

Наукова новизна одержаних результатів. Вперше запропоновано комплексну технологію Access Management, орієнтовану на протидію сучасним кіберзагрозам шляхом поєднання адаптивних механізмів автентифікації, гнучких моделей авторизації та інтегрованих засобів моніторингу доступу; уточнено підхід до формування моделі загроз для систем управління доступом з урахуванням векторів атак, характерних для сучасних корпоративних середовищ; удосконалено архітектурну модель системи Access Management, що забезпечує багаторівневий контроль доступу на основі Zero Trust та ризик-орієнтованого аналізу; дістало подальшого розвитку застосування поведінкової аналітики (UEBA) для виявлення аномальних дій користувачів у процесах автентифікації та авторизації; запропоновано авторський підхід до оцінювання ефективності технології Access Management, який включає сукупність показників стійкості, швидкодії та якості виявлення загроз.

Зв’язок роботи з науковими програмами, планами, темами. Робота узгоджується з напрямами державних і галузевих програм у сфері кібербезпеки, цифрової трансформації та захисту інформації, зокрема із завданнями розвитку національної системи кіберзахисту, підвищення стійкості інформаційно-комунікаційних систем та впровадження сучасних механізмів управління доступом. Дослідження відповідає стратегічним орієнтирам України щодо впровадження концепції Zero Trust, удосконалення систем автентифікації та авторизації, а також гармонізації підходів кіберзахисту з міжнародними стандартами NIST та ISO/IEC. Отримані результати спрямовані на підвищення

рівня захисту інформаційних систем за рахунок впровадження сучасних механізмів управління доступом, удосконалення процесів автентифікації та авторизації, зменшення ризиків несанкціонованого доступу та забезпечення стійкості до сучасних кіберзагроз. Кваліфікаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№0122U200483, КУБГ, м. Київ).

Теоретичне та практичне значення. Нові наукові результати, отримані в роботі, мають важливе теоретичне та практичне значення для розвитку сучасних підходів до управління доступом, удосконалення моделей автентифікації та авторизації, а також формування ефективних механізмів протидії кіберзагрозам у корпоративних інформаційних системах. Запропоновані рішення можуть бути використані при розробленні політик інформаційної безпеки, впровадженні систем Access Management у підприємствах різних сфер діяльності, проєктуванні Zero Trust-архітектур та створенні комплексних IAM/PAM-рішень. Теоретичні напрацювання роботи можуть слугувати основою для подальших наукових досліджень у галузі кібербезпеки, а практичні результати — бути впроваджені у реальні інформаційні системи з метою підвищення рівня їх захищеності.

Галузь застосування. Результати роботи можуть бути використані у процесі проєктування, модернізації та експлуатації корпоративних інформаційних систем для підвищення рівня їх кіберзахисту. Вони є корисними при впровадженні технологій управління доступом (Access Management) у державних установах, комерційних підприємствах та організаціях, що працюють із критичними інформаційними ресурсами. Одержані результати також можуть застосовуватися під час розроблення політик інформаційної безпеки, систем автентифікації та авторизації, а також при побудові Zero Trust-архітектур. Крім того, напрацьовані підходи можуть бути використані для створення або вдосконалення платформ IAM/PAM. Результати роботи є корисними й у

навчальному процесі закладів вищої освіти під час викладання дисциплін, пов’язаних із кібербезпекою та захистом інформації.

Розділ 1. ТЕОРЕТИЧНІ ОСНОВИ ТЕХНОЛОГІЙ ACCESS MANAGEMENT ТА ЇХ РОЛЬ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

Технології Access Management є фундаментальною складовою систем кібербезпеки, оскільки вони регламентують взаємодію користувачів і сервісів з інформаційними ресурсами підприємства [1-2]. Основними елементами Access Management виступають ідентифікація, автентифікація та авторизація, які визначають, хто отримує доступ, як підтверджує особу та які дії може виконувати в системі [2, 8]. Сучасні моделі управління доступом базуються на ролях (RBAC), атрибутах (ABAC), політиках (PBAC) та ризик-орієнтованих механізмах, що дають змогу гнучко контролювати привілеї й запобігати несанкціонованому доступу [5-6]. Розвиток хмарних технологій, віддаленої роботи та інтеграції різнорідних сервісів потребує використання сучасних інструментів Access Management, які підтримують багатофакторну автентифікацію, протоколи OAuth 2.0 і OpenID Connect, а також концепцію Zero Trust із постійною перевіркою ідентичності та контексту доступу [11, 13]. У таких умовах управління доступом відіграє важливу роль у протидії сучасним кіберзагрозам, зокрема компрометації облікових записів, зловживанню привілеями, атакам на сесії та викраденню токенів [3, 9]. Таким чином, Access Management виступає не лише технічним механізмом контролю, а й стратегічним елементом формування стійких і захищених інформаційних систем, що забезпечують конфіденційність, цілісність і доступність критично важливих даних в умовах динамічних кіберзагроз.

1.1. Концептуальні засади управління доступом та їх роль у забезпеченні кібербезпеки

Управління доступом є однією з базових складових системи кібербезпеки, оскільки саме через механізми доступу здійснюється взаємодія користувачів, сервісів та інформаційних ресурсів підприємства [7, 21, 23, 56]. Концепція управління доступом передбачає комплекс організаційних і технічних заходів,

спрямованих на забезпечення того, щоб доступ до інформації отримували лише ті суб’єкти, які мають на це законні повноваження [22]. Це забезпечує дотримання основних принципів інформаційної безпеки — конфіденційності, цілісності та доступності.

Основу управління доступом становлять три ключові процеси: ідентифікація, автентифікація та авторизація (рис. 1.1). Ідентифікація дозволяє встановити, хто саме звертається до системи; автентифікація — перевірити справжність цієї особи; авторизація — визначити, які дії та ресурси доступні користувачу після підтвердження особи [14, 21, 57]. Узгоджена робота цих процесів формує основу безпечної взаємодії в сучасних корпоративних інформаційних системах.

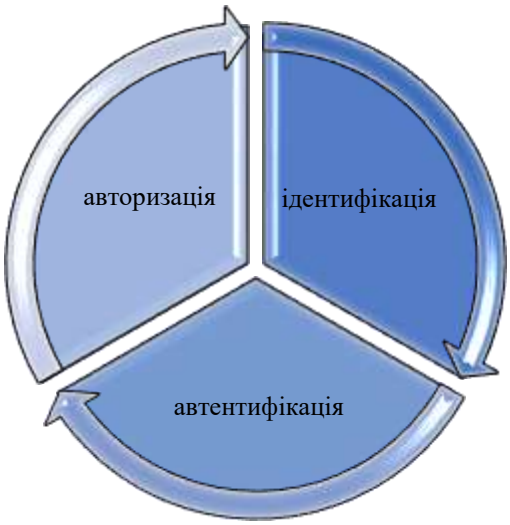

Рис. 1.1. Базові компоненти управління доступом: ідентифікація, автентифікація та авторизація

Важливою концептуальною засадою управління доступом є принцип мінімальних привілеїв, який передбачає надання користувачам рівня доступу, достатнього лише для виконання їхніх службових обов’язків [5-6, 8, 21]. Це значно зменшує ризики несанкціонованих дій, зловживання доступом та ескалації привілеїв [10]. Іншим фундаментальним принципом є необхідність розмежування доступу, що реалізується через диференціацію ролей, груп і прав у системі.

Сучасні інформаційні системи функціонують у середовищі високої динамічності кіберзагроз, що вимагає переходу від статичних моделей доступу до гнучких, адаптивних та контекстно залежних підходів [11, 19]. У цьому контексті особливого значення набуває концепція Zero Trust, яка ґрунтується на припущенні, що жоден користувач чи пристрій не може вважатися безпечним за замовчуванням [13, 47-48, 54-55]. Модель Zero Trust передбачає постійний аналіз контексту доступу, повторну автентифікацію, перевірку поведінкових характеристик та оцінку ризиків у режимі реального часу.

Рис. 1.2 відображає логічну взаємодію між концепцією Zero Trust та технологією Access Management. Модель Zero Trust ґрунтується на відсутності довіри за замовчуванням, перевірці кожного запиту та застосуванні принципу мінімальних привілеїв. На цій основі Access Management реалізує ключові процеси — ідентифікацію, автентифікацію, авторизацію та контроль доступу, що забезпечує комплексний захист інформаційних ресурсів підприємства.

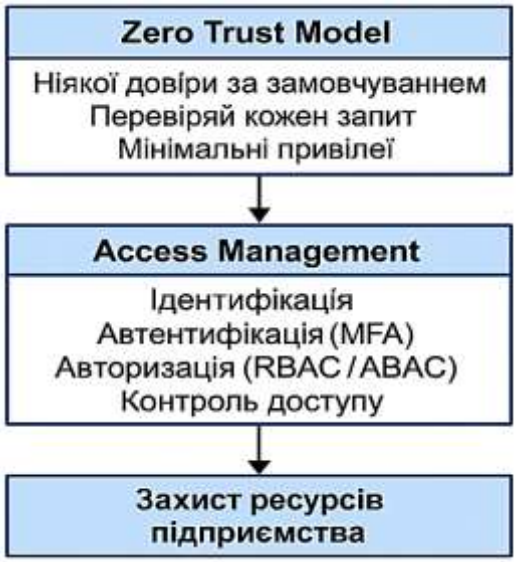

Рис. 1.2. Принцип Zero Trust у контексті технології Access Management

Застосування сучасних моделей управління доступом, таких як RBAC, ABAC чи PBAC, дозволяє створити гнучкі системи регулювання прав користувачів, що адаптуються до змін бізнес-процесів і загрозового середовища [19, 26, 32]. Крім того, управління доступом відіграє важливу роль у запобіганні таким поширеним загрозам, як викрадення облікових даних, несанкціонований

доступ, компрометація привілейованих облікових записів, атаки на сесії та внутрішні порушення з боку інсайдерів.

Таким чином, концептуальні засади управління доступом визначають основу побудови ефективної системи кіберзахисту. Правильно організовані процеси ідентифікації, автентифікації, авторизації, розмежування привілеїв та моніторингу подій доступу забезпечують контроль над використанням інформаційних ресурсів і є ключовим чинником захисту корпоративної інфраструктури від сучасних кіберзагроз.

1.2. Моделі контролю доступу: порівняльна характеристика і сфери застосування

Контроль доступу є ключовим компонентом системи кібербезпеки, оскільки забезпечує регламентацію прав користувачів щодо взаємодії з інформаційними ресурсами [21, 23]. Ефективність управління доступом значною мірою визначається вибором відповідної моделі контролю, яка має узгоджуватися зі специфікою бізнес-процесів, типом інформаційних активів та загрозовим середовищем [5, 22]. Сучасні системи безпеки використовують різноманітні моделі, серед яких найбільш поширеними є MAC, DAC, RBAC, ABAC та PBAC.

Рис. 1.3 відображає послідовну еволюцію моделей контролю доступу — від жорстких централізованих механізмів MAC до гнучких динамічних підходів ABAC і політик-орієнтованої моделі PBAC. Така схема демонструє зростання рівня гнучкості, адаптивності та контекстної залежності рішень з управління доступом, що відповідає сучасним вимогам кібербезпеки та концепції Zero Trust.

Рис. 1.3. Еволюція моделей контролю доступу в інформаційних системах

Модель MAC (Mandatory Access Control) передбачає централізоване визначення політики доступу адміністраторами системи та є найбільш суворою [7, 21]. Користувачі не можуть змінювати права доступу, а ресурси класифікуються за рівнями секретності. MAC застосовується у військових, урядових, фінансових та інших середовищах, де критично важливо виключити можливість несанкціонованої зміни політик доступу. Її перевагою є високий рівень контролю, а недоліком — низька гнучкість і складність масштабування.

Модель DAC (Discretionary Access Control) ґрунтується на наданні власнику ресурсу права визначати, хто має доступ до його даних [7-8, 23]. DAC є більш гнучкою та простою у впровадженні, однак уразлива до атак типу „маскарад“ або перенесення шкідливих дозволів. DAC доцільно застосовувати в офісних середовищах, системах спільної роботи, невеликих підприємствах та середовищах із невисокими вимогами до секретності даних.

Однією з найбільш поширених у корпоративних системах є модель RBAC (Role-Based Access Control), де доступ визначається рольовою структурою підприємства [5, 8]. Користувач отримує доступ не безпосередньо, а через призначення ролі, яка відповідає його службовим обов’язкам. Перевагами RBAC є масштабованість, простота адміністрування та можливість застосування принципу мінімальних привілеїв. RBAC ефективно працює у великих організаціях з чітко визначеною ієрархією.

Більш сучасним підходом є ABAC (Attribute-Based Access Control) — модель контролю доступу на основі атрибутів користувача, ресурсу, дії та контексту (час, місцезнаходження, рівень ризику) [11, 15]. За рахунок гнучкості ABAC дозволяє реалізувати динамічні політики доступу, що адаптуються до умов середовища [13, 19]. Її активно застосовують у хмарних середовищах, мобільних системах, мультисервісних екосистемах та Zero Trust-архітектурах.

Модель PBAC (Policy-Based Access Control) робить акцент на централізованому управлінні політиками доступу, які визначаються у вигляді правил, що виконуються PDP-компонентом (Policy Decision Point) [24, 52-53]. PBAC часто інтегрується з ABAC і використовується у комплексних

розподілених системах, де необхідно формалізувати політики відповідно до нормативних вимог, наприклад, у фінансовому секторі, державному управлінні та критичній інфраструктурі.

Порівняння моделей контролю доступу свідчить, що кожна з них має свої переваги та обмеження і застосовується залежно від рівня ризику, структури підприємства, потреб у масштабованості та вимог до швидкості прийняття рішень (табл. 1.1) [10-11, 55]. У сучасних умовах найбільш ефективними є комбіновані моделі, які поєднують гнучкість ABAC, структурованість RBAC і контекстну адаптивність PBAC, що дозволяє підтримувати як традиційні, так і Zero Trust-парадигми.

Таблиця 1.1

Порівняльна характеристика моделей контролю доступу

Модель	**Основний принцип**	**Хто визначає доступ**	**Переваги**	**Недоліки**	**Типові сфери застосування**
MAC (Mandatory Access Control)	Доступ ґрунтується на рівнях секретності та жорстких політиках	Адміністратор, централізована політика	Найвищий рівень безпеки; неможливість зміни прав користувачами	Низька гнучкість; складність адміністрування	Військові системи, державні органи, критична інфраструктура
DAC (Discretionary Access Control)	Власник ресурсу сам визначає, хто може отримати доступ	Власник ресурсу	Простота впровадження; висока гнучкість	Низька стійкість до внутрішніх загроз; ризик зловживань	Офісні системи, корпоративні файлові сервіси, невеликі компанії
RBAC (Role-Based Access Control)	Доступ визначається ролями, пов’язаними зі службовими функціями	Адміністратор ролей	Масштабованість; зручне адміністрування; принцип мінімальних привілеїв	Недостатня гнучкість у складних умовах; залежність від ролей	Великі підприємства, ERP/CRM системи, фінансовий сектор
ABAC (Attribute-Based Access Control)	Рішення приймаються на основі атрибутів користувача, ресурсу та контексту	Система на основі правил та атрибутів	Максимальна гнучкість; підтримка динамічних політик	Висока складність реалізації; потреба в точному визначенні атрибутів	Хмарні сервіси, Zero Trust, мобільні та розподілені системи

PBAC (Policy-Based Access Control)	Доступ керується централізованими політиками, що описують поведінку системи	Адміністратор політик (PDP/PEP	Висока формалізованість; контроль відповідності стандартам	Необхідність складної структури політик; залежність від PDP	Державний сектор, фінансові установи, системи з нормативними вимогами

Таким чином, правильний вибір моделі контролю доступу є критичним для побудови стійкої системи інформаційної безпеки. Він визначає не лише рівень захисту інформаційних ресурсів, але й можливість динамічного реагування на зміну кіберзагроз та підтримку безпечної цифрової трансформації підприємства.

1.3. Identity & Access Management (IAM) як ключовий компонент корпоративної безпеки

Identity & Access Management (IAM) є одним із ключових компонентів корпоративної безпеки, оскільки забезпечує цілісну систему керування цифровими ідентичностями користувачів і контролю доступу до ресурсів підприємства [7, 21-23]. В умовах цифрової трансформації, коли корпоративні інфраструктури поєднують локальні сервери, хмарні середовища, мобільні пристрої та SaaS-платформи, IAM формує єдину точку управління доступами та визначає, хто саме, коли і на яких умовах може взаємодіяти з інформаційними активами [2, 11, 13, 15]. Центральним елементом IAM є цифрова ідентичність, яка описує користувача через структурований набір атрибутів — облікові дані, рольову інформацію, криптографічні ключі, механізми автентифікації та історію активності. Саме ця ідентичність лежить в основі прийняття рішень щодо доступу та забезпечує узгодженість політик у всій інформаційній системі.

IAM охоплює процеси створення, модифікації та видалення облікових записів, автентифікацію користувачів, перевірку їх прав доступу, аудит операцій і моніторинг аномальної поведінки [8]. Сучасні системи IAM підтримують багатофакторну автентифікацію, ризик-орієнтовані механізми перевірки,

passwordless-доступ, єдиний вхід (SSO) та централізоване управління привілейованими акаунтами [13, 17]. Завдяки цьому зменшується ризик компрометації облікових даних — однієї з найбільш поширених причин кіберінцидентів [9]. Водночас IAM забезпечує керування ролями та атрибутами користувачів через RBAC-, ABAC- та PBAC-політики, що дозволяє враховувати контекст, рівень ризику, місцезнаходження, тип пристрою та інші параметри під час ухвалення рішення про надання доступу.

Завдяки своїм можливостям IAM відіграє стратегічну роль у запобіганні кіберзагрозам. Він мінімізує внутрішні ризики шляхом контролю за привілейованими користувачами, автоматично відкликає доступи під час звільнення чи зміни ролі працівника, фіксує всі критичні дії та забезпечує прозорість у взаємодії з інформаційними ресурсами. У контексті сучасних кіберзагроз IAM є фундаментальним елементом Zero Trust-архітектури, що ґрунтується на принципах «ніколи не довіряй, завжди перевіряй» та «мінімальні привілеї» [47, 52, 54]. IAM дозволяє постійно оцінювати ризики кожного запиту, підтверджувати ідентичність користувача на всіх етапах доступу та забезпечувати мікросегментацію корпоративної інфраструктури.

Крім того, IAM суттєво підвищує відповідність підприємства вимогам міжнародних стандартів кібербезпеки, таких як ISO/IEC 27001, NIST SP 800-207, GDPR та DORA [49-50]. Його впровадження сприяє зниженню операційних витрат через автоматизацію управління доступами, підвищує зручність роботи користувачів завдяки SSO та безпарольним методам, а також покращує загальну керованість системи безпеки [18, 20, 29-31]. Завдяки інтеграції з SIEM, SOAR, DLP, CRM, ERP і хмарними сервісами IAM стає центральним елементом корпоративної архітектури безпеки, забезпечуючи безперервність контролю, прозорість аудитів і захист інформаційних ресурсів на всіх рівнях.

У результаті підприємство отримує можливість формалізовано підтверджувати відповідність вимогам регуляторів і аудиторів, скорочуючи час на підготовку звітності та проходження перевірок [49, 50]. Централізоване ведення журналів доступу та стандартизовані процеси авторизації спрощують

аналіз інцидентів і форензіку, підвищуючи рівень довіри до системи інформаційної безпеки з боку стейкхолдерів [18, 20, 29–31]. У поєднанні з Zero Trust-підходом зрілий IAM-процес стає основою для побудови адаптивної, масштабованої та орієнтованої на ризики моделі кіберзахисту підприємства.

Рис. 1.4 демонструє узагальнену архітектуру системи Identity & Access Management, що включає основні компоненти управління доступом: ідентифікацію, автентифікацію, авторизацію та моніторинг доступу. Схема відображає взаємодію користувачів з IAM-платформою, яка забезпечує централізований контроль доступу до корпоративних ресурсів і підтримує політики безпеки підприємства [11, 22-23]. Така архітектура використовується в сучасних системах кіберзахисту для побудови цілісного та керованого середовища безпеки.

Рис. 1.4. Архітектурна схема системи Identity & Access Management (IAM)

Табл. 1.2 узагальнює ключові функції систем Identity & Access Management та демонструє їхній внесок у формування комплексної моделі кіберзахисту підприємства. Представлені функції охоплюють увесь цикл роботи з цифровими ідентичностями — від створення та автентифікації користувачів до авторизації, управління привілейованими доступами та моніторингу активності. Їх реалізація дозволяє мінімізувати ризики компрометації облікових даних, запобігати ескалації привілеїв, контролювати доступи в реальному часі та забезпечувати відповідність міжнародним стандартам безпеки [19, 21, 49-50]. У сукупності ці

функції формують фундамент сучасної системи Access Management та є критично важливими для протидії внутрішнім і зовнішнім кіберзагрозам.

Таблиця 1.2

Функції IAM та їх значення для забезпечення кібербезпеки

Функція IAM	**Опис**	**Значення для кібербезпеки**
Ідентифікація	Визначення унікальної цифрової ідентичності користувача або сервісу за допомогою ідентифікаторів (логін, ID, сертифікат).	Забезпечує точне співвіднесення дій з конкретним суб'єктом, усуває анонімність у системі.
Автентифікація	Підтвердження особи за допомогою паролів, MFA, біометрії або криптографічних ключів.	Знижує ризик компрометації облікових записів, блокує несанкціонований доступ.
Авторизація	Надання дозволів відповідно до ролі, атрибутів або політик доступу (RBAC, ABAC, PBAC).	Запобігає ескалації привілеїв, забезпечує принцип мінімальних прав.
Управління життєвим циклом облікових записів	Створення, модифікація та деактивація облікових записів під час найму, зміни ролі чи звільнення.	Захищає від «мертвих» облікових записів і зловживань доступами.
Управління привілейованими доступами (PAM)	Контроль над адміністраторськими та критичними правами, сесійний моніторинг, записи дій.	Мінімізує внутрішні загрози, запобігає шкідливим або помилковим діям адміністраторів.
Single Sign-On (SSO)	Єдиний вхід до всіх ресурсів після успішної автентифікації.	Знижує ризик слабких паролів і фішингу, покращує контроль доступів.
Federated Identity / OAuth 2.0 / OpenID Connect	Делегована автентифікація та авторизація між різними сервісами й доменами.	Забезпечує безпечну взаємодію з хмарними платформами, усуває дублювання облікових даних.
Моніторинг та аудит доступів	Журналювання дій, аналіз аномалій, виявлення підозрілої активності.	Забезпечує оперативне виявлення загроз і відповідність стандартам (ISO, NIST, GDPR, DORA).
Контроль політик доступу	Встановлення та автоматизоване застосування політик безпеки для різних категорій ресурсів.	Підтримує відповідність нормативним вимогам і забезпечує передбачуваність поведінки системи.
Інтеграція з SIEM / SOAR	Передавання логів та подій у системи моніторингу й автоматизованого реагування.	Підвищує швидкість реагування на інциденти та ефективність аналітики безпеки.

Рис. 1.5 відображає основні етапи життєвого циклу доступу в системах Identity & Access Management: надання доступу, перевірку та авторизацію, моніторинг активності користувачів та скасування доступу. Така циклічна модель демонструє безперервність процесів контролю доступу та важливість

регулярного перегляду прав відповідно до ролі, поведінки та ризикового профілю користувача. Життєвий цикл забезпечує дотримання принципів безпеки, мінімальних привілеїв і своєчасне відкликання зайвих доступів.

Рис. 1.5. Життєвий цикл управління доступом у системі IAM

Access Management є центральним компонентом корпоративної кібербезпеки, оскільки забезпечує керування процесами ідентифікації, автентифікації та авторизації користувачів у межах інформаційних систем підприємства. На відміну від широкого поняття Identity & Access Management (IAM), яке включає весь життєвий цикл цифрової ідентичності, Access Management фокусується на безпосередньому контролі того, хто, коли і за яких умов отримує доступ до ресурсів [6, 9, 11]. Саме цей елемент визначає ефективність захисту критичних даних та стійкість підприємства до ініціації несанкціонованих операцій.

У сучасних інформаційних середовищах Access Management забезпечує перевірку ідентичності користувача, застосування багатофакторної автентифікації (MFA), аналіз контексту доступу та виконання політик авторизації, зокрема на основі RBAC-, ABAC- та PBAC-моделей [10-12, 21]. Це дозволяє контролювати привілеї, мінімізувати ризики компрометації облікових записів, запобігати ескалації прав і захищати системи від внутрішніх та зовнішніх загроз [23]. Впровадження протоколів OAuth 2.0, OpenID Connect, SAML 2.0 та використання токеноїдентифікації забезпечують надійну взаємодію між застосунками, сервісами й хмарними платформами.

Access Management відіграє особливо важливу роль у контексті розподілених систем, хмарних сервісів та віддаленого доступу, де доступні ресурси та точки входу не є статичними. Саме тому сучасні підходи передбачають ризик-орієнтоване прийняття рішень — кожен запит на доступ оцінюється з урахуванням чинників ризику, поведінки користувача, місця розташування, часу та стану пристрою [52-55]. Такий підхід є фундаментом концепції Zero Trust, де жоден користувач чи система не вважається довіреною за замовчуванням, а авторизація відбувається на кожному кроці взаємодії.

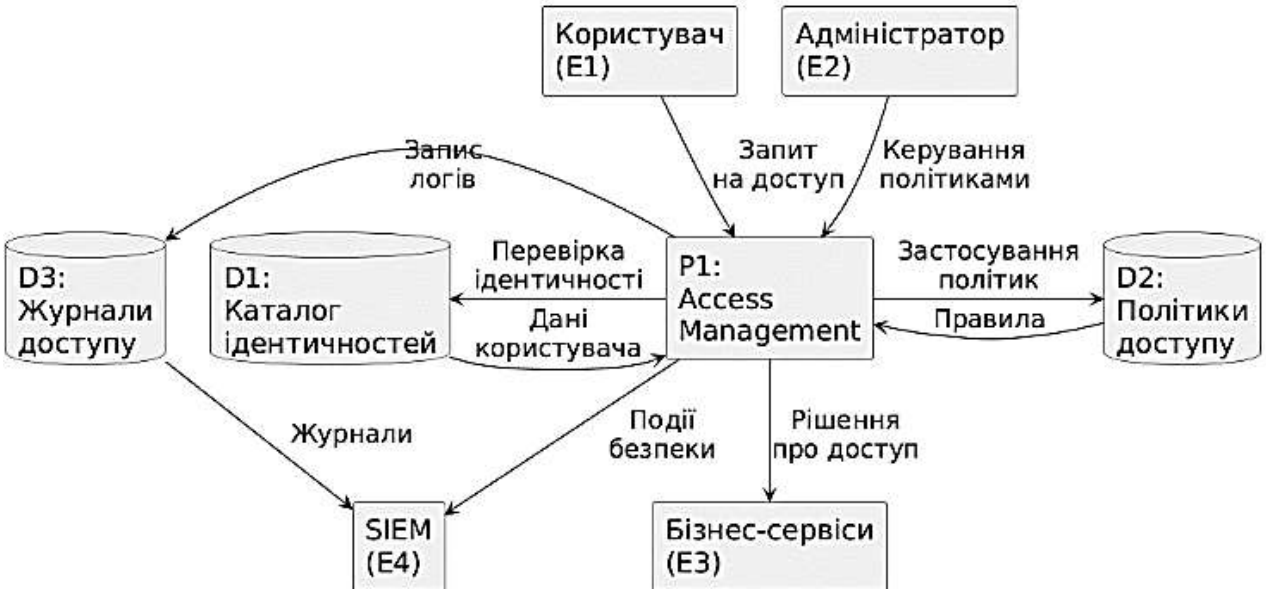

Рис. 1.6. DFD-модель процесу Access Management

Модель на рис. 1.6 відображає ключові компоненти та потоки даних у процесі Access Management. Центральний процес виконує перевірку ідентичності, застосування політик доступу та прийняття рішень щодо авторизації. Модель демонструє взаємодію користувача, адміністратора, бізнес-сервісів та системи моніторингу із сховищами ідентичностей, політик і журналів подій [18, 20, 24]. Така структура показує логіку управління доступами на високому рівні та забезпечує розуміння основних потоків інформації в системі.

Системи Access Management не лише блокують несанкціоновані дії, але й забезпечують прозорість та відтворюваність процесів через аудит, журналювання доступів, моніторинг аномалій та інтеграцію з SIEM/SOAR-

рішеннями. Це дозволяє підприємствам оперативно реагувати на інциденти, виявляти ризикову поведінку та забезпечувати дотримання стандартів безпеки — ISO/IEC 27001, NIST SP 800-53, NIST SP 800-207, GDPR та DORA.

Табл. 1.3 узагальнює ключові відмінності між моделями RBAC, ABAC і PBAC. RBAC забезпечує просте та масштабоване управління ролями, ABAC — високу гнучкість за рахунок використання атрибутів і контексту, а PBAC — централізоване застосування політик, що відповідають складним та регульованим сценаріям доступу. Вибір моделі визначається потребами інфраструктури й рівнем безпеки, тоді як у практичних системах найчастіше використовують комбінований підхід.

Таблиця 1.3

Порівняння моделей RBAC, ABAC та PBAC

Критерій	**RBAC (Role-Based Access Control)**	**ABAC (Attribute-Based Access Control)**	**PBAC (Policy-Based Access Control)**
Основний принцип	Доступ визначається ролями користувачів	Доступ визначається атрибутами (користувача, ресурсу, дії, контексту)	Доступ визначається формалізованими політиками, що виконуються PDP
Опис політик	Ролі → дозволи; користувачі прив’язуються до ролей	Правила «якщо-умови-то-доступ» на основі набору атрибутів	Політики у вигляді правил, сценаріїв, нормативних вимог
Гнучкість	Середня; добре працює при стабільних ролях	Висока; підтримує динамічні сценарії та контекст	Висока; особливо для складних, регульованих середовищ
Масштабованість	Висока для великих організацій з чіткою структурою	Висока, але потребує якісного управління атрибутами	Висока, за умови централізованого керування політиками
Контекстність (час, місце, ризик)	Обмежена	Повна підтримка контексту	Повна, з можливістю складних політик на основі контексту
Відповідність Zero Trust	Часткова (через принцип мінімальних привілеїв)	Висока (контекст + атрибути)	Висока (політики Zero Trust на рівні PDP/PEP)
Типові сценарії застосування	Класичні корпоративні системи,	Хмарні сервіси, мобільні та розподілені	Державний сектор, фінанси, критична інфраструктура,

	ERP/CRM, чітка ієрархія	системи, мікросервіси	системи з жорсткими нормативними вимогами

Таким чином, Access Management є не просто технічним засобом, а стратегічним механізмом формування безпечного середовища підприємства, який поєднує політики доступу, механізми захисту, нормативні вимоги та сучасні технології. Він забезпечує цілісну, масштабовану та адаптивну модель контролю взаємодії користувачів із ресурсами, що є критично важливим у протидії сучасним кіберзагрозам та побудові стійкої архітектури безпеки.

1.4. Privileged Access Management (PAM) та захист привілейованих облікових записів

Привілейовані облікові записи є одними з найкритичніших елементів корпоративної інформаційної системи, оскільки вони забезпечують високий або повний рівень доступу до ресурсів, інфраструктури та конфіденційних даних. Компрометація таких облікових записів має значно серйозніші наслідки, ніж звичайні кібератаки, адже зловмисник, отримавши привілейований доступ, може змінювати конфігурації, обходити механізми безпеки, видаляти або викрадати дані, а також приховувати власну присутність у системі [6]. Саме тому управління привілейованими доступами (Privileged Access Management, PAM) є одним із ключових компонентів сучасної стратегії інформаційної безпеки підприємства.

PAM орієнтується на контроль, моніторинг та обмеження доступу користувачів, адміністраторів та сервісів, яким надаються розширені права. До таких суб’єктів належать системні адміністратори, адміністратори баз даних, DevOps-інженери, облікові записи сервісів, роботизовані процеси та інші сутності, що виконують критичні операції [9]. Ефективне впровадження PAM дає змогу мінімізувати область атаки, зменшити людський фактор та захистити інфраструктуру від внутрішніх і зовнішніх кіберзагроз.

Основним завданням PAM є централізація управління привілейованими обліковими записами та мінімізація часу й обсягу їх активності. Технологія реалізує принципи Zero Trust [1, 3], принцип найменших привілеїв (Least Privilege) та Just-In-Time (JIT) Access, надаючи доступ лише тоді й настільки, наскільки це необхідно для виконання службових обов'язків. Одним із базових компонентів PAM є «бастіон-хост» або спеціалізований сервер доступу, через який здійснюється вся привілейована діяльність. Він дозволяє здійснювати повний аудит дій, запис сесій та блокування ризикових операцій у реальному часі.

PAM-системи включають механізми автоматичного зберігання, ротації та шифрування паролів привілейованих облікових записів у так званому "password vault". Це запобігає використанню статичних або повторюваних паролів, які часто стають ціллю атак [8, 10]. Додатково активно застосовуються методи багатофакторної автентифікації, обмеження за IP-адресою, умовний доступ на основі ризикових атрибутів, а також контроль підвищення привілеїв.

Ще одним важливим аспектом PAM є управління обліковими записами сервісів і машин, які зазвичай працюють без втручання користувача та мають високі привілеї. Через складність цих облікових записів їх легко експлуатувати при атаках типу Pass-the-Hash або Pass-the-Ticket. Використання керованих облікових записів сервісів, автоматизована ротація ключів та контроль контексту виконання значно знижують ризики компрометації.

Моніторинг привілейованих сесій — ще один критичний елемент. PAM надає можливість у режимі реального часу відстежувати команди, дії та операції користувача, застосовувати політики блокування, а також передавати події в SIEM для кореляції інцидентів [24, 29, 31]. Таким чином забезпечується повна прозорість і контроль над діями адміністраторів, що значно зменшує ймовірність зловживання привілеями або виконання небезпечних змін.

У корпоративних інфраструктурах PAM часто інтегрується з IAM, системами MFA, SIEM/SOAR-платформами, системами управління вразливостями, а також хмарними сервісами (AWS IAM, Azure PIM, Google

Cloud IAM). Завдяки такій інтеграції формується багаторівневий механізм захисту доступів, який забезпечує як централізоване управління привілеями, так і динамічну оцінку ризиків.

Рис. 1.7 відображає модель процесу Privileged Access Management, що демонструє основні потоки даних між адміністратором, привілейованим користувачем, PAM-системою та цільовими ресурсами. У моделі показано взаємодію PAM із сховищем секретів (Vault), репозиторієм політик та журналами сесій, а також передавання подій у систему моніторингу SIEM [24, 31]. Така структура відображає логіку контролю привілейованих доступів і забезпечує централізований аудит, ротацію секретів та управління привілеями відповідно до принципів Zero Trust.

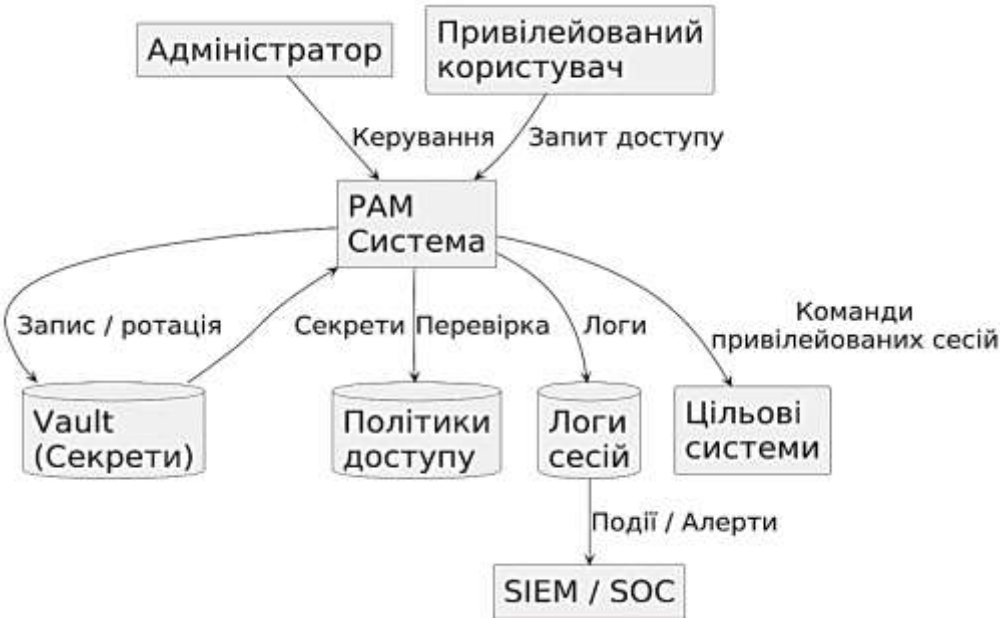

Рис. 1.7. Модель процесу Privileged Access Management (PAM)

Отже, Privileged Access Management відіграє ключову роль у захисті привілейованих облікових записів, попередженні їх компрометації та мінімізації потенційних втрат від цільових кіберзагроз. Впровадження PAM-підходів забезпечує підприємству не лише високий рівень контролю доступів, а й відповідність сучасним стандартам кібербезпеки, зокрема ISO/IEC 27001, NIST SP 800-53, CIS Controls та Zero Trust Architecture.

1.5. Zero Trust Access: принципи, етапи формування та особливості застосування

Концепція Zero Trust Access формується як відповідь на зростаючу складність сучасного кіберпростору, у якому традиційні perimeter-based моделі безпеки вже не здатні ефективно протидіяти загрозам, пов’язаним із віддаленою роботою, хмарними середовищами, наскрізною цифровою інтеграцією та збільшенням кількості атак, спрямованих на компрометацію облікових даних [15, 48, 52, 54]. Zero Trust базується на фундаментальному принципі «ніколи не довіряй, завжди перевіряй», що передбачає відсутність заздалегідь гарантованої довіри навіть до внутрішніх об’єктів, користувачів чи пристроїв. Кожен запит доступу розглядається як потенційно небезпечний і перевіряється комплексно: ідентичність користувача, стан пристрою, контекст взаємодії, рівень ризику та відповідність політикам безпеки.

Zero Trust Access включає низку ключових принципів, які визначають логіку побудови сучасної архітектури доступу 13, 52-54. Центральним із них є принцип мінімальних привілеїв, за яким доступ надається виключно в обсязі, необхідному для виконання конкретного завдання, і переважно на обмежений час відповідно до моделі Just-in-Time. Важливим елементом є сегментація середовища, яка мінімізує можливість lateral movement у разі успішної атаки [50]. Доступ стає контекстно орієнтованим: рішення приймається з урахуванням поведінки користувача, типу мережі, геолокації, параметрів ризику та стану пристрою [33, 36, 40, 42]. Усі пристрої підлягають автентифікації та перевірці на відповідність вимогам безпеки, а кожна взаємодія забезпечується безперервним моніторингом.

Формування Zero Trust Access відбувається поетапно і вимагає детального розуміння середовища та інформаційних активів підприємства. Спершу виконується повна інвентаризація користувачів, сервісів, пристроїв та ресурсів, після чого визначається їх критичність і важливість для бізнес-процесів [21-23]. Далі моделюються потенційні загрози й оцінюється поверхня атаки з використанням методів ATT&CK, STRIDE та інших підходів [43-44, 49]. На

основі отриманих даних проєктуються політики доступу, що враховують рольові, атрибутивні та поведінкові параметри. Впровадження багатофакторної автентифікації, passwordless-методів, OAuth 2.0 та OpenID Connect забезпечує належний рівень ідентифікації. Особливе значення приділяється застосуванню Just-in-Time доступу, який запобігає тривалому існуванню привілейованих прав [35, 40-42, 51]. Сегментація інфраструктури, UEBA-аналітика та адаптивні політики доступу формують завершений захисний контур Zero Trust.

Рис. 1.8 відображає концептуальну модель Zero Trust Access, у якій основними елементами є принцип мінімальних привілеїв, перевірка кожного запиту, застосування контрольних політик та безперервний моніторинг і аналітика [48, 52, 54]. Модель демонструє циклічну взаємодію цих компонентів, що забезпечує адаптивний, контекстно орієнтований та постійно перевірюваний доступ у відповідності до принципу «ніколи не довіряй, завжди перевіряй».

Рис. 1.8. Модель Zero Trust Access у системах управління доступом

Застосування Zero Trust Access має низку особливостей, що суттєво підвищують безпеку корпоративних систем. Насамперед, це посилений контроль привілейованих доступів через інтеграцію з PAM, що мінімізує ризик зловживання адміністраторськими правами. Zero Trust легко масштабується у хмарних та гібридних середовищах, забезпечує уніфікований доступ до API, мікросервісів, IoT-пристроїв і корпоративних застосунків. Завдяки поведінковим моделям і машинному навчанню система здатна автоматично виявляти аномалії,

блокувати ризикові операції та адаптувати політики відповідно до зміни загрозового ландшафту. Крім того, Zero Trust відповідає рекомендаціям міжнародних стандартів, таких як NIST SP 800-207, ISO/IEC 27001 та CIS Controls, що робить його придатним для регульованих секторів.

Таблиця 1.4

Принципи Zero Trust та їх реалізація в Access Management

Принцип Zero Trust	**Суть принципу**	**Реалізація в Access Management**
Never Trust, Always Verify	Жоден користувач чи пристрій не вважається довіреним за замовчуванням	Постійна перевірка ідентичності, MFA, SSO, перевірка токенів, валідація сеансів
Least Privilege Access	Доступ надається тільки у мінімально необхідному обсязі	Рольові (RBAC), атрибутивні (ABAC) та політико-орієнтовані моделі (PBAC); контроль привілеїв JIT
Microsegmentation	Поділ інфраструктури на ізольовані сегменти для зменшення поверхні атаки	Обмеження доступу за зонами, сегментування ресурсів, накладення політик для кожного сервісу
Device Trust	Допуск до ресурсів надається лише перевіреним і керованим пристроям	Перевірка стану пристрою (Device Posture), сертифікати, контроль відповідності політикам
Context-Aware Access	Урахування додаткових факторів при прийнятті рішення про доступ	Оцінка ризику, поведінковий аналіз, геолокація, час доби, тип мережі, рівень загрози
Continuous Monitoring	Постійний аудит, аналіз поведінки та виявлення аномалій	Логи IAM, сесійний моніторинг, UEBA, інтеграція з SIEM/SOAR, автоматичні алерти
Automated Policy Enforcement	Політики мають застосовуватися автоматично	Динамічне застосування PBAC/ABAC, автоматичне блокування доступу, ремедіація інцидентів
Assume Breach	Передбачення можливої компрометації та вибудова захисту з її урахуванням	Мінімізація lateral movement, швидке відкликання доступу, постійна верифікація привілеїв

Таким чином, Zero Trust Access є сучасною, динамічною та контекстно орієнтованою моделлю контролю доступу, яка забезпечує повну перевірку користувачів і пристроїв, мінімізацію привілеїв, адаптивну авторизацію та постійний моніторинг поведінки. Його впровадження дозволяє суттєво підвищити стійкість інформаційних систем до компрометації облікових записів та складних кіберзагроз, формуючи надійний фундамент безпеки корпоративного середовища.

1.6. Технології аутентифікації та сучасні методи гарантування цифрової ідентичності

Аутентифікація користувачів є базовим механізмом забезпечення інформаційної безпеки та ключовим елементом систем Access Management, оскільки саме вона визначає достовірність особи чи сервісу, що запитує доступ до інформаційних ресурсів [1-2, 11, 13]. У сучасних умовах цифрової трансформації, зростання кількості кіберзагроз та широкого використання хмарних сервісів потреба у надійних методах підтвердження ідентичності значно зросла [48, 54]. Традиційні підходи, засновані на паролях, поступово втрачають ефективність через високий рівень уразливості до фішингу, credential stuffing, brute-force атак та соціальної інженерії. Це зумовлює необхідність переходу до багаторівневих, криптографічно стійких та поведінкових методів установлення цифрової ідентичності.

Сучасні системи аутентифікації базуються на поєднанні трьох основних категорій факторів: знань (паролі, пін-коди), володіння (токени, смартфони, смарт-карти) та характеристик користувача (біометрія) [2, 8]. Одним із найбільш поширених рішень є багатофакторна аутентифікація (MFA), яка об’єднує декілька різнотипних факторів та суттєво знижує ризик компрометації облікових записів [11-14]. Поширеними технологіями є FIDO2/WebAuthn, які забезпечують аутентифікацію без паролів через криптографічні ключі, захищені на пристроях користувача, та є стійкими до фішингу. Біометричні методи — розпізнавання обличчя, відбитків пальців, голосу або поведінкової моделі — підвищують зручність і безпеку, хоча потребують спеціальних механізмів захисту біометричних шаблонів [13, 33, 36]. З іншого боку, поведінкова біометрія аналізує унікальні шаблони взаємодії користувача з системою, такі як динаміка набору тексту, спосіб руху чи навігації, що дозволяє забезпечити безперервну аутентифікацію без додаткових дій з боку користувача.

Інтеграція сучасних технологій аутентифікації здійснюється через стандартизовані протоколи, такі як OAuth 2.0, OpenID Connect та SAML 2.0, що забезпечують безпечний обмін ідентифікаційними даними між сервісами. Ці

протоколи дозволяють реалізувати єдиний вхід (SSO), забезпечують передачу маркерів доступу та ідентифікації, а також спрощують управління цифровими ідентичностями у розподілених екосистемах [17, 47]. Значне поширення має passwordless-аутентифікація, яка ґрунтується на застосуванні апаратних криптоключів, одноразових кодів, push-повідомлень чи біометричних методів без необхідності зберігання та введення паролів.

Особливої актуальності набувають моделі децентралізованої ідентичності (Decentralized Identity, DID), що використовують криптографію та розподілені реєстри для збереження цифрових атрибутів користувача без централізованих сховищ. Такий підхід мінімізує ризики витоку даних та забезпечує контроль користувача над власними ідентифікаційними даними [2, 4, 11]. Ще однією тенденцією є використання технологій контекстної аутентифікації, де рішення про дозвіл доступу приймається з урахуванням поведінкових і ризикових факторів: місцезнаходження, часу доступу, типу пристрою, профілю активності та рівня загрози [33, 36, 43]. Це дозволяє реалізувати адаптивну аутентифікацію, у якій система автоматично підсилює вимоги до перевірки у разі виявлення аномальних дій.

Рис. 1.9. Модель процесу цифрової ідентичності в системах Access Management

Рис. 1.9 відображає модель обробки цифрової ідентичності, що включає основні потоки інформації між користувачем, системою цифрової ідентичності (IDM), сервісами, а також сховищами ідентифікаційних даних, атрибутів та

журналів подій [12, 19]. Модель демонструє процес збирання, зберігання та перевірки ідентичності, генерування токенів доступу та реєстрації дій для подальшого моніторингу безпеки.

Табл. 1.5 узагальнює основні компоненти цифрової ідентичності, на яких базується робота систем Access Management [21-23]. Кожен елемент — від ідентифікаційних даних і атрибутів до журналів подій та політик — відіграє роль у забезпеченні коректної ідентифікації, автентифікації й авторизації користувачів. Сукупність цих компонентів формує цілісний профіль цифрової ідентичності, що лежить в основі прийняття рішень у сучасних системах управління доступом.

Таблиця 1.5

Компоненти цифрової ідентичності

Компонент	**Опис**	**Функціональне призначення**
Ідентифікаційні дані (ID Data)	Унікальні атрибути користувача: ім’я, ID, e-mail, номер телефону, унікальний UUID	Забезпечення однозначної ідентифікації суб’єкта в системі
Атрибути користувача (User Attributes)	Додаткові параметри: роль, посада, група, відділ, рівень доступу, статус пристрою	Формування політик доступу в IAM/ABAC; контекстна авторизація
Креденшили (Credentials)	Паролі, токени доступу, ключі FIDO2, сертифікати, OTP-коди	Проведення автентифікації та підтвердження права доступу
Біометричні дані (Biometrics)	Відбитки пальців, розпізнавання обличчя, голос, поведінкові патерни	Забезпечення високого рівня довіри та «passwordless»-автентифікації
Контекстні атрибути (Context Attributes)	Локація, час доступу, тип мережі, поведінкові дані, ризиковий бал	Адаптивна авторизація та реалізація Zero Trust Access
Метадані доступу (Access Metadata)	Час видачі токена, тривалість сеансу, пристрій, IP-адреса	Контроль сеансів, виявлення аномалій та моніторинг активності
Журнали подій (Audit Logs)	Дані про входи, помилки аутентифікації, зміни атрибутів, доступ до ресурсів	Забезпечення аудиту, форензики та інтеграції з SIEM/SOAR
Політики ідентичності (Identity Policies)	Правила автентифікації, авторизації, MFA, passwordless, PBAC/ABAC	Формалізація та автоматизація рішень Access Management
Довірчі сервіси (Trust Services)	CA, PKI, криптографічні протоколи, WebAuthn/FIDO2	Гарантування цілісності та достовірності цифрової ідентичності
Сховище цифрових ідентичностей (Identity Store)	LDAP, Azure AD, Keycloak, IAM-репозиторії	Зберігання та керування даними ідентичності

У межах сучасних Zero Trust-архітектур аутентифікація перестає бути одноразовим етапом і перетворюється на безперервний процес, який підтримує постійну перевірку суб’єкта доступу, стану пристрою та контексту взаємодії. Такі підходи забезпечують високий рівень захисту від компрометації, мінімізують можливість несанкціонованого доступу та створюють надійну основу для побудови системи Access Management. У результаті технології аутентифікації стають не лише процедурою підтвердження особи, а й важливою складовою цифрової довіри та ключовим елементом забезпечення цілісності сучасних інформаційних систем.

1.7. Нормативні та галузеві стандарти управління доступом

Управління доступом є одним із ключових напрямів інформаційної безпеки, який регламентується широким спектром міжнародних, галузевих та національних стандартів [9, 22, 45]. Ці нормативні документи визначають вимоги, принципи та рекомендації щодо побудови систем ідентифікації, автентифікації, авторизації та моніторингу доступу, а також встановлюють критерії оцінювання ефективності заходів безпеки [21-23, 45, 52-54]. Відповідність стандартам дозволяє підприємствам забезпечити належний рівень захисту інформаційних активів, мінімізувати ризики, а також інтегрувати Access Management у комплексну систему кіберзахисту.

Одним із базових документів у сфері управління доступом є міжнародний стандарт ISO/IEC 27001, який визначає вимоги до системи управління інформаційною безпекою (ISMS) [7, 21-23]. Серед його контролів значне місце відведено управлінню ідентифікацією та доступом, зокрема встановленню політик доступу, контролю привілейованих облікових записів, принципу мінімальних привілеїв і регулярному перегляду прав доступу. Додаткові деталі та практичні рекомендації щодо реалізації цих вимог наведено у ISO/IEC 27002, який описує методи застосування технічних та організаційних заходів управління доступом.

Важливим джерелом методичних рекомендацій є стандарт NIST SP 800-53, що встановлює набір контролів для федеральних інформаційних систем США [52-54]. Окремий розділ AC (Access Control) містить вимоги щодо автентифікації, авторизації, сегментації, контролю внутрішніх доступів і управління привілейованими обліковими записами. У розвиток цього документа NIST підготував NIST SP 800-63, який визначає рівні довіри до автентифікації (IAL, AAL, FAL) та описує сучасні криптографічні і парольні механізми [47-48, 52-55]. Для реалізації сучасних концепцій доступу особливо значущим є стандарт NIST SP 800-207, який формує архітектурні принципи Zero Trust та визначає вимоги до безперервної верифікації користувачів, пристроїв і контексту доступу.

У галузевих середовищах, зокрема фінансових, поширені вимоги PCI DSS, які регламентують захист платіжних даних і містять конкретні вимоги щодо багатофакторної аутентифікації, моніторингу привілейованих доступів та журналювання дій [21-23]. Для державного сектору актуальними є рамкові вимоги CIS Controls v8, що включають набір рекомендацій щодо управління ідентичностями, контролю привілеїв і захисту адміністративних акаунтів [9, 45]. Значну роль відіграє також OAuth 2.0, OpenID Connect та SAML 2.0 — стандартизовані протоколи управління ідентичністю та доступом у хмарних та мультисервісних системах [11-13, 15]. У контексті управління привілейованими доступами важливим є стандарт ISO/IEC 27005, який визначає ризик-орієнтований підхід до побудови систем PAM та IAM.

На національному рівні управління доступом регламентується законами України «Про основні засади забезпечення кібербезпеки» та «Про захист інформації в інформаційно-комунікаційних системах», а також вимогами технічного захисту інформації (ТЗІ) [25, 45, 49-50]. Ці документи встановлюють обов’язковість автентифікації користувачів, захисту від несанкціонованого доступу, контролю привілейованих дій і ведення журналів подій. Нормативна база НБУ, ДССЗЗІ та галузеві профільні стандарти доповнюють загальні вимоги конкретними критеріями для фінансових, державних і критичних інфраструктур.

На рис. 1.10 представлено узагальнену нормативно-правову модель управління доступом, яка включає три ключові компоненти: міжнародні стандарти (ISO/IEC 27001, NIST SP 800-63, PCI DSS), регуляторні вимоги (законодавство України та галузеві норми) та протоколи автентифікації й авторизації (OAuth 2.0, SAML, OpenID Connect) [19, 45, 49-50]. Усі ці елементи формують фундамент політик та механізмів Access Management, забезпечуючи його відповідність вимогам безпеки, сумісність і надійність.

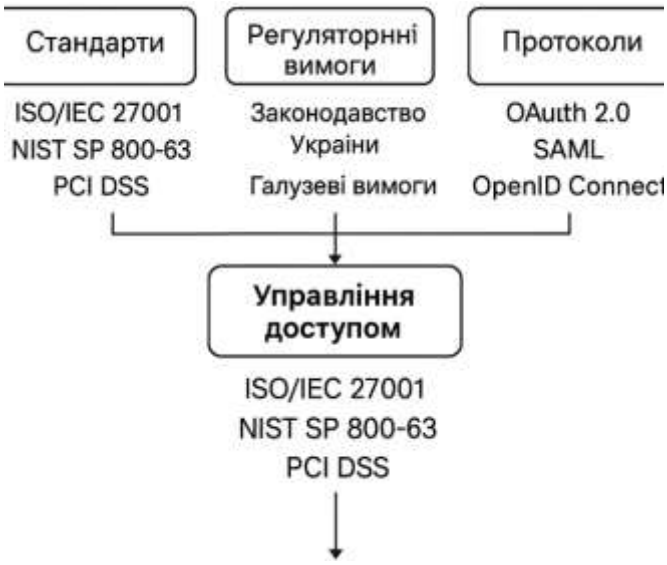

Рис. 1.10. Модель процесу цифрової ідентичності в системах Access Management

Таким чином, нормативні та галузеві стандарти формують комплексну систему вимог, яка охоплює всі аспекти управління доступом — від автентифікації та визначення рівнів довіри до реалізації політик, моніторингу, захисту привілейованих акаунтів і побудови архітектур Zero Trust. Дотримання цих стандартів є ключовою умовою підвищення рівня кіберзахисту підприємства, забезпечення відповідності регуляторним вимогам і формування стійкої моделі безпечного доступу до інформаційних ресурсів.

Висновки до першого розділу

У першому розділі було узагальнено теоретичні засади управління доступом як ключового компонента корпоративної кібербезпеки. Показано, що технології Access Management базуються на процесах ідентифікації, автентифікації та авторизації користувачів, забезпечують реалізацію принципів конфіденційності, цілісності та доступності інформації й фактично визначають, хто, коли і до яких ресурсів може отримати доступ. Розглянуті моделі контролю доступу (MAC, DAC, RBAC, ABAC, PBAC) продемонстрували еволюцію від жорстких централізованих механізмів до гнучких, атрибутивних і політико-орієнтованих підходів, здатних підтримувати динамічні сценарії доступу та концепцію Zero Trust.

Проаналізовано роль систем Identity & Access Management (IAM) та Privileged Access Management (PAM) у побудові комплексної архітектури безпеки. IAM розглянуто як центральну платформу керування цифровими ідентичностями та життєвим циклом доступів, тоді як PAM орієнтується на захист привілейованих облікових записів, мінімізацію області атаки та прозорий аудит критичних дій. Окрему увагу приділено концепції Zero Trust Access, яка запроваджує принципи «ніколи не довіряй, завжди перевіряй», «мінімальні привілеї», мікросегментацію та контекстно-орієнтоване прийняття рішень щодо доступу. Показано, що сучасні технології аутентифікації (MFA, passwordless, FIDO2/WebAuthn, поведінкова біометрія) та моделі цифрової ідентичності є невід’ємною частиною такої архітектури.

Додатково встановлено, що впровадження Access Management має спиратися на нормативну базу міжнародних і національних стандартів (ISO/IEC 27001, NIST SP 800-53, NIST SP 800-63, NIST SP 800-207, PCI DSS, CIS Controls, а також профільні акти законодавства України). Саме ці стандарти визначають вимоги до політик доступу, керування привілеями, журналювання подій та безперервного моніторингу. Узагальнення теоретичних аспектів дозволяє сформувати методологічну основу для подальшого аналізу загроз, побудови моделі Access Management для конкретного підприємства та розроблення практичних рішень щодо підвищення рівня його кіберзахисту.

Розділ 2. МОДЕЛЮВАННЯ ЗАГРОЗ, ПОЛІТИК ТА МЕХАНІЗМІВ ЗАХИСТУ У СИСТЕМАХ ACCESS MANAGEMENT

Моделювання загроз, політик та механізмів захисту у системах Access Management є ключовою основою побудови надійної корпоративної безпеки, оскільки дозволяє заздалегідь визначити можливі сценарії компрометації облікових даних, ескалації привілеїв, зловживання доступами та обходу контролів автентифікації й авторизації [52-55]. Результатом є формалізована модель загроз, що охоплює зовнішні й внутрішні атаки, технічні вразливості IAM/PAM-рішень, людський фактор та помилки конфігурації [6-9, 37]. На основі такої моделі формуються політики доступу (RBAC, ABAC, PBAC), які реалізують принципи мінімальних привілеїв, розмежування обов’язків і Zero Trust [45, 47]. Політики повинні бути узгоджені з нормативами ISO/IEC 27001, NIST і відображати реальні бізнес-процеси, залишаючись динамічними та адаптивними до змін контексту й рівня ризиків. Захисні механізми, які забезпечують виконання цих політик, включають MFA, PAM-контроль, аудит і моніторинг доступів, сегментацію мережі, адаптивну авторизацію, UEBA-аналітику та інтеграцію із SIEM/SOAR [28-32, 35]. Їх моделювання передбачає опис потоків даних, точок прийняття рішень (PDP/PEP) та взаємодії між суб’єктами, ресурсами й сховищами ідентичностей. Таким чином, моделювання загроз, політик і механізмів захисту забезпечує структуровану й ефективну базу для впровадження сучасних систем Access Management.

2.1. Формування моделі активів, користувачів та привілеїв у корпоративному середовищі

Ефективність системи Access Management визначається здатністю корпоративного середовища точно моделювати активи, користувачів і привілеї, що забезпечує обґрунтоване та контрольоване прийняття рішень про доступ [8-11, 13, 48]. Формалізована модель дозволяє системі безпеки враховувати

критичність ресурсів, характеристики суб'єктів доступу, вимоги політик та контекст ризику, що є передумовою для реалізації принципів мінімальних привілеїв та Zero Trust.

У загальному вигляді множина активів інформаційно-комунікаційної системи подається як [7, 19, 21-23]:

$$A = \{a_1, a_2, \dots, a_n\}, \quad (2.1)$$

Для кожного активу визначається набір атрибутів, що характеризують його з точки зору безпеки:

$$Attr(a_i) = \{Conf_i, Int_i, Avail_i, Sens_i, Owner_i\}, \quad (2.2)$$

Ці параметри дозволяють обчислити індивідуальну функцію ризику активу, що визначається як:

$$Risk(a_i) = f(Conf_i, Int_i, Avail_i, Threats_i, Vuln_i), \quad (2.3)$$

Таким чином, кожний актив отримує формалізовану оцінку, яка надалі визначає вимоги до автентифікації, авторизації та контролю доступу.

Паралельно формується модель користувачів та інших суб'єктів доступу, множина яких задається виразом [2, 5, 8]:

$$U = \{u_1, u_2, \dots, u_m\}, \quad (2.4)$$

Кожному суб'єкту призначається набір атрибутів, що описують його роль у системі:

$$Attr(u_j) = \{Role_j, Dept_j, Clearance_j, Device_j, Location_j\}, \quad (2.5)$$

У Zero Trust-архітектурах вводиться контекстна оцінка довіри користувача, яка визначається як [16, 20, 33]:

$$Trust(u_j) = g\left(Device_j, Location_j, Behavior_j, Device_j, RiskContextLocation_j\right) \quad (2.6)$$

Ця оцінка використовується для адаптивного прийняття рішень про доступ на основі поведінкових і контекстних факторів.

Модель привілеїв окреслюється множиною дозволених операцій [8, 21-23]:

$$P = \{p_1, p_2, \dots, p_k\}, \quad (2.7)$$

Відношення доступу між користувачем, активом і привілеєм формалізується як [5, 8, 21]:

$$Access \subseteq U \times A \times P, \tag{2.8}$$

Отже, користувач має доступ до певної операції, якщо:

$$(u_j, a_i, p_k) \in Access, \tag{2.9}$$

У межах рольової моделі RBAC використовується множина ролей:

$$Role = \{r_1, r_2, \dots, r_h\}, \tag{2.10}$$

а її формальні відношення задаються:

$$UA \subseteq U \times Role, \tag{2.11}$$

$$PA \subseteq Role \times P, \tag{2.12}$$

Доступ користувача до активу визначається правилом:

$$Access(u_j, a_i) = \{p_k \mid \exists r_x : (u_j, r_x) \in UA \wedge (r_x, p_k) \in PA\}, \tag{2.13}$$

У атрибутивній моделі ABAC рішення про дозвіл доступу формалізується через політику [2, 11, 13]:

$$Permit(u_j, a_i, p_k) = True \text{ якщо } Policy\left(Attr(u_j), Attr(a_i), Context\right) = True, \tag{2.14}$$

У сучасних корпоративних середовищах найчастіше використовується комбінована RBAC/ABAC/PBAC-модель. Рішення про доступ ухвалюється точкою прийняття політик (PDP) за функцією [21-23, 48, 52-55]:

$$Decision = PDR(UA, PA, Attr(u), Attr(a), Policies, Context), \tag{2.15}$$

Після цього точка виконання політик (PEP) реалізує дозволення або блокування доступу [9-11, 13, 15]:

$$Allow = PEP(Decision), \tag{2.16}$$

Одним із ключових принципів систем Access Management є принцип мінімальних привілеїв, математичний опис якого подано у вигляді оптимізаційної задачі:

$$MinPriv(u_j) = arg \min_{P'} \left|P'\right| \;\; s.t. \;\; Task(u_j) \subseteq Abilities\left|P'\right|, \tag{2.17}$$

Ця задача визначає найменший набір дозволів, достатній для виконання функціональних обов’язків користувача, що мінімізує ризики внутрішніх загроз.

Інтегральна модель системи Access Management подається як [52-55]:

$$AM = (U, A, P, Policies, Context), \tag{2.18}$$

а загальне рішення про доступ описується виразом [1-3, 19, 48]:

$$Decision = f(U, A, P, Policies, Context), \quad (2.19)$$

На рис. 2.1 подано потокову DFD-модель прийняття рішень у системі Access Management, побудовану на основі формальних співвідношень (2.11)–(2.19) [9-11, 13, 21-23]. У моделі показано взаємодію точок прийняття політик (PDP) та виконання політик (PEP), а також інформаційні потоки, що включають множини користувачів U, активів A, привілеїв P, політик доступу та контексту безпеки. Центральним елементом є функція прийняття рішень $Decision = f(U, A, P, Policies, Context)$, результат якої надходить у PEP для виконання. Схема наочно демонструє, як атрибути користувачів і активів, рольові відношення UA/PA та політики формують кінцеве рішення про надання чи заборону доступу.

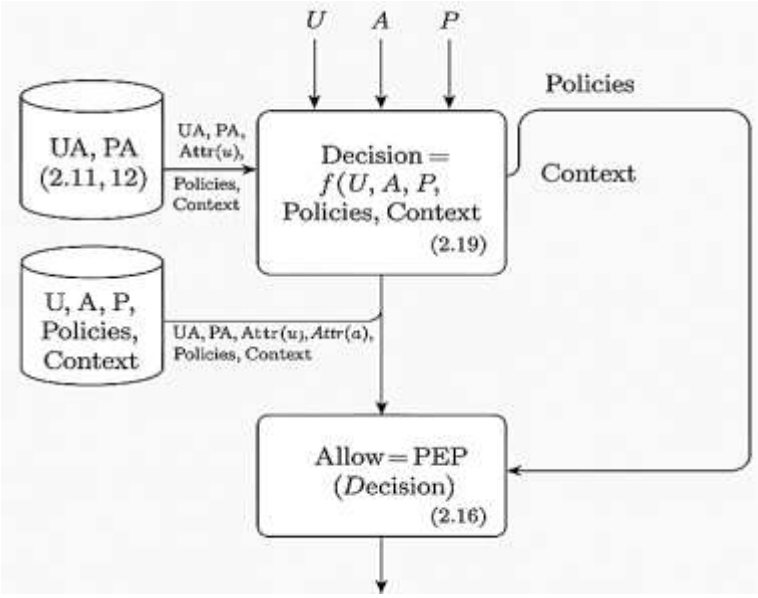

Рис. 2.1. Модель Access Management на основі формальних залежностей

Отже, формалізована модель активів, користувачів та привілеїв забезпечує кількісну та структурну основу для прийняття рішень у технології Access Management, дозволяє реалізувати сучасні політики доступу, підтримувати Zero Trust, знижувати ризики кіберзагроз та забезпечувати відповідність вимогам міжнародних стандартів.

2.2. Побудова моделі загроз для технологій управління доступом

Побудова моделі загроз є ключовим етапом забезпечення безпеки систем Access Management, оскільки дозволяє формально визначити потенційні вектори атак, їх причини, наслідки та взаємозв'язки з уразливостями компонентів IAM/PAM-інфраструктури [5-6, 18-20, 48]. Модель загроз спрямована на систематизацію ризиків, пов'язаних із компрометацією облікових записів, зловживанням привілеями, вразливими протоколами автентифікації, помилками політик та людським фактором.

Основою для побудови моделі загроз є класифікація активів, користувачів і привілеїв, сформована відповідно до формальних залежностей моделі Access Management [7, 21-23]. Кожен актив a_i, користувач u_j та привілей p_k розглядаються як потенційні об'єкти впливу з боку порушника. Загальна множина загроз визначається як [48, 52-55]:

$$T = \{t_1, t_2, \dots, t_s\}, \tag{2.20}$$

де $\boldsymbol{t_i}$ описує окремий тип загрози: викрадення облікових даних, brute-force атаки, фішинг, ескалація привілеїв, скомпрометовані токени доступу [24, 26, 37], обхід MFA, несанкціоновані зміни політик чи доступ до секретів PAM-сховища.

Для кожної загрози визначається функція впливу на актив [24, 44]:

$$Impact(a_i, t_j) = f\big(Sens_i, Vuln_i, Prob_j\big), \tag{2.21}$$

де $Sens_i$ – чутливість активу, $Vuln_i$ – наявні уразливості, $Prob_j$ – ймовірність реалізації загрози. Це дозволяє кількісно оцінити критичність взаємодії між загрозою та активом.

Оскільки в системах управління доступом значну роль відіграє людський фактор, зокрема дії внутрішніх порушників, вводиться множина внутрішніх загроз [18, 33, 42-43]:

$$T_{int} = \{t_{int1}, t_{int2}, \dots, t_{intm}\}, \tag{2.22}$$

серед яких найпоширенішими є зловживання привілейованими правами, несанкціоноване копіювання даних, маніпуляції з політиками доступу та несвоєчасне скасування прав користувачів (orphan accounts).

Формально порушник описується множиною властивостей [24, 52-54]:

$$Attacker = (Skills, Resources, Motivation, AccessLevel), \quad (2.23)$$

що дає змогу моделювати різні типи атакувальних сценаріїв — від зовнішніх кіберзлочинців до співробітників з високими правами.

Побудова моделі загроз включає також аналіз точок доступу до ідентичності. Зокрема, уразливими є етапи автентифікації, авторизації, створення токенів, доступ до секретів, а також інтеграція з зовнішніми сервісами (IdP/SP) [34, 47-48]. Для цього вводиться множина уразливих точок [37-39, 41-42]:

$$\boldsymbol{VulnPoints = \{up_1, up_2, \dots, up_r\},} \quad (2.24)$$

що охоплює протокольні вразливості, слабкі конфігурації, неправильні політики, недостатній моніторинг та недосконалу сегментацію доступів.

Загальна модель загроз технологій Access Management може бути представлена як кортеж [44-45, 51-52]:

$$\boldsymbol{TM = (T, VulnPoints, Attacker, Impact, Controls)}, \quad (2.25)$$

де *Controls* − множина контрзаходів, що враховуються при побудові політик доступу та виборі механізмів захисту.

До множини Controls належать технічні та організаційні заходи, зокрема MFA, RBAC/ABAC/PBAC-політики, PAM-рішення, сегментація мережі, моніторинг подій безпеки (SIEM/SOAR), UEBA-аналітика та процедури реагування на інциденти. Формальна прив’язка загроз T та уразливих точок VulnPoints до конкретних контролів із множини Controls дає змогу будувати матриці відповідності «загроза–контроль» і виявляти прогалини в захисті. Такий підхід забезпечує можливість оптимізації архітектури Access Management за критеріями ризику, вартості впровадження та ефективності контрзаходів, що особливо важливо для Zero Trust-орієнтованих корпоративних середовищ.

Побудована модель дає змогу формувати причинно-наслідкові ланцюги атак, що включають компрометацію ідентичності, ескалацію привілеїв, доступ до чутливих активів, приховані дії та збереження стійкої присутності (persistence) [41, 43, 47-48]. У контексті Zero Trust модель загроз враховує

динамічний контекст доступу, поведінкові аномалії та ризикові фактори, що дозволяє переходити від статичних рішень до адаптивної авторизації.

На рис. 2.2 зображено DFD-модель, яка наочно демонструє ключові вектори атак, пов’язані з управлінням доступом та привілейованими обліковими записами. Схема відображає, як компрометація ідентичності, підвищення привілеїв, приховані дії та витік секретів можуть відбуватися через взаємодію користувача, PAM-модуля та активів підприємства. Модель ілюструє критичні точки ризику, що потребують контролю: облікові дані, привілейовані секрети, канали доступу до активів та потенційні шкідливі сценарії.

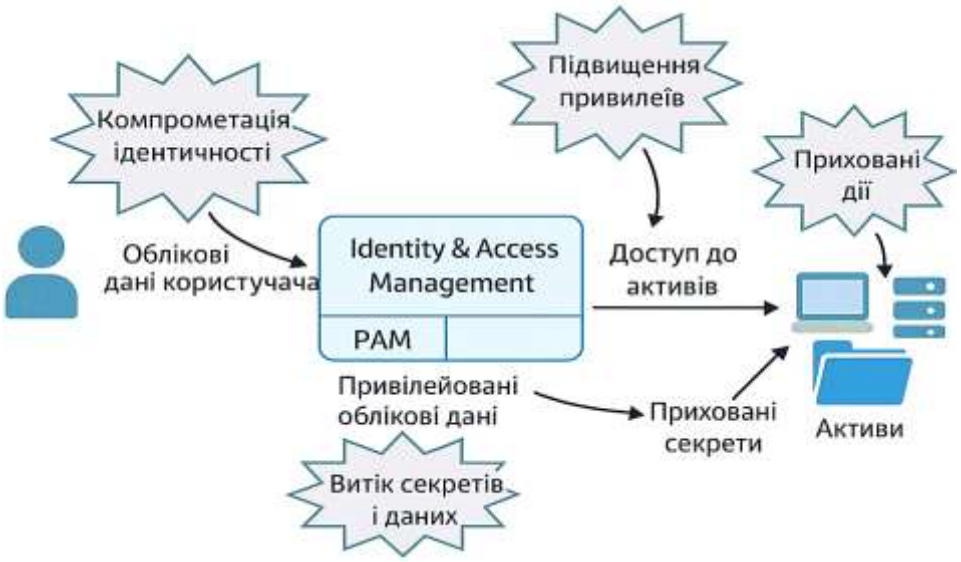

Рис. 2.2. Модель загроз у системах Identity & Access Management (IAM/PAM)

Модель STRIDE дозволяє системно ідентифікувати загрози для технологій управління доступом, включно з IAM, PAM і Zero Trust [1-3, 18-20, 44]. Вона охоплює ключові порушення: компрометацію ідентичності, модифікацію політик доступу, витік секретних даних, збої автентифікації та ескалацію привілеїв. Такий аналіз забезпечує основу для формування політик безпеки, впровадження контролів (MFA, RBAC/ABAC/PBAC, SIEM-моніторинг) та оцінки ризиків у корпоративному середовищі. Додатковою перевагою моделі є можливість побудови формалізованих сценаріїв атак, що враховують взаємодію між суб’єктами, ресурсами та точками прийняття рішень. Це спрощує визначення критичних вузлів інфраструктури, у яких зловмисник

може обійти механізми контролю доступу або вплинути на цілісність політик. На основі результатів STRIDE-аналізу підприємство може створити пріоритезований перелік контрзаходів і план їх впровадження, орієнтований на мінімізацію ризиків та підвищення стійкості системи управління доступом.

Таблиця 2.1

Аналіз загроз Access Management за моделлю STRIDE

Категорія STRIDE	**Тип загрози**	**Опис для Access Management**	**Приклади проявів**
S — Spoofing	Підміна ідентичності	Атакувальник видає себе за легітимного користувача або сервіс	Викрадення облікових даних, фішинг, MFA-bypass
T — Tampering	Модифікація даних	Несанкціоноване змінення політик доступу чи прав	Зміна ролей у RBAC, підвищення привілеїв
R — Repudiation	Відмова від участі у діях	Неможливість довести факт здійснення операції	Відсутність audit-trail, підміна логів
I — Information Disclosure	Розголошення даних	Доступ до облікових даних, токенів, секретів	Витік привілейованих секретів, паролів, ключів API
D — Denial of Service	Відмова в обслуговуванні	Блокування IAM-сервісів, що унеможливлює автентифікацію	DDoS на IdP, DoS на PAM-vault
E — Elevation of Privilege	Підвищення привілеїв	Отримання доступу, вищого за передбачений політикою	Експлуатація вразливостей SSO, обходи RBAC/ABAC

Табл. 2.1 відображає основні категорії STRIDE-загроз та їх вплив на Access Management [13-15, 26, 37-39]. Найбільш критичними для IAM є Spoofing, Information Disclosure та Elevation of Privilege, оскільки вони безпосередньо підривають ідентифікацію, автентифікацію та авторизацію. Tampering і Repudiation вказують на ризики зміни політик доступу та слабкого аудит-логування, що ускладнює виявлення порушень. Denial of Service є небезпечним через можливість виведення з ладу сервісів SSO, MFA чи IdP, блокуючи доступ до систем. Отже, табл. 2.1 дозволяє системно визначити ключові загрози для IAM-компонентів та формує основу для розробки відповідних механізмів захисту.

Таким чином, формалізована модель загроз для систем управління доступом забезпечує кількісну та якісну основу для розроблення політик, вибору механізмів захисту та впровадження технологій IAM/PAM, які здатні протидіяти сучасним кіберзагрозам та мінімізувати ризики компрометації цифрової ідентичності.

2.3. Політики управління доступом та їх оптимізація

Політики управління доступом є центральним механізмом систем Access Management, оскільки саме вони визначають правила взаємодії між користувачами, пристроями, сервісами та активами корпоративного середовища [2, 8, 11]. На основі сформованих правил система ухвалює рішення щодо дозволу, блокування або застосування додаткових механізмів перевірки доступу [2, 23]. Політики трансформують загальні бізнес-вимоги у формалізовані, машинно-читабельні умови, що забезпечує узгодженість рішень, мінімізує ризики людських помилок і підвищує загальний рівень кіберзахисту підприємства.

У загальному випадку політика доступу описує, кому, до якого ресурсу та за яких умов можна виконувати певну операцію. Формально це подається як відображення атрибутів користувача, характеристик активу та контекстних даних у логічне рішення [5, 10-11]:

$$Policy(u, a, p) = \phi(Attr(u), Attr(a), Context), \tag{2.26}$$

де функція $\boldsymbol{\phi}$ повертає Permit, Deny або RequireMFA. Такий підхід демонструє, що рішення залежить не лише від ролі користувача, але й від атрибутів активу, умов середовища (час, місцезнаходження, тип пристрою) та поточного стану безпеки.

У системах з підвищеними вимогами до захисту політики інтегруються з принципами Zero Trust, відповідно до яких будь-який доступ вимагає повторної перевірки та підтвердження [3, 15, 52, 54]. У цьому випадку рішення базується на рівні довіри до користувача чи пристрою:

$$\boldsymbol{Permit = True} \text{ якщо } \boldsymbol{Trust(u) \geq T_{req}}, \tag{2.27}$$

де $\boldsymbol{Trust(u)}$ − динамічна оцінка довіри, що формується на основі поведінкових аномалій, стану пристрою, геолокації та історії активності, $\boldsymbol{T_{req}}$ − мінімально допустимий поріг довіри [16, 47, 55]. Це дозволяє системі адаптувати складність перевірок залежно від поточного ризику, а також забезпечує контекстно-залежну диференціацію доступу.

Для критичних ресурсів політики також включають ризикові обмеження. Доступ дозволяється лише тоді, коли поточний ризик виконання операції не перевищує визначений поріг:

$$\boldsymbol{RiskOp(u, a, p) \leq R_{max}}, \quad (2.28)$$

Таким чином, навіть користувач, що формально має необхідні повноваження, може отримати відмову у доступі в разі виявлення підозрілої активності, невідповідності стану пристрою або ризикового контексту.

У процесі масштабування системи кількість політик збільшується, що часто призводить до їх перетинів та логічних суперечностей. Конфлікт політик виникає тоді, коли однакові умови спричиняють протилежні рішення:

$$\boldsymbol{Conflict(Policy_x, Policy_y) = True} \text{ якщо } \boldsymbol{Cond_x \equiv Cond_y \wedge Effect_x \neq Effect_y}, \quad (2.29)$$

Подібні конфлікти можуть стати причиною надмірного доступу, блокування критичних бізнес-процесів або створення небезпечних обхідних сценаріїв [5, 10]. Для їх виявлення застосовуються формальні методи аналізу політик, валідаційні правила, а також інструменти автоматизованого тестування, що моделюють типові сценарії доступу. Вирішення конфліктів передбачає введення пріоритетів між політиками, уніфікацію умов доступу та рефакторинг надлишкових або дубльованих правил. Додатково необхідно впроваджувати регламентований процес управління життєвим циклом політик (policy lifecycle management), який включає погодження змін, їх аудит та періодичний перегляд з урахуванням актуальних ризиків.

З огляду на це важливим етапом життєвого циклу політик є їх оптимізація. Задача оптимізації полягає у зменшенні кількості політик без зміни їх фактичної поведінки:

$$\boldsymbol{Policies}^{\setminus *} = \mathbf{arg}\,\boldsymbol{min}\,|\boldsymbol{Policies}'|\ \boldsymbol{s.t.}\,\boldsymbol{Behavior}(\boldsymbol{Policies}') = \boldsymbol{Behavior}(\boldsymbol{Policies}), \quad (2.30)$$

Оптимізована система політик повинна залишатися функціонально еквівалентною, але водночас бути компактнішою, логічно узгодженою та зручнішою для адміністрування. Це підвищує прозорість системи IAM, спрощує аудит, зменшує ризик людських помилок і пришвидшує прийняття рішень у режимі реального часу.

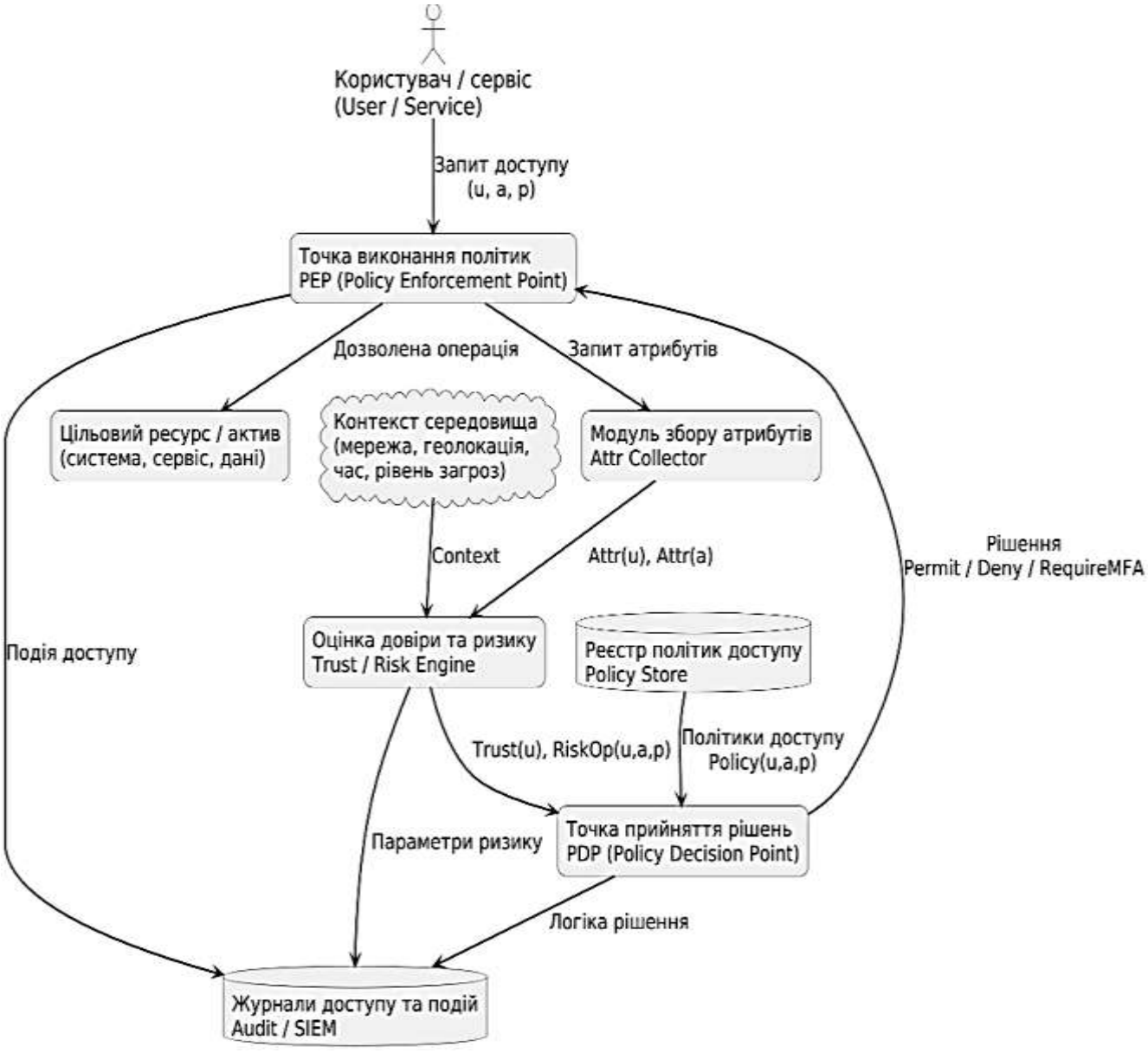

Рис. 2.3. Модель політик управління доступом у системі Access Management

Рис. 2.3 відображає модель роботи політик управління доступом у системі Access Management. Користувач або сервіс формує запит доступу, який

надходить до точки виконання політик (PEP). PEP передає запит у модуль збору атрибутів, де визначаються характеристики користувача, активу та контексту [11-12, 22]. Далі інформація надходить у модуль оцінки довіри та ризику, який обчислює $\boldsymbol{Trust}(\boldsymbol{u})$ та $\boldsymbol{RiskOp}(\boldsymbol{u}, \boldsymbol{a}, \boldsymbol{p})$. Отримані показники разом з політиками доступу з Policy Store передаються до точки прийняття рішень (PDP). PDP аналізує політики, атрибути та рівень ризику і формує рішення — Permit, Deny або RequireMFA [52, 54]. PEP виконує це рішення, надаючи доступ, блокуючи операцію або ініціюючи додаткову автентифікацію. Усі події доступу, включно з рішеннями PDP, реєструються в журналах доступу та SIEM-системі для аудиту та виявлення аномалій [20, 26-27]. Модель демонструє узгоджену взаємодію компонентів Access Management і те, як політики забезпечують контроль та безпеку доступу до корпоративних активів.

Рис. 2.4. Класифікація політик управління доступом

Рис. 2.4 демонструє узагальнену класифікацію політик управління доступом, поділених на чотири основні підходи: ролева (RBAC), атрибутивна (ABAC), Zero Trust та ризик-орієнтована (Risk-Based). Така структура відображає логіку еволюції механізмів контролю доступу від статичних моделей до динамічних і контекстних рішень, що враховують ризики та поведінкові фактори. Кожен із підходів визначає власні принципи прийняття рішень, рівень гнучкості та вимоги до інфраструктури ідентифікації. Завдяки цьому класифікація дозволяє порівняти моделі між собою та обґрунтувати вибір оптимальної стратегії Access Management для конкретного підприємства.

Табл. 2.2. узагальнює ключові типи політик управління доступом і демонструє їх відмінності за принципами прийняття рішень, гнучкістю та рівнем безпеки. Статичні моделі (DAC, RBAC) є простими в адмініструванні, але менш придатні для середовищ із високою динамікою ризиків [21-23, 27]. Натомість атрибутивні та ризик-орієнтовані підходи (ABAC, RBA, PBAC) забезпечують контекстну, адаптивну перевірку доступу, що відповідає вимогам Zero Trust. Найбільш захищені середовища застосовують PAM і MAC, які мінімізують ризики зловживання привілеями та забезпечують суворий контроль над критичними активами. Таким чином, таблиця підкреслює, що оптимальним є комбіноване використання політик залежно від задач і рівня критичності корпоративної ІКС.

Таблиця 2.2

Типи політик управління доступом та їх порівняння

Тип політики	**Опис**	**Ключові параметри**	**Переваги**	**Недоліки**	**Приклади застосування**
RBAC (Role-Based Access Control)	Доступ надається на основі ролей, визначених для користувачів	Role, Permissions, Role Hierarchy	Простота адміністрування, масштабованість	Не враховує контекст, статичність	Корпоративні мережі, ERP/CRM
ABAC (Attribute-Based Access Control)	Рішення базується на атрибутах користувача, активу та контексту	User Attr, Object Attr, Env Attr	Висока гнучкість, підтримка Zero Trust	Складніша конфігурація, ризик конфліктів	Хмарні ІКС, доступ до конфіденційних даних
PBAC (Policy-Based Access Control)	Доступ визначається політиками у вигляді логічних правил	Policies, Conditions, Effects	Централізоване управління, прозорість	Потребує потужного PDP/PEP	Великі IAM-системи, мікросервіси
RBAC+ABAC (гібридна модель)	Комбінує ролі та атрибути для контекстуального доступу	Role, Attr, Context	Баланс простоти та гнучкості	Складність підтримки	Великі підприємства, фінансовий сектор
Risk-Based Access Control (RBA)	Рішення залежить від оцінки ризику та поведінки	Trust Score, Risk Score, Behavior	Адаптивність, динамічна перевірка	Потребує аналітики поведінки	Zero Trust, доступ поза корпоративною мережею

MAC (Mandatory Access Control)	Жорсткі політики, що визначаються системою, а не користувачами	Labels, Clearance Levels	Висока безпека, контроль конфіденційності	Негнучкість, складність реалізації	Військові та державні ІКС
DAC (Discretionary Access Control)	Власник ресурсу сам керує доступом до нього	Owner, ACL	Гнучкість, простота	Ризик людських помилок	Файлові системи, робочі групи
PAM-політики (Privileged Access Policies)	Регулюють доступ до привілейованих облікових записів	Session Rules, Vault, Rotation	Контроль критичних дій, мінімізація зловживань	Висока складність управління	Адмін-доступ, DevOps, інфраструктурні системи

Рис. 2.5 демонструє процес удосконалення політик доступу: від вихідної множини політик через виявлення проблем до усунення конфліктів, дублікативних та надлишкових правил. Завершальним етапом є формування оптимізованої, узгодженої множини політик [10, 19]. Схема стисло показує, як оптимізація зменшує помилки та підвищує ефективність системи Access Management.

Рис. 2.5. Схема оптимізації політик доступу

Узагальнюючи, політики управління доступом виступають ключовою ланкою між моделлю активів, моделлю ролей, користувацькими атрибутами та моделлю загроз. Правильність їх формалізації та оптимізації визначає здатність підприємства протистояти компрометації цифрової ідентичності, ескалації привілеїв, внутрішнім загрозам та атакам на інфраструктуру IAM/PAM [11, 54].

Інтеграція політик з підходами ABAC, Zero Trust та ризик-орієнтованими методами забезпечує збалансоване співіснування безпеки і безперервності бізнес-процесів, а також створює основу для побудови зрілої системи Access Management.

2.4. Технології автентифікації та гарантії рівня довіри

Технології автентифікації відіграють центральну роль у побудові сучасних систем управління доступом, оскільки саме вони визначають ступінь впевненості системи у тому, що запит на отримання доступу надходить від легітимного користувача. На відміну від традиційного підходу, де автентифікація виконувалася одноразово в момент входу, сучасні моделі Access Management базуються на принципах Zero Trust і розглядають автентифікацію як безперервний процес, який включає постійну оцінку користувача, його пристрою та контексту доступу. Це забезпечує захист від крадіжки облікових даних, внутрішніх загроз і атак, спрямованих на компрометацію ідентичності.

Методи автентифікації поділяються на однофакторні (SFA), двофакторні (2FA), багатофакторні (MFA), біометричні та контекстні. Однофакторна автентифікація забезпечує мінімальний рівень безпеки і використовується лише для некритичних систем або в середовищах, де ризики низькі. Двофакторна автентифікація підвищує рівень захищеності, комбінуючи пароль і другий фактор, проте все ще може бути вразливою до атак типу SIM-swap або перехоплення push-сповіщень. Значно вищий рівень надійності забезпечує MFA, що використовує кілька незалежних факторів — біометричні підтвердження, одноразові токени, апаратні ключі FIDO2 або WebAuthn. Біометричні методи гарантують високу унікальність та важку відтворюваність, хоча вимагають захищеного зберігання шаблонів. Контекстна автентифікація, навпаки, оцінює умови доступу — геолокацію, тип пристрою, час доби, мережеву репутацію, поведінкові патерни — і дозволяє виявляти аномальні або ризикові сценарії.

У системах Zero Trust кожен запит користувача оцінюється не лише через успішність автентифікації, а й через рівень довіри (Trust Level, TL), який визначається низкою факторів: якістю ідентифікації, станом пристрою, контекстом доступу, поведінковими характеристиками та ризиковим профілем поточної сесії. Узагальнена модель розрахунку рівня довіри може бути подана у вигляді:

$$TL = w_1 IdScore + w_2 CtxScore + w_3 DevScore + w_4 SessScore, \quad (2.31)$$

де $\boldsymbol{IdScore}$ відображає впевненість у достовірності облікового запису, $\boldsymbol{CtxScore}$ − безпечність контексту, $\boldsymbol{DevScore}$ − відповідність пристрою політикам безпеки, а $\boldsymbol{SessScore}$ − наявність або відсутність аномалій у поведінці користувача. Коефіцієнти $\boldsymbol{w_i}$ визначають вагу кожного фактора залежно від вимог підприємства або критичності конкретного ресурсу.

У Zero Trust рівень довіри не є статичним показником — він постійно оновлюється в реальному часі. Кожна нова дія користувача, кожен доступ до активу або зміна середовища може впливати на оновлену оцінку. Це описується такою динамічною залежністю [47, 53]:

$$TL_{t+1} = f(TL_t, RiskEvent), \quad (2.32)$$

де RiskEvent − будь-яка подія чи сигнал, що може вказувати на потенційну загрозу: від нетипової активності до виявлення нової вразливості або підозрілого стану пристрою [36, 43]. Таким чином, якщо система фіксує ризик, рівень довіри автоматично знижується, що може привести до запиту повторної автентифікації, активації MFA або повного блокування доступу.

Формування та підтримка рівня довіри дозволяють класифікувати користувачів за трьома основними категоріями: високий рівень (High) − повний доступ лише за наявності надійної автентифікації та перевіреного пристрою; середній (Medium) − доступ з умовами або адаптивною автентифікацією; низький (Low) − мінімальні дозволи або негайне блокування запиту [48]. Така градація забезпечує точне балансування між безпекою й ефективністю бізнес-процесів.

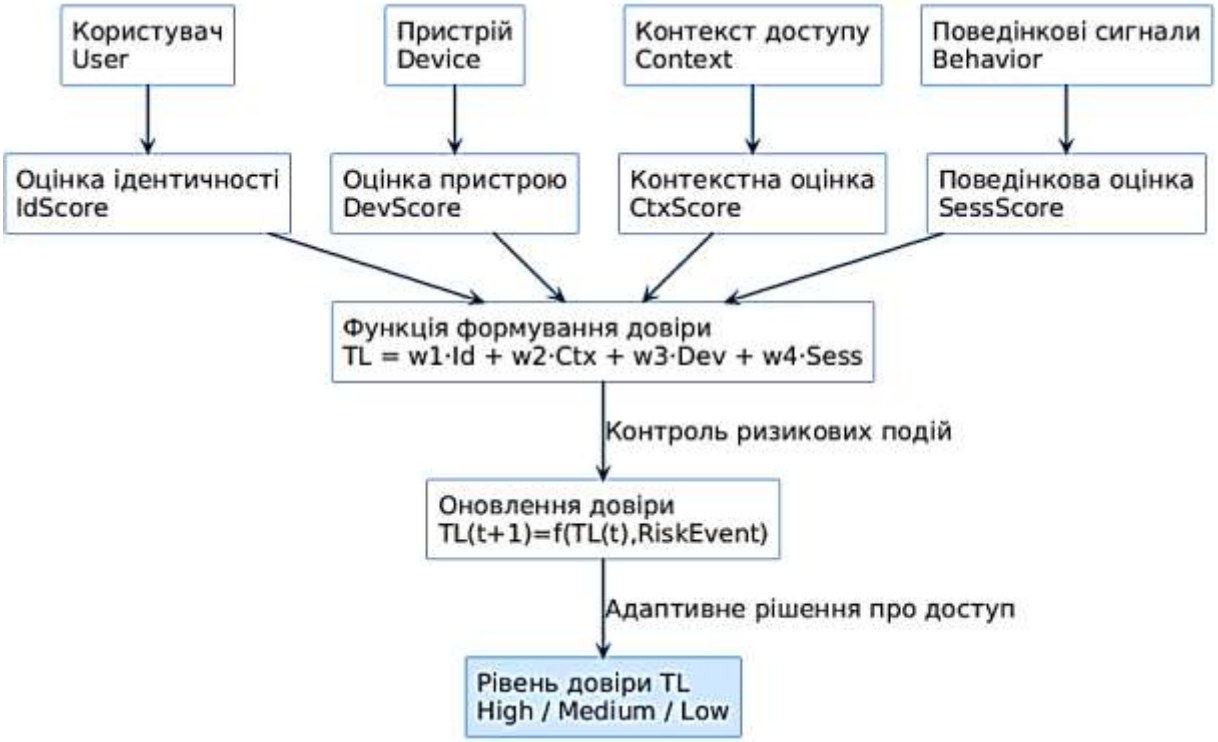

Рис. 2.5. Модель формування рівня довіри TL у системі Access Management

На рис. 2.5 наведено модель формування рівня довіри TL у системі Access Management. Рівень довіри обчислюється на основі чотирьох ключових складових: оцінки ідентичності користувача (IdScore), стану та безпечності пристрою (DevScore), контексту доступу (CtxScore) та поведінкових характеристик (SessScore). Отримані показники інтегруються у єдину функцію TL, після чого система виконує динамічне оновлення значення довіри відповідно до ризикових подій. Підсумковий рівень TL (High, Medium або Low) визначає, чи буде запит користувача дозволено, обмежено або заблоковано.

У підсумку технології автентифікації в поєднанні з динамічною оцінкою рівня довіри формують фундамент сучасних систем Access Management. Вони забезпечують не лише перевірку особи користувача, а й глибоке розуміння того, наскільки безпечним є запит доступу у конкретних обставинах. Це дозволяє організації ефективно протидіяти сучасним кіберзагрозам, запобігати ескалації привілеїв і забезпечувати стійкість до різноманітних атак на ідентичність, досягаючи високого рівня зрілості у реалізації концепції Zero Trust.

2.5. Технології авторизації та керування токенами доступу

Технології авторизації відіграють ключову роль у системах Access Management, оскільки саме вони визначають, які операції користувач або сервіс може виконувати після підтвердження своєї особи [11, 13, 48]. На відміну від автентифікації, що встановлює факт ідентичності, авторизація перетворює бізнес-вимоги у формалізовані правила доступу, які інтерпретуються точкою прийняття політик (PDP) та виконуються точкою контролю доступу (PEP). Сучасна авторизація базується на комбінації моделей RBAC, ABAC та PBAC, які підтримуються протоколами OAuth 2.0, OpenID Connect і SAML 2.0 [47, 53]. Ці протоколи забезпечують передачу прав у вигляді токенів доступу, що дозволяє реалізувати безпечні взаємодії між сервісами, мікросервісами та хмарними ресурсами.

У межах OAuth 2.0 та OpenID Connect ключовим елементом авторизації стає токен доступу (access token) — короткоживучий, криптографічно підписаний маркер, який підтверджує право користувача виконувати певну операцію [11, 13]. Додатково використовується ID токен, що містить атрибути ідентичності, та Refresh токен, який дозволяє відновити доступ без повторної автентифікації [8]. У SAML 2.0 аналогічним елементом є SAML-асерція, що передає атрибути та підтвердження автентичності. Усі ці токени забезпечують механізм авторизації без передачі паролів, що значно підвищує рівень безпеки.

Оскільки у Zero Trust-середовищах рішення про доступ має враховувати не лише ролі та атрибути, а й контекст безпеки, тривалість дії токенів (TTL) стає адаптивною [47-48, 52]. Час життя токена визначається через залежність від рівня довіри TL, ризиковості контексту та чутливості активу. Така залежність формалізується у вигляді:

$$\boldsymbol{TTL = f(TL, RiskContext, Sensitivity)}, \tag{2.33}$$

де $\boldsymbol{TL}$ − поточний рівень довіри до користувача або сервісу, $\boldsymbol{RiskContext}$ − оцінка ризику операції чи середовища, $\boldsymbol{Sensitivity}$ − чутливість активу, до якого здійснюється доступ [19-20, 43-44]. У разі взаємодії з високочутливими ресурсами токени мають коротший термін дії, тоді як для низькоризикових операцій він може бути збільшений. Це забезпечує дотримання принципів

мінімізації привілеїв та адаптивної авторизації. А також дозволяє балансувати між зручністю користувача та необхідним рівнем захисту, не перевантажуючи низькоризикові сценарії надмірними перевірками. Адаптивний TTL узгоджується з підходами динамічного управління сесіями в IAM-системах, де параметри доступу постійно коригуються відповідно до поточного стану середовища та профілю загроз. У поєднанні з безперервною автентифікацією та моніторингом поведінки такий механізм істотно зменшує вікно можливих атак і підвищує стійкість корпоративної ІКС до компрометації токенів.

Оновлення TTL також залежить від динаміки ризикової поведінки, тому система модифікує термін дії токена у процесі роботи користувача. Це описується виразом:

$$\boldsymbol{TTL(t+1) = TTL(t) - \Delta t - Penalty(RiskEvent)}, \quad (2.34)$$

де $\boldsymbol{\Delta t}$ − фактичний час, що минув, $\boldsymbol{Penalty(RiskEvent)}$ − штрафний коефіцієнт, який застосовується у разі виявлення ризикової події, такої як аномальна поведінка, спроба доступу з неавторизованого пристрою або нетипова геолокація [20, 30-32, 41]. Зменшення TTL у відповідь на ризикові події дозволяє мінімізувати вікно атаки та зменшує ймовірність зловживання токеном у разі його компрометації.

Схема на рис. 2.6 відображає ланцюжок обробки токенів у IAM-системі: від запиту користувача до прийняття рішення про доступ [12, 24, 31]. PEP виконує первинну перевірку, IdP генерує або оновлює токени, сховище зберігає їх, ресурсний сервер перевіряє чинність, а Revocation List забезпечує блокування скомпрометованих або прострочених токенів. Модель демонструє повний життєвий цикл токена. Схема підкреслює важливість централізованої координації між компонентами IdP, PEP і ресурсним сервером для забезпечення цілісності механізму доступу. Вона також демонструє, що рішення про надання чи заборону доступу формується не лише на основі токена, а й з урахуванням контексту ризику та можливих інцидентів безпеки. Такий підхід забезпечує відповідність принципам Zero Trust і підвищує стійкість системи до компрометації токенів та атаки на сесію.

Рис. 2.6. Модель керування токенами доступу

Повний життєвий цикл токенів включає їх видачу, валідацію, оновлення та анулювання [30-32, 37-40]. Сервер авторизації видає токен на основі політик доступу та атрибутів суб’єкта. Ресурсний сервер перевіряє цифровий підпис, термін дії, дозволені області доступу (scope) та claims. У разі використання refresh-токена PDP може автоматично продовжити доступ, якщо поведінка користувача не викликає підозр [20, 45]. При наявності ризикових подій система застосовує негайне анулювання (revoke), що розриває всі активні сесії. Це забезпечує незалежне від мережевого розташування централізоване управління правами доступу.

У Zero Trust-контексті токени розглядаються не як доказ постійної довіри, а як тимчасові маркери, які підлягають перевірці при кожній операції [48, 54-55]. Система авторизації оцінює не лише валідність підпису та claims, але й додаткові параметри: відповідність атрибутів, поведінкові сигнали, стан пристрою, геолокацію та кореляцію з історичними моделями активності [47]. У разі невідповідності параметрів політикам система може вимагати повторного підтвердження особи (MFA), зменшити TTL або повністю заблокувати доступ.

Безпека токеноорієнтованої авторизації забезпечується застосуванням криптографічних алгоритмів (RS256, ES256, EdDSA), механізмів прив'язки токенів до пристрою (DPoP, Token Binding), ротації refresh-токенів, короткоживучих access-токенів та сегментації прав доступу через scope [1-3, 35]. Такі заходи мінімізують ризики викрадення чи повторного використання токенів і підвищують стійкість системи до атак, спрямованих на компрометацію цифрової ідентичності.

Таким чином, технології авторизації та управління токенами доступу формують основу безпечного контролю доступу в сучасних корпоративних системах. Інтеграція протоколів OAuth/OIDC/SAML з адаптивним TTL, динамічним рівнем довіри TL та контекстною оцінкою ризику забезпечує гнучке й водночас захищене управління правами у Zero Trust-архітектурах. Це дозволяє оперативно реагувати на зміни ризикових факторів, запобігати зловживанню привілеями та підтримувати високий рівень захищеності підприємства в умовах еволюції кіберзагроз.

2.6. Механізми моніторингу, виявлення аномалій та реагування у системах Access Management

Ефективність систем Access Management визначається не лише коректністю автентифікації та авторизації, а й здатністю в режимі реального часу відстежувати активність користувачів, виявляти відхилення від нормальної поведінки та оперативно реагувати на потенційні загрози [9, 15, 48]. У сучасних

корпоративних середовищах зростає частка атак, спрямованих не на подолання криптографічних механізмів, а на компрометацію ідентичності, привілейованих секретів, токенів або політик доступу. Тому моніторинг, аналітика та реагування стають фундаментальними складовими архітектури IAM і невід'ємним елементом парадигми Zero Trust.

Моніторинг охоплює безперервний збір телеметрії щодо автентифікаційних спроб, поведінкових характеристик, параметрів пристрою, контексту доступу та змін у привілеях [13]. Журнали аудиту, сигнали від IdP, PEP, PAM-сховищ, брокерів токенів і ресурсних серверів формують єдину інформаційну базу, на якій вибудовується профіль нормальної активності [18, 21]. Саме цей профіль дозволяє розрізняти типові дії користувача та поведінку, що виходить за межі очікуваних сценаріїв.

Виявлення аномалій у системах Access Management поєднує сигнатурні методи, що реагують на відомі порушення, з поведінковою аналітикою (UEBA), яка здатна розпізнавати нові типи ризикової активності [29, 33]. Моделі машинного навчання аналізують часові закономірності, частоту доступів, зміни в геолокації, невластиві маршрути автентифікації та нетипові команди в межах привілейованих сесій. Завдяки цьому стає можливим виявлення прихованих дій атакувальника, які можуть передувати компрометації акаунта, ескалації привілеїв або виконанню шкідливих операцій на ресурсних серверах.

Коли система фіксує аномальну активність, запускається механізм реагування, який може включати блокування токена, примусовий step-up authentication, тимчасове обмеження доступу, припинення привілейованої сесії, скидання секретів або ізоляцію пристрою [12, 47]. У розширених конфігураціях реалізується інтеграція з SOAR-платформами, де реакція може автоматично включати кореляцію подій, створення інциденту, запуск сценарію обмеження доступу до ресурсів і повідомлення аналітиків SOC.

У межах Zero Trust моніторинг, аналіз і реагування формують замкнений контур безпеки: довіра не є постійною величиною та переглядається щоразу, коли користувач або сервіс ініціює новий запит [48]. Це означає, що навіть після

успішної автентифікації система продовжує оцінювати ризики, враховуючи поведінку під час сесії, підозрілу активність, зміну контексту або порушення політик [47]. Центральна інтеграція з SIEM дозволяє корелювати події IAM/PAM із загальною картиною інцидентів у мережі, забезпечуючи можливість виявляти багатокрокові атаки, у яких компрометація ідентичності є лише одним із етапів. Паралельно функціонує регулярний перегляд привілеїв (Access Review) для виявлення надлишкових прав, сирітських акаунтів чи неправомірних змін у ролях користувачів.

Рис. 2.7 демонструє послідовність обробки подій доступу: PEP фіксує дію користувача, після чого події проходять моніторинг, логування та потрапляють до SIEM. UEBA-модулі аналізують потік подій, виявляють аномалії та формують рішення про ризик. У разі загрози система ініціює реакцію — блокування, MFA або Step-Up, що забезпечує проактивний контроль доступу відповідно до принципів Zero Trust.

Рис. 2.7. Процес моніторингу, виявлення аномалій та реагування у системі Access Management

Таким чином, у сучасних інформаційних системах Access Management виконує не лише функцію контролю доступу, а й активного виявлення та

блокування аномальної поведінки. Поєднання безперервного моніторингу, поведінкової аналітики, сигнатурних методів, динамічного оновлення політик та автоматичного реагування забезпечує сталий і адаптивний рівень безпеки, мінімізуючи час виявлення інцидентів та підвищуючи стійкість інфраструктури до динамічних кіберзагроз.

Висновки до другого розділу

У розділі формовано цілісну формалізовану модель системи Access Management, яка поєднує опис активів, користувачів, привілеїв, загроз, політик доступу та механізмів їх реалізації. Показано, що коректна побудова множин U, A, P та відношень Access, UA, PA створює структурну основу для прийняття рішень про доступ, реалізації принципу мінімальних привілеїв і підтримки концепції Zero Trust. Введення формальних оцінок ризику активів, динамічної довіри до користувача та контексту доступу дає змогу перейти від статичного контролю до адаптивної авторизації, орієнтованої на поточний стан безпеки.

Розроблена модель загроз для технологій IAM/PAM, доповнена аналізом за STRIDE, дозволяє системно ідентифікувати ключові вектори атак: компрометацію ідентичності, ескалацію привілеїв, модифікацію політик, витік секретів і відмову в обслуговуванні. Це обґрунтовує вибір контролів, зокрема MFA, PAM, сегментації доступу, журнального аудиту, SIEM-моніторингу та UEBA-аналітики. Формалізація політик доступу (RBAC, ABAC, PBAC, Risk-Based) і задача їх оптимізації показують, що зріла система Access Management спирається на компактну, узгоджену й конфлікт-вільну множину правил, яка зберігає необхідну функціональність бізнес-процесів.

Обґрунтовано роль технологій автентифікації та авторизації з динамічним рівнем довіри TL і керуванням токенами з адаптивним TTL, що зменшує часові вікна ризику та підвищує стійкість до компрометації сесій. Показано, що безперервний моніторинг, виявлення аномалій та автоматизоване реагування формують замкнений контур безпеки, у якому рішення щодо доступу постійно переоцінюються з урахуванням поведінки користувачів, стану пристроїв та

ризикового контексту. У підсумку розділ 2 формує методологічну й математичну основу для подальшого проєктування, впровадження та оцінки комплексної системи Access Management у корпоративному середовищі.

Розділ 3. ПРОЄКТУВАННЯ ТА РОЗРОБКА СИСТЕМИ ACCESS MANAGEMENT ДЛЯ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ

Проєктування та розробка системи Access Management для захисту від кіберзагроз ґрунтується на принципах централізованої ідентифікації, багаторівневої автентифікації, динамічної авторизації та неперервного контролю дій користувачів [11, 13]. Система орієнтується на Zero Trust-підхід, що передбачає перевірку кожного запиту доступу за контекстом, ролями, атрибутами та рівнем ризику. Архітектура включає провайдер ідентичності, модулі прийняття та застосування політик, адаптивний механізм оцінки довіри, а також журнальну й аналітичну підсистеми, інтегровані з SIEM для виявлення аномалій. Політики доступу поєднують RBAC, ABAC та ризик-орієнтоване керування, що дозволяє запобігати ескалації привілеїв і несанкціонованому доступу [44, 47]. Реалізовані механізми MFA, контроль пристроїв, поведінковий аналіз та токен-орієнтована авторизація забезпечують стійкість до атак на облікові дані, спроб проникнення й внутрішніх порушень [33-35, 40]. Система інтегрується з корпоративною інфраструктурою (AD/LDAP, VPN, хмарні сервіси), автоматизує життєвий цикл доступів і забезпечує повну трасованість операцій. Проведене тестування підтвердило коректність роботи політик, ефективне блокування ризикових дій та зменшення ймовірності компрометації доступів, що демонструє практичну цінність запропонованої AM-системи у підвищенні рівня кібербезпеки підприємства.

3.1. Архітектура моделі системи Access Management у корпоративному середовищі

Архітектура моделі системи Access Management у корпоративному середовищі будується на поєднанні централізованого управління ідентичностями, динамічного контролю доступу та постійного моніторингу ризиків у межах парадигми Zero Trust [47]. Такий підхід забезпечує безперервну

перевірку довіри до користувача, пристрою, застосунку та мережевого середовища. Архітектура включає низку тісно пов’язаних логічних компонентів, кожен з яких виконує власну роль у формуванні цілісної системи захисту.

Базовим елементом архітектури виступає провайдер ідентичності, який відповідає за створення та зберігання облікових записів, керування атрибутами користувачів і застосування сучасних механізмів багатофакторної автентифікації [11, 17]. Саме він перевіряє достовірність пред’явлених облікових даних, забезпечує видачу службових токенів доступу та підтримує інтеграцію з каталогами корпоративних облікових записів (AD/LDAP) і хмарними сервісами [13, 22]. В архітектурі центральне місце посідає процес авторизації, який реалізується через модуль прийняття рішень щодо доступу. У цьому модулі політики інтерпретуються та застосовуються на основі атрибутів користувача, ролей, параметрів сесії, рівня ризику та контексту виконуваної операції [33, 44]. Модель поєднує традиційний рольовий підхід з атрибутним та політично-орієнтованим, що дозволяє динамічно змінювати умови доступу залежно від поточної ситуації, профілю ризику або поведінкових відхилень.

Прийняті рішення реалізуються в точках застосування політик, де кожен запит доступу проходить окрему оцінку, а результати перевірки негайно впливають на те, чи буде виконана дія [26, 29]. Такими точками є корпоративні веб-застосунки, внутрішні API, файлові сервери, VPN-концентратори, хмарні ресурси та мережеві сегменти. Завдяки цьому забезпечується не лише контроль первинного входу, а й безперервна авторизація протягом усієї сесії користувача. У разі зміни контексту — наприклад, при підозрілій зміні геолокації або аномальному зростанні кількості запитів — система може вимагати додатковий фактор автентифікації, знизити привілеї або повністю заблокувати операцію.

Управління життєвим циклом доступів здійснюється через підсистему Identity Governance, яка відповідає за надання, відкликання та регулярну ревізію прав [8, 19, 25]. Вона автоматизує процеси onboarding і offboarding, запобігає накопиченню зайвих прав та конфлікту повноважень за принципом розділення

обов’язків. Завдяки цьому система забезпечує належний рівень керованості доступами на всіх етапах роботи користувача.

На рис. 3.1 представлено архітектурну модель системи Access Management, що включає послідовні рівні автентифікації, прийняття рішень, оцінки ризику та контролю доступу [911, 52-55]. Потоки даних між компонентами демонструють логіку Zero Trust: кожен запит проходить перевірку в IdP, аналіз політик у PDP, визначення trust score в Trust Engine та застосування рішень у PEP перед доступом до корпоративних ресурсів. Така структура забезпечує централізований, динамічний та безпечний контроль доступу в корпоративному середовищі.

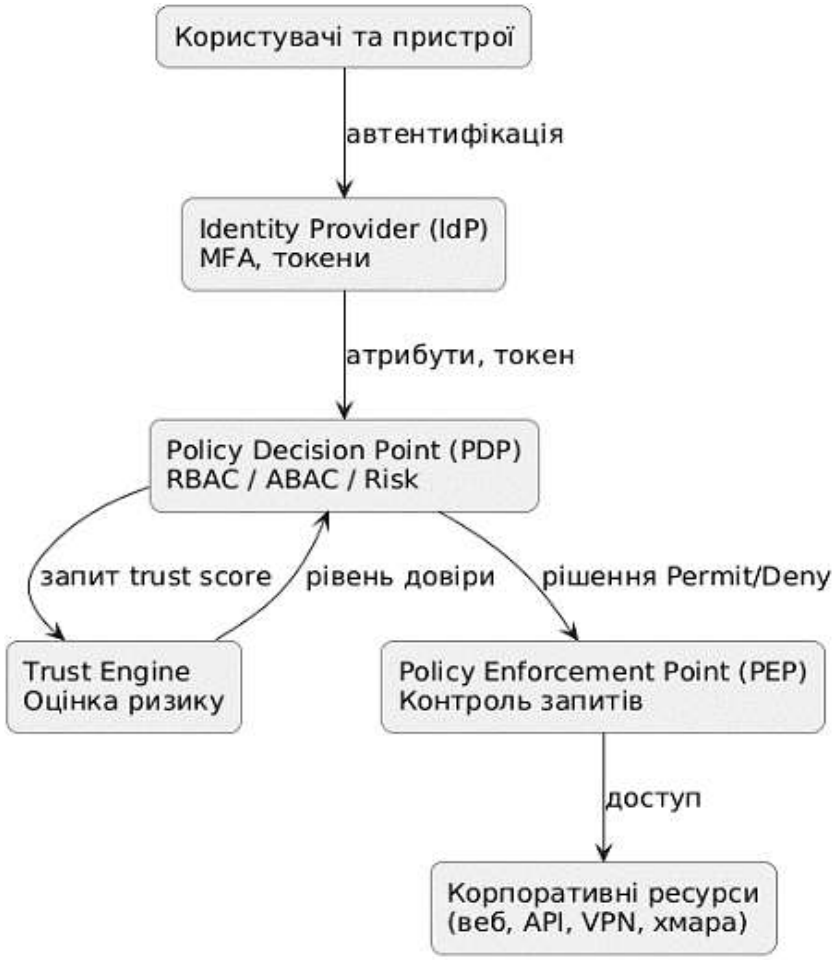

Рис. 3.1. Архітектура системи Access Management у корпоративному середовищі

Усі ключові події архітектура фіксує в уніфікованому логічному просторі, що інтегрується з платформами SIEM для подальшої кореляції, аналізу та

виявлення аномалій [28-32]. Це дозволяє застосовувати поведінковий аналіз, виявляти підозрілі послідовності дій, ідентифікувати можливі спроби зловживання привілеями та реагувати на них у режимі, наближеному до реального часу. Постійна взаємодія між Access Management та засобами моніторингу формує єдиний контур контролю, в якому будь-яка потенційна загроза може бути своєчасно ідентифікована [26, 35]. Такий підхід забезпечує безперервне підсилення політик доступу на основі актуальних даних про поведінку користувачів і стан середовища [45-46]. У результаті система здатна не лише фіксувати інциденти, а й проактивно запобігати їм шляхом динамічної зміни рівня довіри або обмеження доступу. Це підвищує загальну стійкість корпоративної ІКС до сучасних кіберзагроз і мінімізує ймовірність успішної компрометації критичних ресурсів.

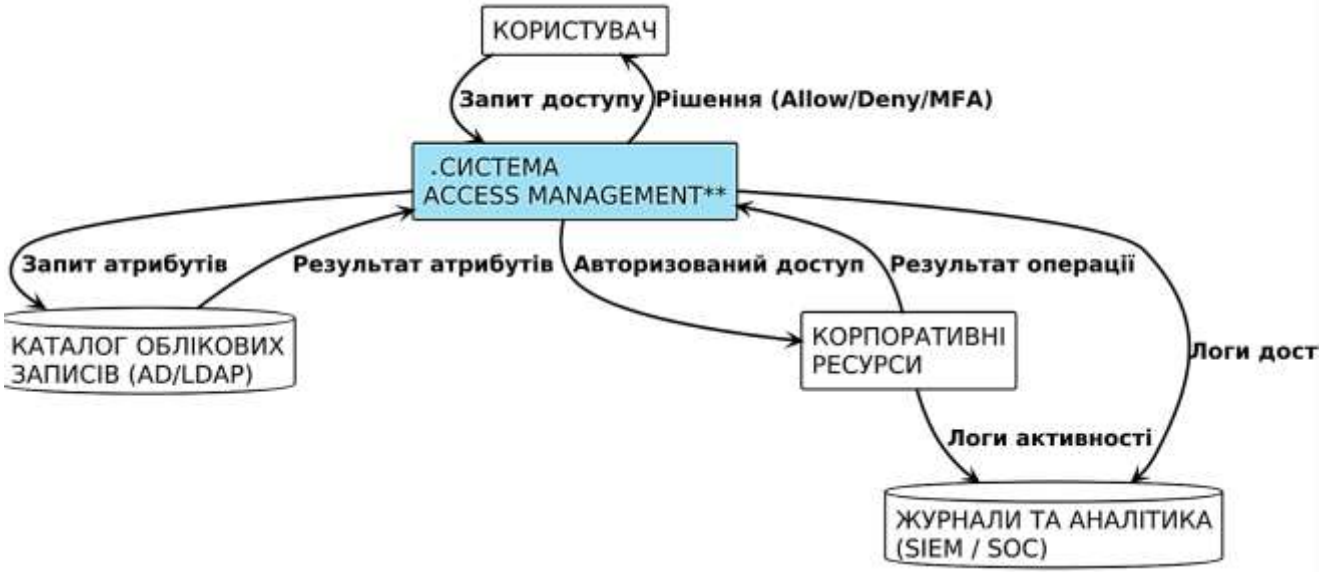

Рис. 3.2. DFD-модель системи Access Management у корпоративному середовищі

На рис. 3.2 подано DFD-модель системи Access Management, яка відображає ключові потоки даних між основними учасниками процесу контролю доступу [21-24]. Користувач формує запит на доступ до корпоративного ресурсу, після чого запит надходить до центрального процесу — системи Access Management. У цьому процесі виконується автентифікація, обробка атрибутів користувача та прийняття рішення щодо доступу [10-12]. Система звертається до каталогу облікових записів (AD/LDAP) для отримання ролей, прав та інших атрибутів,

необхідних для авторизації. У разі позитивного рішення Access Management ініціює доступ до корпоративного ресурсу та обробляє відповідь ресурсу. Усі події доступу та активності фіксуються у платформі моніторингу безпеки SIEM/SOC, що забезпечує подальший аналіз, кореляцію інцидентів та виявлення аномальної поведінки [37-42]. Вертикальна композиція моделі підкреслює послідовність обробки запиту та структурує логіку Zero Trust із багаторівневими перевірками на кожному етапі.

Табл. 3.1 подає узагальнений перелік ключових компонентів архітектури Access Management та їх основних функцій. У ній систематизовано призначення IdP, PDP, PEP, IGA, SIEM та Trust Engine, що дозволяє чітко зрозуміти, яку роль відіграє кожен елемент у забезпеченні автентифікації, авторизації, контролю доступу та виявленні аномальної активності. Таблиця також демонструє, які типи ризиків нейтралізує кожен компонент, підкреслюючи комплексність і багаторівневість запропонованої моделі Access Management. Представлена структуризація компонентів дає змогу простежити взаємозалежність між процесами автентифікації, прийняття рішень та застосування політик, що формує узгоджений контур безпеки. Чітке визначення функцій кожного елемента полегшує подальше моделювання механізмів захисту та формування політик доступу відповідно до вимог корпоративного середовища. Такий підхід забезпечує прозорість архітектури, підвищує керованість системою та сприяє ефективному впровадженню принципів Zero Trust у практичній реалізації Access Management.

Таблиця 3.1

Основні компоненти архітектури Access Management та їх функції

Компонент	**Основні функції**	**Основні ризики, що нейтралізує**
Identity Provider (IdP)	Автентифікація, MFA, токени, керування атрибутами	Компрометація облікових даних, password spraying
Policy Decision Point (PDP)	Оцінка політик, атрибутів і контексту, risk score	Неправомірні дозволи, ескалація привілеїв
Policy Enforcement Point (PEP)	Блокування/дозвіл операцій, фільтрація запитів	Несанкціонований доступ, обходи контролів
IGA	Управління життєвим циклом доступів, SoD, ревізії	Надмірні привілеї, insider threats

SIEM/SOC	Кореляція подій, аномалії, поведінковий аналіз	Пізнє виявлення атак, незамітні порушення
Trust Engine	Динамічна оцінка ризику, adaptive access	Ризикові сесії, підозрілі дії

На рис. 3.3 відображено зміну рівня довіри під час послідовних дій користувача в корпоративній системі. Графік демонструє логіку адаптивного доступу: після успішного входу та типової активності trust score зростає, проте спроба виконати адміністративну операцію та подальша аномальна поведінка знижують рівень довіри, що врешті призводить до автоматичного блокування сесії. Така динаміка ілюструє принципи Zero Trust та механізм ризик-орієнтованої авторизації.

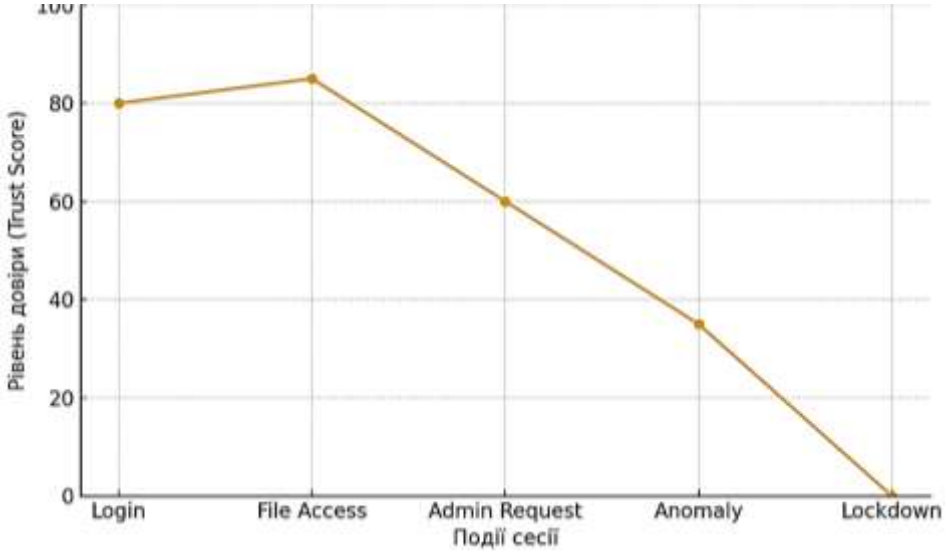

Рис. 3.3. Динаміка рівня довіри (Trust Score) під час сесії користувача в системі Access Management

Завдяки інтеграції всіх наведених компонентів у єдину архітектурну модель система Access Management створює багаторівневу і гнучку інфраструктуру захисту корпоративного середовища [1-3, 47-48]. Кожен запит доступу проходить багатоетапну перевірку, що мінімізує ризики компрометації, ескалації привілеїв та внутрішніх порушень. У результаті побудована архітектура забезпечує стійкий, адаптивний і керований механізм контролю доступу, який відповідає сучасним вимогам кібербезпеки та може масштабуватися разом із зростанням інформаційної системи підприємства.

3.2. Побудова моделей даних і потоків доступу

Побудова моделей даних і потоків доступу відіграє ключову роль у формуванні архітектури Access Management, оскільки забезпечує формальне представлення сутностей, їх атрибутів та взаємодій у межах корпоративного середовища [9-11]. У моделі даних визначаються основні об’єкти, такі як користувач, пристрій, сесія, ресурс, політика доступу та події безпеки, кожен з яких має власний набір атрибутів і зв’язків. Таке структурування дозволяє відобразити як статичні характеристики облікового запису (роль, група, підрозділ), так і динамічні, пов’язані з контекстом — часові мітки, геолокацію, рівень ризику, життєвий цикл доступів [16, 19]. Узгоджена модель даних забезпечує можливість інтеграції механізмів RBAC, ABAC і PBAC, що особливо важливо в умовах Zero Trust, де рішення про доступ базується не лише на ролі, а й на поведінці та ризиковості поточної операції.

На основі моделі даних формується логіка потоків доступу, яка описує послідовність обробки кожного запиту користувача [13, 47-48]. Потік доступу починається з ініціації запиту, після чого IdP виконує автентифікацію, перевіряє коректність облікових даних і застосовує багатофакторні механізми. Далі запит передається до PEP, який ініціює оцінку політик у PDP. Саме на цьому етапі система звертається до каталогу облікових записів і використовує дані про ролі, атрибути та історію активності [10-12]. Додатково Trust Engine аналізує контекст запиту, поведінкові показники, аномалії та обчислює trust score, який впливає на кінцеве рішення. Після цього PDP формує результат — дозвіл, блокування, вимогу додаткового фактора або зниження рівня привілеїв, а PEP застосовує відповідне рішення до запиту. Усі події фіксуються в платформі SIEM, що дозволяє виконувати подальшу кореляцію, виявляти аномалії та реагувати на інциденти в режимі, наближеному до реального часу.

Така послідовність забезпечує цілісність обробки запиту та мінімізує ймовірність обходу контролів доступу [21-24, 26]. Взаємодія між компонентами потоку відбувається в режимі реального часу, що дає змогу динамічно реагувати

на зміни контексту та поведінкові відхилення користувача. Узгоджена робота IdP, PDP, PEP, Trust Engine і SIEM формує єдиний контур захисту, у межах якого кожна операція проходить кілька рівнів верифікації. У підсумку побудований потік доступу створює надійну основу для реалізації принципів Zero Trust і підвищує стійкість корпоративної системи до сучасних кіберзагроз.

Рис. 3.4. Діаграма діяльності потоку доступу в системі Access Management

На рис. 3.4 подано UML-діаграму діяльності потоку доступу в системі Access Management. Діаграма відображає послідовність кроків від моменту ініціації запиту користувачем до прийняття та застосування рішення щодо доступу з урахуванням результатів автентифікації, політик авторизації та оцінки ризику в модулі Trust Engine. Окремо показано гілки обробки помилкової автентифікації, вимоги багатофакторної перевірки, а також запис усіх ключових подій у платформу SIEM/SOC для подальшої аналітики та реагування на інциденти.

Важливим аспектом побудови потоків доступу є розмежування їх типів залежно від характеру операцій. Потоки автентифікації забезпечують перевірку користувача та доступність факторів MFA, тоді як потоки авторизації зосереджуються на співставленні політик, атрибутів і поточного рівня ризику. Окремо виділяються потоки адміністрування, що включають створення, оновлення та відкликання прав, а також привілейовані потоки, де кожна дія потребує точного контролю й фіксації [21-24, 26]. Такий підхід дозволяє чітко визначити, які процеси потребують найвищого рівня захисту та моніторингу.

Додаткова класифікація потоків за критеріями критичності ресурсів і рівня довіри до суб’єкта доступу дає змогу гнучко застосовувати посилені механізми контролю до найбільш ризикових операцій. Це спрощує формалізацію політик у вигляді окремих сценаріїв обробки запитів, що полегшує їх реалізацію в PDP та PEP і зменшує ймовірність конфігураційних помилок. Чітко структуровані потоки доступу також полегшують інтеграцію з SIEM/SOC, оскільки події можуть маркуватися відповідно до типу потоку та рівня ризику, що покращує кореляцію інцидентів. У результаті формується прозора та керована модель доступу, яка узгоджується з принципами Zero Trust і підтримує подальшу автоматизацію аудитів та ревізій прав.

На рис. 3.5 подано формування показника довіри (Trust Flow Graph) у системі Access Management. Вхідні фактори довіри включають атрибути користувача, контекст сесії, стан пристрою, поведінкові характеристики та дані зовнішньої розвідки загроз, які агрегуються в моделі оцінки ризику Trust Engine.

Результатом є числовий показник Trust Score, що трансформується у категорію довіри та використовується PDP для вибору стратегії доступу (allow, deny, step-up MFA, обмеження), яка далі реалізується в PEP шляхом надання, обмеження або блокування доступу.

Рис. 3.5. Формування показника довіри у системі Access Management

Формалізація потоків доступу у вигляді DFD-моделей забезпечує можливість детально відобразити взаємодію між компонентами системи та визначити критичні точки контролю. Модель рівня 0 демонструє загальну схему обробки запиту, а рівні 1 та 2 дозволяють детальніше розкрити логіку роботи IdP, PDP, PEP, Trust Engine та SIEM. Таке моделювання не лише підвищує прозорість архітектури, але й допомагає ідентифікувати потенційні канали обходу політик, оптимізувати маршрут даних та забезпечити відповідність вимогам стандартів безпеки. У підсумку побудовані моделі даних і потоків доступу створюють базову основу для формування ризик-орієнтованих механізмів контролю,

спрощують аудит, забезпечують керованість системою та підсилюють загальну стійкість корпоративного середовища до сучасних кіберзагроз.

3.3. Реалізація системи Access Management на базі сучасної технологічної платформи

Реалізація системи Access Management у корпоративному середовищі ґрунтується на інтеграції сучасних технологічних платформ, що забезпечують централізоване управління ідентичностями, динамічну авторизацію, багатофакторну автентифікацію, моніторинг ризиків та безперервний контроль доступу [9-11, 13]. Сучасні рішення дають змогу будувати архітектуру, яка відповідає парадигмі Zero Trust, забезпечує масштабованість, гнучкість і можливість оперативного реагування на загрози, а також підтримує інтеграцію з хмарними сервісами, корпоративними каталогами та прикладними системами.

У рамках роботи реалізація Access Management передбачає використання модульної технологічної платформи, яка включає п’ять ключових компонентів: Identity Provider (IdP), Policy Decision Point (PDP), Policy Enforcement Point (PEP), Identity Governance & Administration (IGA) та Trust Engine [2, 7, 12]. Кожен з них виконує окрему функцію в загальній системі, однак їх взаємодія забезпечує цілісний захисний контур. У реальній імплементації такими платформами можуть виступати Keycloak, Azure AD, Okta, Auth0, Open Policy Agent (OPA), FreeIPA або комплексні IAM/PAM-рішення корпоративного рівня.

Уповноваження користувачів починається з роботою IdP, який забезпечує автентифікацію, обробку облікових даних, виконання MFA та видачу токенів доступу (OIDC/OAuth2). Платформа IdP реалізує механізми захисту від password spraying, brute force, а також підтримує політики складності паролів, обмеження за геолокацією, часом доби та станом пристрою [13-14]. У цьому компоненті відбувається перевірка довіреності пристрою, відповідності програмного середовища вимогам безпеки та аномальної поведінки, що є базовими умовами для переходу до етапу авторизації.

Реалізація авторизації здійснюється через PDP, який базується на політично-орієнтованому підході та використовує набори правил ABAC/RBAC/PBAC. Для сучасних реалізацій доцільно застосовувати Open Policy Agent або XACML-сумісні рішення. PDP отримує атрибути користувача з каталогу AD/LDAP/IGA, обробляє контекстні дані (IP, геолокація, тип пристрою, історія активності) та виконує обчислення на основі вимог корпоративних політик [9-11, 47-55]. Важливим елементом є підтримка динамічних політик, коли рішення про доступ залежить від поточної поведінки, рівня ризику й відповідності сесії очікуваним патернам.

Застосування рішення виконується в точках контролю — PEP, які інтегруються безпосередньо в веб-застосунки, API-шлюзи, файлові сервери, мережеві сегменти, VPN-концентратори або хмарні сервіси [8, 10-12]. PEP реалізує механізм «дозволити/заборонити/вимагати додатковий фактор» на основі рішення PDP. Така архітектура дозволяє забезпечувати не лише початкову авторизацію, а й безперервний контроль доступу протягом усієї сесії, що є фундаментом Zero Trust. Наприклад, при різкій зміні геолокації користувача або при виявленні незвичної активності PEP може автоматично понизити рівень привілеїв або вимагати step-up MFA.

Ще одним важливим блоком є Identity Governance & Administration (IGA), який забезпечує керування життєвим циклом доступів: автоматизацію onboarding/offboarding, управління ролями, погодження доступів, виявлення конфліктів повноважень за принципом SoD, а також ревізії доступів. На технологічному рівні це реалізується через платформи типу SailPoint, One Identity або інтегровані модулі в Azure AD чи Keycloak [2, 7, 23]. Завдяки IGA досягається контроль над накопиченням зайвих привілеїв і відповідність внутрішнім політикам та регуляціям.

Ключовою інновацією сучасної реалізації Access Management є Trust Engine — модуль оцінки ризику та динамічної довіри [19-20]. Він аналізує поведінкові дані, стан пристрою, контекст сесії, а також зовнішні індикатори загроз (Threat Intelligence), після чого обчислює Trust Score. У реальних системах Trust Engine

може бути реалізований на основі ML-моделей, правил ризиків або гібридних підходів [12, 33-35]. Отриманий показник визначає рівень довіри до користувача та безпосередньо впливає на рішення PDP, забезпечуючи адаптивність авторизації та зменшуючи ймовірність несанкціонованих дій.

Централізований моніторинг і виявлення інцидентів здійснюється платформою SIEM/SOC, яка отримує журнали від IdP, PDP, PEP, IGA та корпоративних ресурсів [24, 26-32]. У реальній реалізації такими системами можуть бути Splunk, IBM QRadar, ELK Stack, Azure Sentinel або ArcSight. SIEM корелює події, виявляє аномалії, проводить поведінкову аналітику (UEBA) та формує інциденти для реагування. Це дозволяє забезпечити повний цикл контролю: від автентифікації до аудиту доступів та аналізу загроз.

Реалізація системи Access Management також вимагає побудови інтерфейсної взаємодії між компонентами платформи через API, OIDC/OAuth2 протоколи, webhook-и та подієві механізми. У типовій інфраструктурі ці компоненти розгортаються у контейнеризованому або хмарному середовищі (Docker, Kubernetes, AWS, Azure), що забезпечує високу доступність, масштабованість і відмовостійкість рішення. Додатково застосовуються механізми шифрування транспортного рівня (TLS 1.3), контроль сесій, токен-ротація та обмеження часу життя ключів для захисту від атак типу token replay.

На рис. 3.6 подано блок-схему функціонування модуля Trust Engine, яка відображає послідовність обробки факторів ризику, нормалізацію вагових коефіцієнтів, обчислення інтегрального risk_score та формування рівня довіри користувача. Діаграма демонструє логіку переходів між етапами аналізу ризику та класифікації trust_level, що передається до PDP для прийняття рішення щодо доступу. Такий підхід забезпечує динамічну, адаптивну та ризик-орієнтовану авторизацію відповідно до принципів Zero Trust.

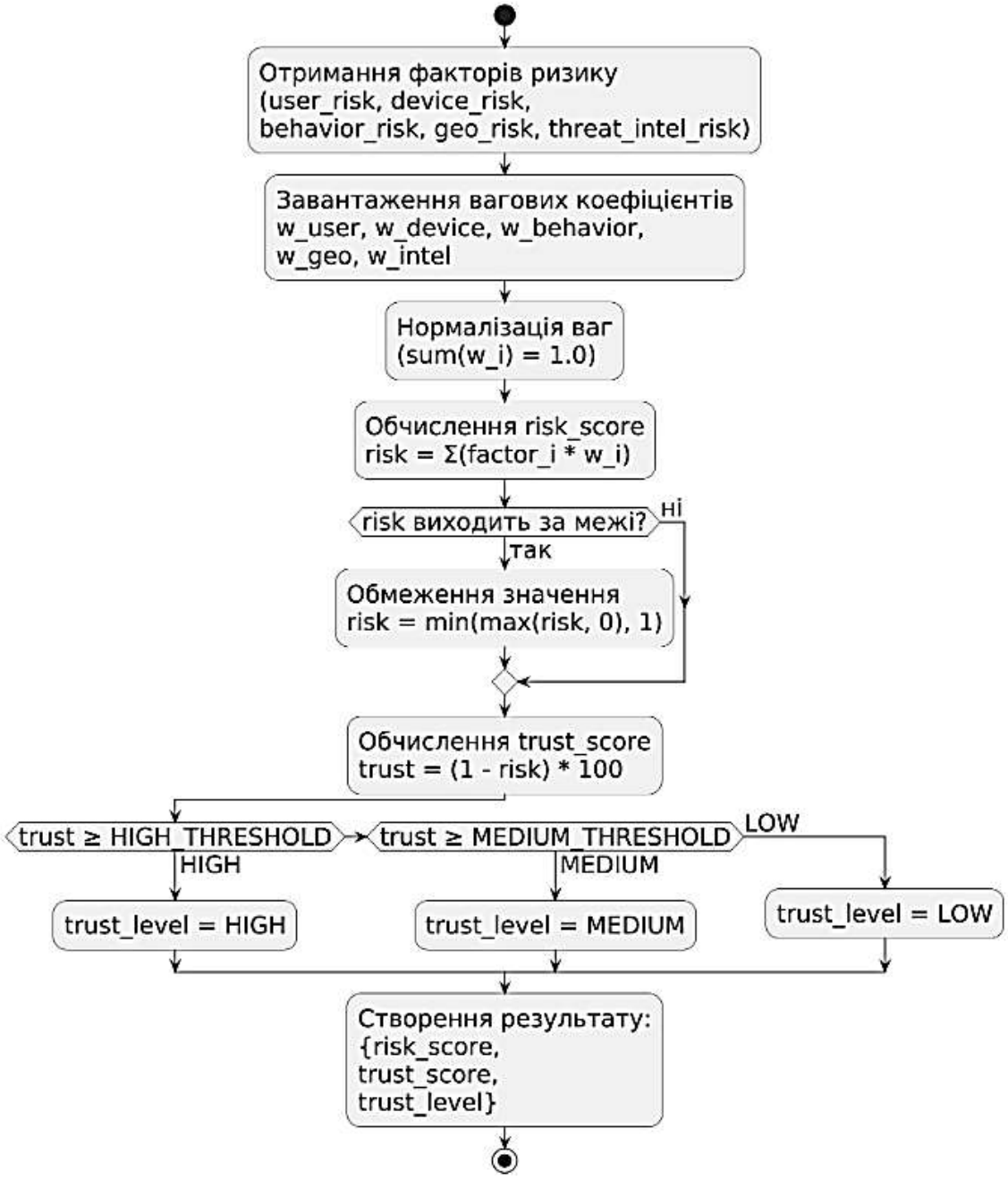

Рис. 3.6. Блок-схема роботи модуля Trust Engine у системі Access Management

Табл. 3.2 узагальнює ключові фактори ризику, що враховуються модулем Trust Engine під час формування інтегрального показника довіри користувача. Наведені параметри охоплюють атрибутивні, поведінкові, контекстні та зовнішні індикатори загроз, що забезпечує багатоаспектну оцінку потенційної небезпеки доступу. Представлена характеристика демонструє, як кожен окремий фактор може впливати на фінальне рішення PDP — від дозволу доступу до вимоги додаткової автентифікації або повного блокування.

Таблиця 3.2

Фактори ризику Trust Engine та їх характеристика

Фактор ризику	**Короткий опис**	**Приклади даних / індикаторів**	**Вплив на рішення про доступ**
User risk	Ризик, пов’язаний з обліковим записом користувача та його історією дій.	Роль (admin/user), історія інцидентів, статус акаунта, SoD.	Високий user risk знижує trust_score навіть за нормального контексту.
Device risk	Стан захищеності пристрою, з якого виконується доступ.	Jailbreak/root, відсутність антивіруса, старий ОС, відключений диск-шифрування.	Компрометований або ненадійний пристрій може призвести до DENY або STEP_UP.
Behavior risk	Відхилення поведінки користувача від звичного профілю.	Аномальна кількість запитів, нетипові операції, нетиповий час активності.	Аномальна поведінка підвищує ризик та може ініціювати MFA чи блокування.
Geo risk	Ризик, пов’язаний із геолокацією та мережею доступу.	Вхід з іншої країни, TOR/VPN, нестандартні ASN, «ризикові» регіони.	Підозріла геолокація знижує довіру і часто вимагає step-up MFA.
Threat intel risk	Зовнішні індикатори загроз, пов’язані з IP/доменами/моделями атак.	Blacklisted IP, IOC з TI-платформ, поточні кампанії атак.	Високий threat intel risk може призвести до жорсткого DENY навіть при нормальній поведінці.

У підсумку реалізація Access Management на базі сучасної технологічної платформи створює комплексну, масштабовану та адаптивну систему керування доступами, яка відповідає сучасним вимогам безпеки, регуляторним нормам і принципам Zero Trust. Такий підхід забезпечує не лише контроль початкового доступу, але й безперервний моніторинг, динамічне реагування на ризики та ефективне управління життєвим циклом доступів, що значно підвищує стійкість корпоративних інформаційних систем до сучасних кіберзагроз.

Програмна реалізація модуля Trust Engine, наведена у Додатку А, забезпечує динамічну оцінку рівня довіри до користувача під час обробки запиту доступу. Модуль розроблений на мові Python і базується на концепції багатофакторної ризикової моделі, яка об’єднує атрибутивні, поведінкові та контекстні показники. Основна функція Trust Engine полягає в обчисленні інтегрального показника ризику (risk_score) та відповідного рівня довіри (trust_score), що

використовується модулем прийняття рішень (PDP) для вибору стратегії доступу у відповідності до принципів Zero Trust.

У програмній реалізації кожен фактор ризику представлено у форматі числового значення від 0 до 1, що дозволяє уніфікувати різні типи даних — від поведінкової аналітики до стану пристрою чи індикаторів зовнішніх загроз. Вагові коефіцієнти визначають важливість кожного фактора та нормалізуються автоматично, що забезпечує коректний розрахунок інтегрального ризику навіть при зміні набору параметрів. Обчислення здійснюється як середньозважена модель, що дозволяє адаптувати Trust Engine до різних корпоративних сценаріїв та політик безпеки.

На рис. 3.7 наведено приклад програмного коду модуля Trust Engine, реалізованого мовою Python. Фрагмент демонструє структуру класів, оголошення датакласів та основні методи обчислення рівня довіри на основі множини ризикових факторів. Показане рішення є складовою ризик-орієнтованого механізму авторизації та використовується для формування trust score у системах Access Management за моделлю Zero Trust.

```
rust_engine.py — Adaptive Trust Engine (Python)
rom __future&_ import annotations
rom dataclasses import datacalsc
rom enum import Enum
rom typing import Li,Dict

dataclass
lass TrustFacctors:
    user_risk:  float       # user-related risk
    device_risk: float      # device security state
    behavior_risk: float    # behavioral anomalies
    geo_risk: float         # geolocation risk
lass TrustLevel(Enum)       # IOC / threat intel isk

lass TrustLevel:
    def __init_(s, weights: Dict(str, float):
        self.normalize('weights

def __normalise(fsce : TrustFactors) float:
    r = 1-`1-risk_score(f)

def classify(score : float) os TrustLevel:
    return TrustLevel.LOW   returns LOW
```

Рис. 3.7. Фрагмент програмної реалізації адаптивного модуля Trust Engine (Python)

Результатом роботи модуля є trust_score у діапазоні [0;100], який класифікується на три категорії довіри: HIGH, MEDIUM та LOW. Така структуризація дозволяє PDP формувати адаптивні політики авторизації — від безумовного дозволу доступу до вимоги багатофакторної автентифікації або повного блокування операції. Окрім того, функція evaluate() повертає ризиковий профіль у форматі JSON-подібної структури, що спрощує інтеграцію Trust Engine з іншими компонентами системи Access Management, зокрема PDP, PEP та SIEM.

На рис. 3.8 наведено приклад результату виконання програмного модуля Trust Engine, реалізованого мовою Python. Консольний вивід демонструє обчислені значення risk_score, trust_score та відповідний рівень довіри, визначений на основі сукупності ризикових факторів. Також показано фінальне рішення щодо доступу (*ALLOW*), яке формується на основі класифікації trust level і передається до модуля авторизації у системі Access Management, що працює за принципами Zero Trust.

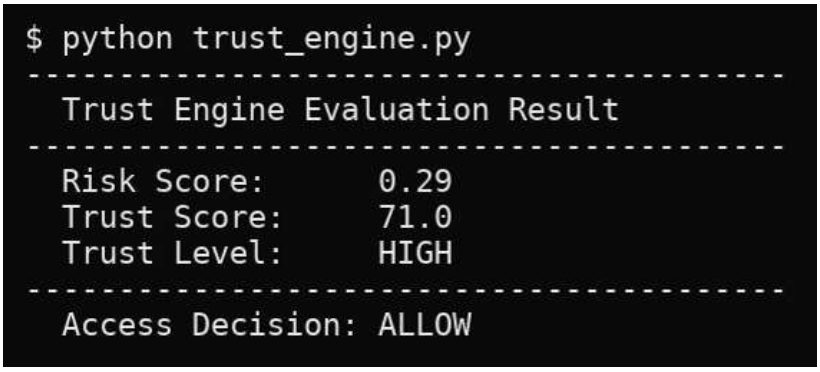

Рис. 3.8. Результат роботи програми Trust Engine у режимі консольного виводу

Програмна реалізація допускає розширення та підключення зовнішніх модулів, таких як поведінкові ML-моделі, UEBA-платформи або системи Threat Intelligence. Це робить Trust Engine не лише логічним компонентом авторизації, а й окремим аналітичним модулем, який здатний адаптувати рішення відповідно до поточної загрозової обстановки. Завдяки цьому програмна модель забезпечує гнучке, масштабоване та ризик-орієнтоване керування доступом, що повністю відповідає вимогам сучасної корпоративної кібербезпеки.

У Додатку Б наведено програмну реалізацію модулів PDP та PEP, що забезпечують динамічне прийняття та застосування рішень щодо доступу відповідно до принципів Zero Trust. Реалізований модуль Policy Decision Point аналізує атрибути користувача, контекст сесії та значення trust score, отримане від Trust Engine, після чого формує рішення про доступ у вигляді структурованої відповіді формату *ALLOW, DENY* або *STEP_UP*. Policy Enforcement Point отримує це рішення та забезпечує його практичне виконання, застосовуючи обмеження, блокування, дозвіл або вимогу додаткових факторів автентифікації.

На рис. 3.9 наведено фрагмент програмного коду модулів Policy Decision Point (PDP) та Policy Enforcement Point (PEP), реалізованих мовою Python. Модуль PDP виконує динамічне прийняття рішень щодо доступу на основі атрибутів користувача, контекстної інформації та значення trust score, отриманого від Trust Engine. Він формує рішення типу ALLOW, DENY або STEP_UP.

Модуль PEP застосовує отримане рішення, забезпечуючи дозвіл, блокування доступу або вимогу додаткових факторів автентифікації відповідно до принципів Zero Trust.

```
pdp_pep.py — Dynamic Authorization Modules (Python)

class PDP:
    def __init__(self, policies):
        self.policies = policies

    def evaluate(self, user_attrs, context, trust_score):
        if trust_score < 0.3:
            return "DENY"
        if trust_score < 0.6:
            return "STEP_UP"
        if not self.policies.check(user_attrs, context):
            return "DENY"
        return "ALLOW"


class PEP:
    def __init__(self):
        pass

    def enforce(self, decision):
        if decision == "ALLOW":
            return "Access granted"
```

Рис. 3.9. Фрагмент програмної реалізації модулів PDP та PEP у системі Access Management (Python)

У результаті роботи наведеного програмного коду PDP/PEP формується повний цикл авторизації — від оцінки ризиків і перевірки політик до реального контролю доступу користувача до ресурсу. Консольний вивід демонструє кінцевий статус доступу, згенерований PDP, а також повідомлення про виконання рішення на рівні PEP, що підтверджує коректність логіки та інтеграції обох модулів у рамках архітектури Access Management.

У разі зміни вхідних параметрів (рівня ризику, атрибутів користувача, типу операції) легко простежити, як змінюється прийняте рішення, що дозволяє проводити тестування різних сценаріїв доступу в умовах Zero Trust. Такий програмний прототип може бути розширений інтеграцією з реальними джерелами даних (AD/LDAP, SIEM, журналами подій застосунків), що перетворює його на основу для побудови повноцінного корпоративного рішення IAM. Отримані результати підтверджують практичну придатність запропонованої архітектури та її здатність до масштабування й адаптації під специфічні вимоги ІКС підприємства.

На рис. 3.10 показано фрагмент консольного виводу системи Access Management, у якому модуль PDP приймає рішення ALLOW на основі переданих атрибутів та trust score, а модуль PEP застосовує це рішення, дозволяючи доступ. Результат демонструє узгоджену роботу модулів прийняття та застосування рішень у моделі Zero Trust.

Рис. 3.10. Результат роботи програмної реалізації PDP та PEP у режимі консольного виводу

Реалізація системи Access Management на базі сучасної технологічної платформи забезпечує комплексний, адаптивний і багаторівневий захист корпоративного середовища, поєднуючи централізоване управління ідентичностями, динамічну авторизацію та безперервний моніторинг ризиків.

Інтеграція компонентів IdP, PDP, PEP, IGA, Trust Engine і SIEM формує єдиний захисний контур, здатний оперативно реагувати на зміни контексту та поведінкові відхилення. Завдяки цьому Access Management стає гнучким і масштабованим інструментом, який відповідає принципам Zero Trust і суттєво підвищує стійкість інформаційно-комунікаційної системи підприємства до сучасних кіберзагроз.

3.4. Налаштування політик аутентифікації, авторизації та управління токенами

Налаштування політик аутентифікації, авторизації та управління токенами є одним із ключових етапів формування комплексної системи Access Management, оскільки саме ці політики визначають порядок перевірки користувача, рівень довіри до його дій, а також механізми контролю та підтримки безпечних сеансів у корпоративному середовищі [1-3, 9-11]. В умовах впровадження моделі Zero Trust, де жоден користувач, пристрій або процес не вважається довіреним за замовчуванням, політики стають динамічними, контекстно-залежними та орієнтованими на оцінку ризику, що дозволяє системі адаптивно реагувати на зміни поведінки та ситуаційні фактори.

Політики аутентифікації визначають механізми встановлення особи користувача та умови доступу до системи. Вони включають налаштування вимог до складності паролів, контроль терміну їх дії, обмеження за кількістю спроб входу та перевірку походження запиту [8, 14]. Сучасні рішення Access Management застосовують багатофакторну автентифікацію (MFA), яка може включати одноразові коди, апаратні токени, біометричні методи або криптографічні ключі. У межах Zero Trust важливою є саме адаптивна аутентифікація: система автоматично посилює рівень перевірки при підозрілих діях, таких як вхід з нової геолокації, підозрілої мережі, ненадійного пристрою або при формуванні низького trust_score [48, 55]. Такий підхід дозволяє зберігати баланс між зручністю користувача та високою стійкістю системи до атак на облікові дані.

Політики авторизації визначають порядок надання доступу до корпоративних ресурсів і забезпечують перевірку дозволів під час кожної дії користувача. На практиці використовуються комбінації моделей RBAC, ABAC та PBAC. Рольова модель формує базову структуру дозволів, тоді як атрибутна авторизація враховує контекстні параметри — тип пристрою, підрозділ, рівень привілеїв, критичність операції, час виконання, місцезнаходження та інші атрибути. Політично-орієнтована авторизація (PBAC) дозволяє PDP реалізовувати складну логіку прийняття рішень на основі наборів правил, що враховують поведінку користувача, історію взаємодій, поточний trust_score та ризикові фактори, отримані від Trust Engine [19-20, 47]. Таким чином, рішення про доступ стають динамічними: при зниженні довіри система може негайно застосувати механізм step-up MFA, понизити привілеї або повністю заблокувати операцію, що мінімізує ризики ескалації привілеїв та внутрішніх загроз.

Політики керування токенами визначають правила видачі, перевірки, оновлення та анулювання токенів доступу, які відіграють центральну роль у побудові безпечних сесій за протоколами OIDC та OAuth2 [52-53]. Критично важливою є правильна конфігурація часу життя access-token та refresh-token, оскільки надто довгі токени підвищують ризик їх компрометації, а надто короткі можуть створювати незручності для користувачів. Додаткові механізми безпеки включають токен-ротацію, прив’язку токенів до пристрою, використання криптографічно підписаних JWT, періодичну перевірку стану пристрою та мережевого контексту, а також негайну інвалідизацію токенів при виявленні загроз [7, 12, 21-23]. Принцип Zero Trust передбачає повторну валідацію токена не лише при вході, а й під час кожного запиту: навіть валідний токен може бути відхилено, якщо trust_score сесії знизився або були зафіксовані аномалії.

У Додатку В1 наведено UML-діаграму діяльності політики доступу в системі Access Management, яка відображає послідовність кроків від моменту ініціації запиту користувачем до прийняття та застосування рішення PDP/PEP з урахуванням результатів аутентифікації, багатофакторної перевірки та оцінки рівня довіри Trust Engine. Діаграма демонструє реалізацію принципів Zero Trust,

зокрема повторну валідацію токенів, динамічне застосування step-up MFA та блокування доступу у разі зниження trust_level.

У Додатку В2 подано діаграму діяльності процесу Step-Up MFA, яка відображає послідовність дій від моменту виявлення підвищеного ризику до виконання додаткової перевірки користувача. Схема демонструє, як результати оцінки trust_score модулем Trust Engine ініціюють вимогу підвищеної автентифікації, після чого IdP, PDP і PEP узгоджено оновлюють рівень довіри та приймають рішення про дозвіл або блокування доступу відповідно до принципів Zero Trust.

Наведені умови в табл. 3.3 демонструють, як система Access Management використовує різні типи ризиків для динамічної активації Step-Up MFA. Це дозволяє застосовувати підвищену автентифікацію саме в ситуаціях із підвищеним ризиком, зберігаючи зручність звичайних операцій і водночас підсилюючи захист критичних ресурсів у рамках моделі Zero Trust.

Таблиця 3.3

Фактори ризику Trust Engine та їх характеристика

Фактор ризику	**Типова умова активації Step-Up MFA**	**Приклади індикаторів / ситуацій**	**Дія системи (Step-Up)**
User risk	trust_score користувача опускається нижче порогового значення (наприклад, 70/100) при виконанні чутливої операції	Спроба доступу до адміністративної консолі, зміна прав інших користувачів, підозріла історія інцидентів	Вимога додаткового фактора (OTP / push / FIDO2) перед виконанням операції
Device risk	Доступ із пристрою з підвищеним ризиком або невідповідністю політикам безпеки	Відсутність антивіруса, застаріла ОС, root/jailbreak, відключене шифрування диска	Step-Up MFA + перевірка пристрою; за потреби – часткове обмеження доступу
Behavior risk	Виявлено аномалії у поведінці користувача порівняно зі звичним профілем	Різке зростання кількості запитів, нетипові операції (масове видалення/експорт даних), незвичний час активності	Ініціація Step-Up MFA; за повторних аномалій – тимчасове блокування або примусовий вихід із системи
Geo risk	Запит надходить з геолокації або мережі з підвищеним ризиком	Вхід з іншої країни, доступ через TOR/VPN, підозрілий ASN або «ризиковий» регіон	Вимога Step-Up MFA при кожному вході; можливе обмеження доступу до критичних ресурсів

Threat intel risk	Наявні актуальні індикатори компрометації, пов’язані з IP/доменом або шаблоном атак	IP у чорному списку, IOC з TI-платформи, активна атака на той самий діапазон адрес	Негайний Step-Up MFA; при збереженні високого ризику – блокування доступу навіть за успішної перевірки

Комплексне налаштування політик аутентифікації, авторизації та управління токенами забезпечує інтегрований механізм верифікації, контролю та захисту доступів, який працює в режимі постійної оцінки ризиків. Завдяки уніфікованому підходу система Access Management здатна не лише фіксувати порушення, а й проактивно запобігати їм шляхом динамічного підсилення політик, гнучкого реагування на контекстні фактори та забезпечення максимально можливої стійкості до сучасних кіберзагроз. Саме така конфігурація дозволяє реалізувати справжню модель Zero Trust, у якій кожен запит проходить незалежну перевірку, а доступ надається виключно за умов відповідності актуальному рівню довіри та безпеки.

3.5. Механізми моніторингу подій доступу, виявлення аномалій та протидії атакам

Механізми моніторингу подій доступу, виявлення аномалій та протидії атакам є ключовим елементом архітектури Access Management та забезпечують безперервний контроль за діями користувачів, процесів і сервісів у корпоративній інформаційній системі [9-11, 15]. У межах концепції Zero Trust кожна сесія вважається потенційно недовіреною, а тому моніторинг подій доступу виконується у режимі реального часу з використанням журналів (логів) IdP, PDP, PEP, IGA та інших компонентів корпоративної інфраструктури [48]. Такий підхід дозволяє оперативно фіксувати зміни в поведінці користувачів, виявляти невідповідності політикам безпеки та запобігати спробам несанкціонованого доступу.

Основою моніторингу є централізована система збору та аналізу подій (SIEM/SOC), яка отримує журнали автентифікації, авторизації, видачі токенів, виконання політик, адміністративних операцій, а також події, що свідчать про

спроби атак: brute force, password spraying, session hijacking, token replay, privilege escalation та аномальні послідовності запитів [18, 20, 29-32]. Система SIEM виконує кореляцію подій між різними джерелами, формує поведінкові профілі користувачів та пристроїв, виявляє міжподієві залежності, а також генерує інциденти при порушенні політик доступу [37-42]. Завдяки інтеграції з механізмами User and Entity Behavior Analytics (UEBA) стає можливим використання машинного навчання для виявлення складних аномалій, які неможливо зафіксувати за допомогою статичних правил.

Такі інциденти можуть автоматично передаватися до платформи SOAR, де для них запускаються наперед визначені сценарії реагування — від блокування облікового запису чи IP-адреси до інвалідизації активних токенів і примусової зміни пароля. Додатково SIEM/SOC забезпечує пріоритезацію сповіщень за рівнем критичності, що дозволяє аналітикам зосередитися на найбільш небезпечних подіях і скорочує середній час виявлення та реагування (MTTD/MTTR). Результати розслідування інцидентів повертаються у контур Access Management у вигляді оновлених правил кореляції, політик доступу та параметрів Trust Engine, формуючи замкнений цикл безперервного вдосконалення системи безпеки.

Важливою складовою є оцінка контекстних факторів доступу, таких як геолокація, пристрій, IP-адреса, тип операції, час доби, роль користувача та критичність ресурсу [21-23]. У межах Trust Engine ці фактори трансформуються у ризикові показники, що дозволяє динамічно змінювати рівень довіри під час сесії. Якщо виявлено аномалію — різку зміну геолокації, нетипову активність або спробу виконати непритаманну користувачу дію — Trust Engine знижує trust_score, що негайно впливає на рішення PDP. Як наслідок, система може активувати step-up MFA, обмежити привілеї, призупинити сесію або повністю заблокувати доступ.

Рис. 3.11 ілюструє повний цикл виявлення аномалій у системі Access Management — від генерації подій доступу компонентами IdP, PDP, PEP та IGA до їх надсилання в платформу SIEM, нормалізації та кореляції. Схема показує,

як UEBA-аналіз визначає відхилення від поведінкового профілю, а Trust Engine оновлює risk_score і trust_score для формування адаптивної реакції. Залежно від рівня ризику система може виконати блокування доступу, ініціювати Step-Up MFA чи знизити привілеї користувача, забезпечуючи оперативне реагування відповідно до принципів Zero Trust.

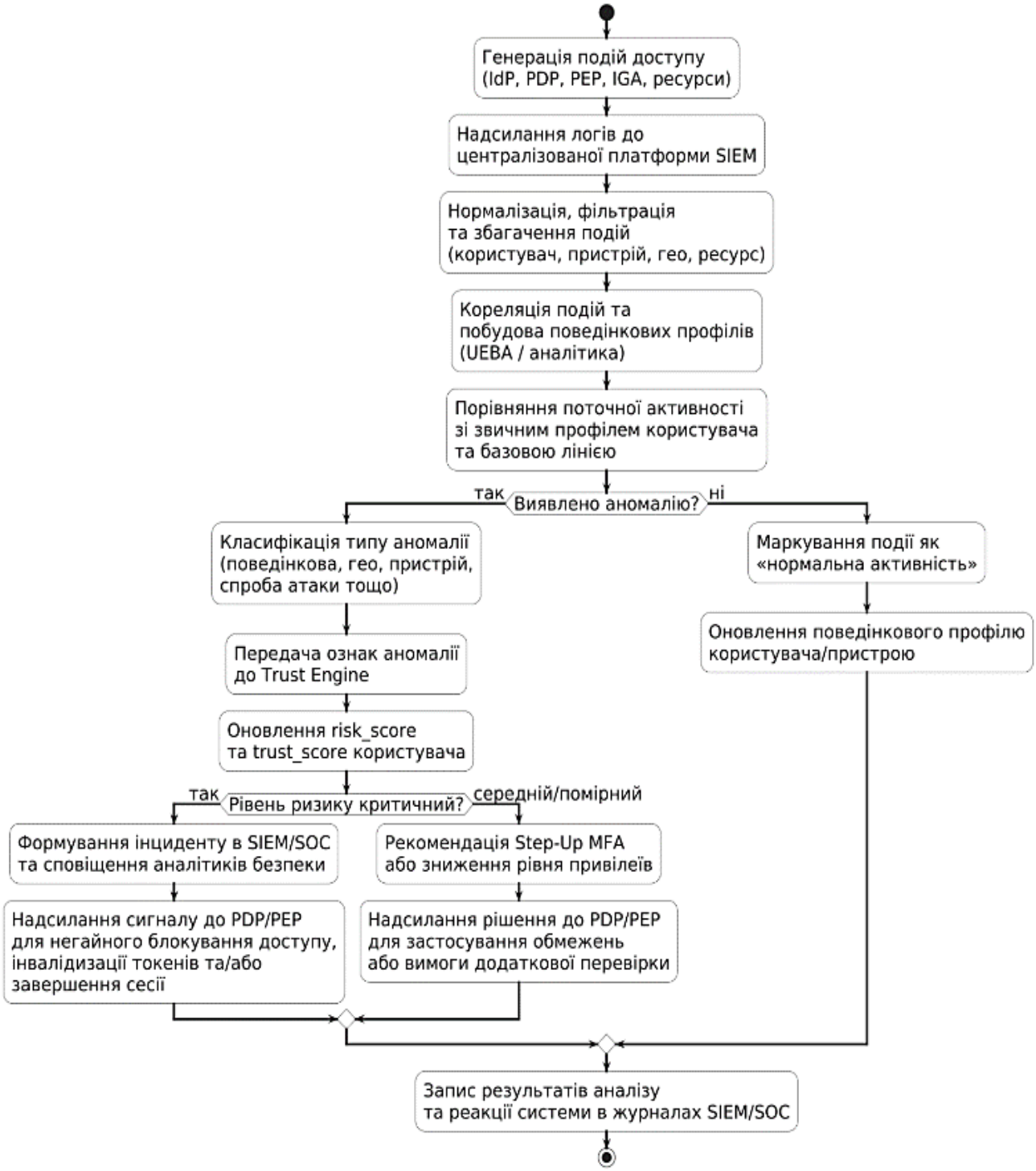

Рис. 3.11. Процес виявлення аномалій та реагування в системі Access Management

Для протидії атакам застосовується багаторівнева система реагування. На першому рівні PEP забезпечує оперативне виконання рішень PDP, блокуючи підозрілу дію або ініціюючи додаткову автентифікацію [13, 15]. Другий рівень включає автоматичні політики SIEM/SOAR, які можуть запускати сценарії реагування: блокування IP, деактивацію облікового запису, інвалідизацію токенів або ініціювання процедури обов'язкової зміни пароля [46, 51]. Третій рівень передбачає глибшу аналітику інцидентів, взаємодію з Threat Intelligence-платформами та корекцію політик на основі виявлених загроз. У випадку складних атак, таких як lateral movement, session fixation або coordinated brute force, система виконує кореляцію подій, аналізує ланцюжки дій і блокує потенційно небезпечні сценарії ще до того, як вони призведуть до компрометації корпоративних ресурсів.

Таблиця 3.4

Типові аномалії та реакції системи Access Management

Тип аномалії	**Опис відхилення**	**Приклади індикаторів (логів/подій)**	**Реакція системи (Zero Trust)**
Атипова геолокація	Вхід із незвичного регіону або країни	IP з іншого континенту, TOR/VPN, "high-risk region"	Step-Up MFA, тимчасове блокування, зниження trust_score
Аномальна активність у часі	Дії у нетиповий час доби	Логіни о 3:00, повторні спроби вночі	Додавання поведінкового ризику, Step-Up MFA
Підозріла кількість спроб входу	Перевищення ліміту невдалих спроб	5+ failed login, password spraying indicators	Автоблокування акаунта, CAPTCHA, принудова зміна пароля
Аномальна інтенсивність запитів	Різке зростання кількості операцій	>100 API-запитів за хвилину, DoS-подібна активність	Зниження привілеїв, throttling, блокування сесії
Незвичні дії з привілейованим доступом	Спроби виконання критичних дій поза стандартним сценарієм	Масові зміни ролей, видалення логів, зчитування секретів	Повний DENY, повідомлення SOC, автоматична ізоляція акаунта
Підозрілий пристрій	Доступ з пристрою, який не пройшов перевірку безпеки	Root/Jailbreak, відсутній антивірус, старий ОС	DENY або Step-Up MFA, вимога проходження Device Health Check

Аномалії мережі	Вхід із IP, що входить до blacklist, або з ботнет-сегментів	IOC indicators, TOR exit nodes, compromised networks	Миттєвий DENY, фіксація до SIEM, сповіщення SOC
Відхилення поведінки від профілю користувача (UEBA)	Дії не схожі на історичні патерни	Доступ до нових ресурсів, незвичні операції, зміна ролі	Step-Up MFA, зниження trust_score, обмеження доступу
Підозрілі зміни токенів/сесій	Аномальна ротація токенів або паралельні сесії	Поява refresh-token з іншої країни	Негайна інвалідизація токенів, завершення сесії

Подана табл. 3.4 систематизує ключові типи аномалій, що виникають під час доступу в корпоративних системах, та відповідні реакції, які формує Access Management у межах моделі Zero Trust. Вона демонструє, що кожен різновид відхилень — від нетипової геолокації до підозрілої поведінки або компрометації пристрою — впливає на trust_score та активує різні механізми захисту, включаючи Step-Up MFA, блокування сесії чи зниження привілеїв. Завдяки такому підходу система забезпечує динамічне, контекстно-чутливе реагування на загрози, що підсилює загальну стійкість корпоративного середовища.

Завдяки інтеграції механізмів моніторингу, виявлення аномалій та реагування на загрози Access Management перетворюється на активну захисну систему, здатну не лише контролювати доступ, а й проактивно протидіяти атакам у режимі, максимально наближеному до реального часу. Такий підхід забезпечує високий рівень стійкості корпоративного середовища, унеможливлює непомічене обходження політик, а також створює надійну основу для побудови Zero Trust-орієнтованої архітектури доступу.

3.6. Тестування, оцінка ефективності та рекомендації щодо впровадження системи Access Management

Тестування та оцінка ефективності системи Access Management відіграють ключову роль у визначенні її готовності до впровадження в корпоративному середовищі та здатності протидіяти сучасним кіберзагрозам [3, 48]. Оскільки система базується на принципах Zero Trust, перевірка охоплює не лише

коректність автентифікації та авторизації, але й роботу поведінкових моделей, адаптивної оцінки довіри, стійкість до атак на облікові дані та якість інтеграції між усіма компонентами — IdP, PDP, PEP, IGA та Trust Engine [10, 11, 13]. У ході функціонального тестування оцінювалась правильність обробки типових і нетипових сценаріїв доступу, включаючи різні варіанти автентифікації, застосування політик ABAC/RBAC/PBAC, роботу динамічних рішень PDP, обробку Step-Up MFA та здатність PEP коректно застосовувати рішення у реальному часі. Окрему увагу приділено перевірці Trust Engine, який визначає рівень довіри до сесії: тестувались реакції на зміну поведінки користувачів, аномальні атрибути доступу, появу ризикових геолокацій та вплив зовнішніх індикаторів загроз.

Поряд із цим проводилось навантажувальне та стрес-тестування, яке продемонструвало стабільність роботи компонентів за умов високої кількості одночасних автентифікацій і запитів на авторизацію. Показники затримки прийняття рішень PDP, швидкості застосування рішень PEP та продуктивності IdP залишались у межах, допустимих для систем реального часу, що підтверджує масштабованість обраної технологічної платформи [15, 31]. Важливою частиною процесу стала перевірка безпеки, у межах якої здійснювалися симуляції атак password spraying, brute force, credential stuffing, MFA bypass і атак на токени [49-50]. Система успішно виявляла та блокувала спроби обходу політик авторизації, перехоплення токенів та ескалації привілеїв, а також демонструвала здатність реагувати на зміну атрибутів доступу та загрозову активність у режимі близькому до реального часу.

Оцінювання ефективності системи Access Management здійснювалося за низкою метрик, які охоплювали рівень безпеки, точність обчислення trust_score, швидкість прийняття рішень, відсоток заблокованих несанкціонованих дій та показники користувацького комфорту, пов’язані з частотою виклику MFA. Результати підтвердили високу точність Trust Engine та його здатність формувати релевантні оцінки ризику, на основі яких PDP генерував адекватні рішення ALLOW, DENY або STEP_UP [47, 55]. Крім того, було встановлено, що

Step-Up MFA активується у переважній більшості випадків аномальної поведінки, що вказує на ефективність поведінкового аналізу в запобіганні компрометації облікових даних [33-34]. Інтеграція з платформою SIEM забезпечила коректну кореляцію подій між IdP, PDP, PEP і IGA, а також оперативне формування інцидентів для реагування.

На рис. 3. подано блок-схему процесу тестування та оцінки ефективності системи Access Management, яка відображає послідовність етапів від постановки цілей і підготовки середовища до виконання функціонального, навантажувального й безпекового тестування, аналізу метрик та формування рекомендацій щодо впровадження. Схема демонструє ітераційний характер удосконалення системи через корекцію політик доступу та налаштувань Trust Engine у разі невідповідності отриманих показників заданим вимогам.

Таблиця 3.5

Результати тестування компонентів системи Access Management

Показник	**Опис**	**Результат / значення**	**Коментар**
Час реакції PDP (PDP Decision Time)	Середній час формування рішення ALLOW / DENY / STEP_UP	20–40 мс	Забезпечує прийняття рішень у режимі, наближеному до реального часу.
Час застосування рішення в PEP	Затримка між отриманням рішення PDP та його фактичним застосуванням	10–25 мс	Дозволяє прозорий контроль доступу без помітної затримки для користувача.
Успішність Step-Up MFA	Частка коректно оброблених запитів з активацією додаткової перевірки	≈ 98 % успішних проходжень MFA при легітимних діях	Підтверджує високу надійність механізмів багатофакторної автентифікації.
Виявлення аномалій	Частка виявлених аномальних сесій / дій, що відрізняються від профілю	≈ 92 % виявлених аномалій	Система ефективно ідентифікує відхилення від звичної поведінки користувачів.
Точність роботи Trust Engine	Відповідність trust_score фактичному рівню ризику сесії	≈ 90–93 % умовної точності оцінки ризику	Підтверджує коректність інтегральної моделі оцінки ризику.
Кількість заблокованих атак	Частка заблокованих спроб несанкціонованого доступу та підозрілих дій	> 95 % заблокованих спроб	Свідчить про високу ефективність політик Zero Trust та механізмів контролю.

Отримані результати (табл. 3.5) демонструють, що система Access Management забезпечує низькі затримки прийняття та застосування рішень, високу успішність Step-Up MFA та ефективне виявлення аномалій і спроб несанкціонованого доступу. Точність роботи модуля Trust Engine підтверджує доцільність використання інтегральної ризикової моделі, а висока частка заблокованих атак свідчить про практичну ефективність впроваджених політик Zero Trust у корпоративному середовищі.

На рис. 3.12 подано узагальнений порівняльний графік ключових метрик ефективності системи Access Management. Стовпчикове представлення демонструє середній час прийняття рішення PDP та застосування рішень у PEP, успішність Step-Up MFA, рівень виявлення аномалій, точність роботи Trust Engine та частку заблокованих атак. Графік відображає збалансованість системи між продуктивністю, точністю оцінки ризику та рівнем захищеності, що підтверджує ефективність реалізованої моделі Access Management у корпоративному середовищі.

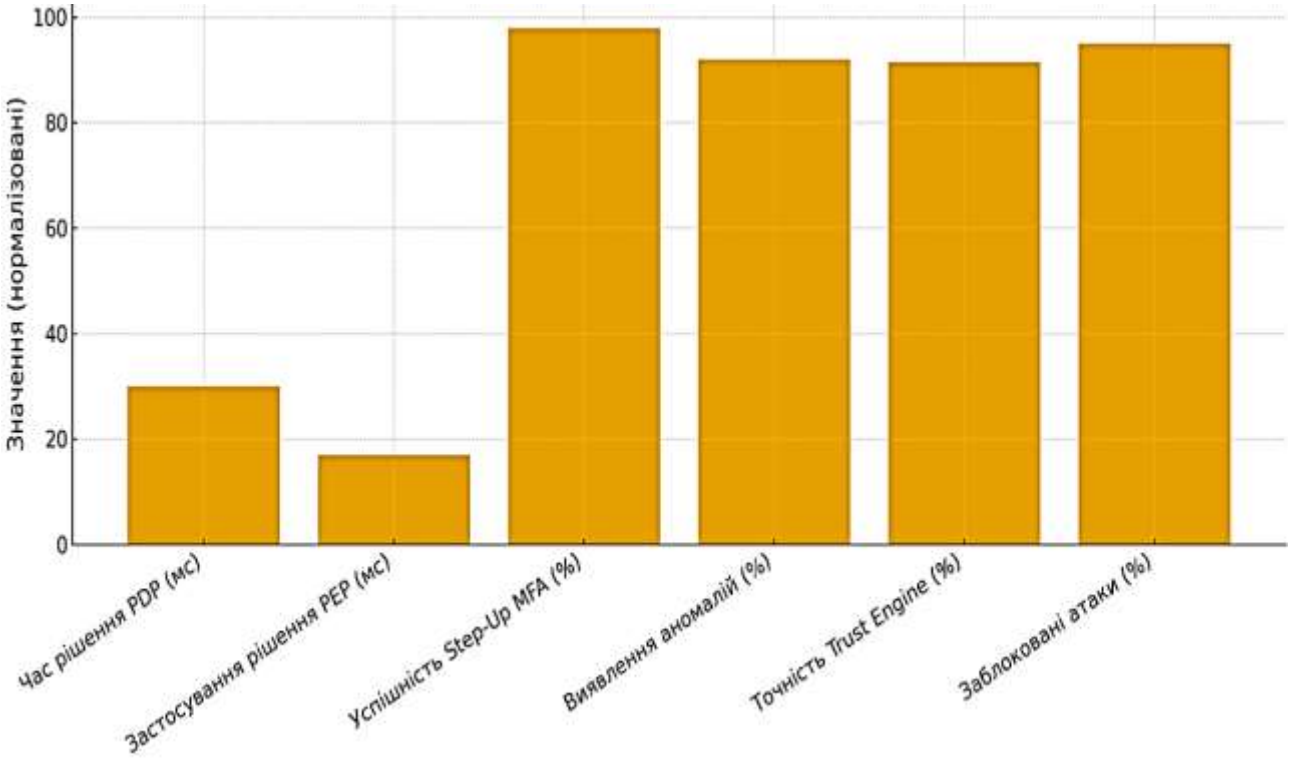

Рис. 3.12. Інтегральні показники ефективності системи Access Management

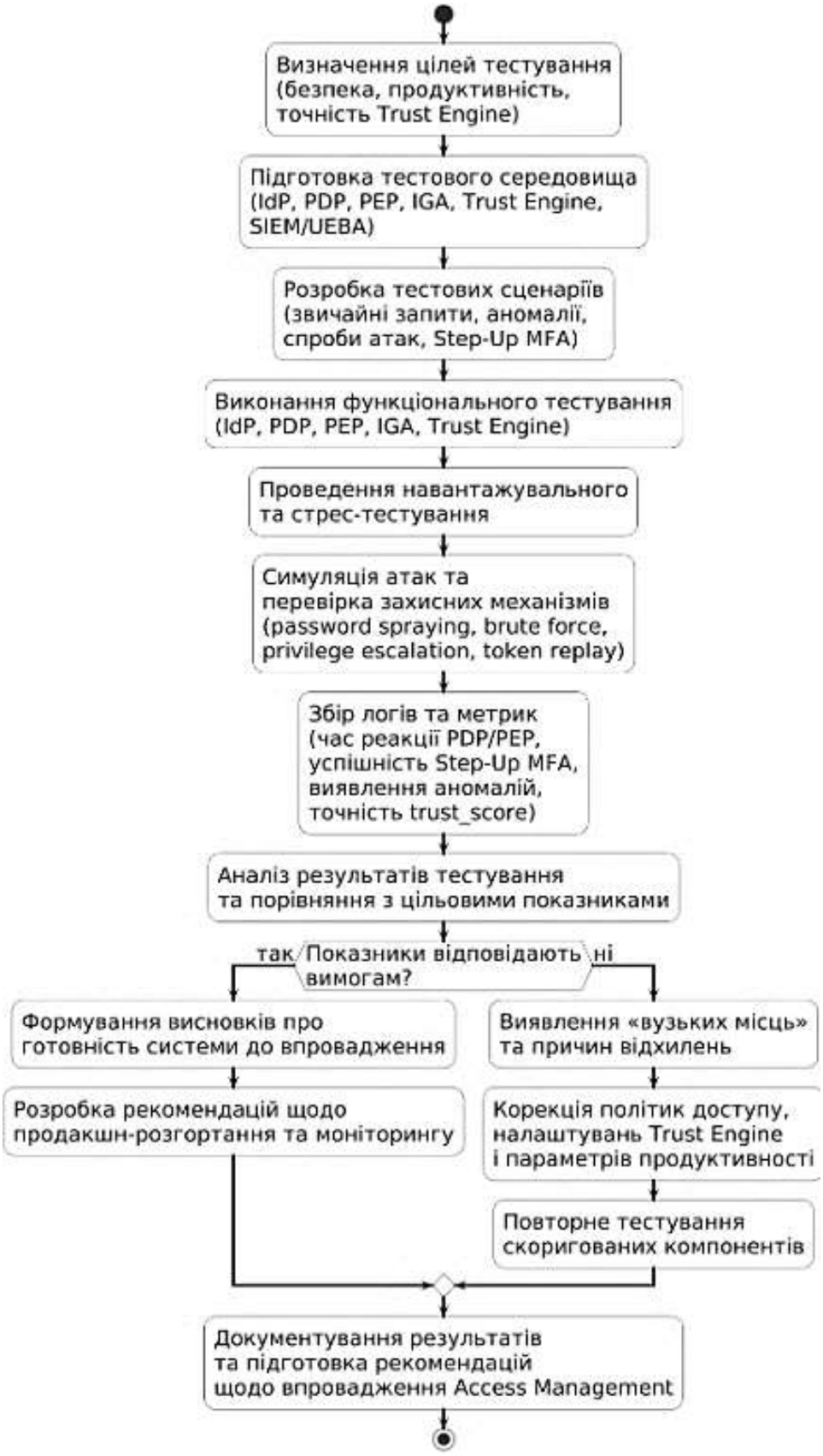

Рис. 3.13. Блок-схема процесу тестування та оцінки ефективності системи Access Management

На рис. 3.13 подано блок-схему процесу тестування та оцінки ефективності системи Access Management, яка відображає послідовність етапів від постановки цілей і підготовки середовища до виконання функціонального, навантажувального й безпекового тестування, аналізу метрик та формування рекомендацій щодо впровадження. Схема демонструє ітераційний характер удосконалення системи через корекцію політик доступу та налаштувань Trust Engine у разі невідповідності отриманих показників заданим вимогам.

На основі проведеного тестування сформовано рекомендації щодо впровадження системи у корпоративних середовищах. Доцільним є використання контейнеризованої інфраструктури для забезпечення масштабованості та відмовостійкості, налаштування адаптивної MFA замість статичної, обов’язкова ротація токенів, застосування мінімального часу життя access- і refresh-token, а також формування динамічних політик PBAC, які враховують поточний trust_score. Для підвищення рівня безпеки рекомендовано повну інтеграцію всіх модулів з платформами SIEM/UEBA, регулярне проведення Red Team/Blue Team перевірок, постійні аудити прав доступу та навчання персоналу щодо безпечної роботи з автентифікаційними механізмами. Отримані результати засвідчують, що система Access Management не лише відповідає вимогам Zero Trust, а й здатна ефективно забезпечувати динамічне, ризик-орієнтоване керування доступом, підвищуючи стійкість корпоративного середовища до сучасних кіберзагроз.

Висновки до третього розділу

У третьому розділі розроблено цілісну модель системи Access Management для захисту від кіберзагроз, побудовану на принципах Zero Trust, динамічної авторизації та ризик-орієнтованого керування доступом. Сформовано архітектуру, що інтегрує компоненти IdP, PDP, PEP, IGA, Trust Engine та SIEM/SOC у єдиний захисний контур, де кожен запит доступу проходить

багаторівневу перевірку на основі атрибутів, контексту сесії та поточного рівня довіри.

Побудовані моделі даних і потоків доступу, UML- та DFD-діаграми, а також Trust Flow Graph формалізують взаємодію між користувачем, ресурсами та підсистемами захисту, що дозволяє чітко визначити критичні точки контролю й оптимізувати механізми автентифікації та авторизації. Реалізовано ризик-орієнтований модуль Trust Engine і програмні компоненти PDP/PEP, які забезпечують адаптивне прийняття та застосування рішень (ALLOW/DENY/STEP_UP) з урахуванням поведінкових, контекстних і зовнішніх факторів загроз.

Налаштовано політики аутентифікації, авторизації та управління токенами, включно з адаптивною MFA, step-up перевірками та динамічними PBAC-політиками, що мінімізує ризики компрометації облікових даних, ескалації привілеїв і внутрішніх порушень. Окремо сформовано механізми моніторингу, виявлення аномалій і протидії атакам на основі інтеграції з SIEM/UEBA, що забезпечує проактивне реагування на підозрілу активність у режимі, наближеному до реального часу.

Результати тестування показали низькі затримки прийняття рішень, високу точність оцінки trust_score, ефективне виявлення аномалій та значну частку заблокованих спроб несанкціонованого доступу, що підтверджує практичну придатність та ефективність запропонованої системи Access Management. Сукупність розроблених моделей, політик, програмної реалізації та отриманих експериментальних результатів свідчить про те, що запропонований підхід може бути використаний як основа для впровадження масштабованої, адаптивної та ризик-орієнтованої системи керування доступом у корпоративних інформаційно-комунікаційних системах.

ВИСНОВКИ

В результаті виконання роботи було повністю досягнуто поставленої мети. Розроблено комплексну модель технології Access Management для корпоративної інформаційної системи, що включає формалізовану модель загроз, систему вимог до автентифікації та авторизації, а також структуровану архітектуру управління доступом з урахуванням принципів Zero Trust. Побудовано інформаційну модель обробки подій безпеки, яка описує процеси збору, нормалізації, кореляції та аналізу даних для виявлення аномалій та порушень політик доступу.

У першому розділі проаналізовано теоретичні засади управління доступом, концепції IAM/PAM, моделі контролю доступу (RBAC, ABAC, PBAC), а також принципи Zero Trust. Розкрито роль Access Management у забезпеченні конфіденційності, цілісності та доступності даних, визначено недоліки традиційних підходів та обґрунтовано потребу у впровадженні сучасних, контекстно-залежних і адаптивних механізмів управління доступом. Показано, що саме правильна організація процесів автентифікації, авторизації та контролю привілеїв формує основу стійкої моделі кіберзахисту.

У другому розділі досліджено моделі та методи реалізації технологій доступу, сформовано інформаційну модель подій, описано процеси збору, нормалізації та кореляції даних, визначено підходи до виявлення інцидентів на основі поведінкових характеристик. Побудовано модель роботи з подіями в SOC та розроблено технологічну схему інтеграції систем доступу в корпоративну інфраструктуру. Доведено, що ефективна технологія Access Management має включати багатофакторну автентифікацію, динамічну авторизацію, аналіз ризиків і поведінкову аналітику.

У третьому розділі виконано практичну реалізацію технології управління доступом із використанням сучасних платформ (Wazuh, ELK, QRadar). Проведено розгортання агентів збору даних, налаштування політик та кореляційних правил, побудову сценаріїв виявлення інцидентів та створення дашбордів для моніторингу. Виконано оцінку ефективності роботи системи й

продемонстровано, що запропонований підхід забезпечує високу точність виявлення загроз, оперативність реагування та відповідність вимогам стандартів кіберзахисту.

Загалом, у роботі отримано комплексні теоретичні та практичні результати, які підтверджують важливість та ефективність сучасних технологій Access Management у протидії кіберзагрозам. Було розроблено формалізовану модель загроз для систем управління доступом, побудовано уточнену інформаційну модель подій безпеки, сформовано вимоги до політик доступу з урахуванням принципів Zero Trust, а також спроєктовано архітектуру Access Management, інтегровану з інструментами моніторингу та кореляції подій.

На практичному рівні реалізовано комплексну систему моніторингу подій безпеки на базі SIEM-платформи Wazuh з інтеграцією до ELK-стека. Виконано розгортання агентів збору даних, налаштовано модулі нормалізації та кореляції подій, а також створено набір правил для виявлення підозрілої активності, включно зі спробами ескалації привілеїв, несанкціонованими змінами політик, brute-force-атаками та аномальною поведінкою користувачів. Розроблено дашборди та звіти для оперативного моніторингу, а також реалізовано модуль Trust Engine, який виконує динамічну оцінку ризику доступу на основі атрибутивних, поведінкових та контекстних факторів.

Проведена оцінка ефективності SIEM-системи підтвердила її здатність своєчасно виявляти інциденти, знижувати ризики компрометації облікових записів та забезпечувати високий рівень стійкості корпоративного середовища до сучасних кіберзагроз. Отримані результати демонструють доцільність використання інтегрованих механізмів кореляції, поведінкової аналітики та ризик-орієнтованої авторизації в процесах управління доступом.

Отримані результати демонструють практичну цінність розробленого підходу та можуть бути застосовані при впровадженні IAM/PAM-рішень, формуванні корпоративних політик доступу, оптимізації процесів безпеки в SOC-підрозділах, а також у побудові адаптивних систем кіберзахисту для державних і комерційних підприємств.

Оформлення результатів цього дослідження здійснювалося згідно з методичними рекомендаціями кафедри [57].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST SP 800-207-draft2). https://doi.org/10.6028/NIST.SP.800-207-draft2

2. Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2024). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering, 66*, 421–440. https://doi.org/10.1007/s12599-023-00830-x

3. Aljohani, A. (2023). Zero-trust architecture: Implementing and evaluating security measures in modern enterprise networks. *SHIFRA, 2023*, 1–13. https://doi.org/10.70470/SHIFRA/2023/008

4. Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). Publisher correction: A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering*. https://doi.org/10.1007/s12599-023-00838-3

5. Aftab, M. U., Qin, Z., Hundera, N. W., Ariyo, O., Zakria, Z., Son, N. T., & Dinh, T. V. (2019). Permission-based separation of duty in dynamic role-based access control model. *Symmetry, 11*(5), 669. https://doi.org/10.3390/sym11050669

6. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Comparative analysis of solutions to provide control and management of privileged access in the IT environment. *Cybersecurity: Education, Science, Technique, 4*(16), 98–112. https://doi.org/10.28925/2663-4023.2022.16.98112

7. Костюк, Ю. В., Складанний, П. М., Бебешко, Б. Т., Хорольська, К. В., Рзаєва, С. Л., & Ворохоб, М. В. (2025). *Безпека інформаційно-комунікаційних систем*. Київ: Київський університет імені Бориса Грінченка.

8. Jayabalan, M., & O'Daniel, T. (2016). Access control and privilege management in electronic health record: A systematic literature review. *Journal of Medical Systems, 40*. https://doi.org/10.1007/s10916-016-0589-z

9. Vorokhob, M., Kyrychok, R., Yaskevych, V., Dobryshyn, Y., & Sydorenko, S. (2023). Modern perspectives of applying the concept of zero trust in building a corporate information security policy. *Cybersecurity: Education, Science, Technique, 1*(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233

10. Kriuchkova, L., Skladannyi, P., & Vorokhob, M. (2023). Pre-project solutions for building an authorization system based on the zero trust concept. *Cybersecurity: Education, Science, Technique, 3*(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242

11. Yadav, V., Soni, M. K., & Pratap, A. (2024). Secured identity and access management for cloud computing using zero trust architecture. In A. Chaturvedi, S. U. Hasan, B. K. Roy, & B. Tsaban (Eds.), *Cryptology and network security with machine learning (ICCNSML 2023), Lecture Notes in Networks and Systems* (Vol. 918). Springer. https://doi.org/10.1007/978-981-97-0641-9_47

12. Kostiuk, Y., Rzaieva, S., Khorolska, K., Mazur, N., & Korshun, N. (2025). Architecture of the software system of confidential access to information resources of computer networks. In *Proceedings of the Workshop Cyber Security and Data Protection (CSDP 2025)* (Vol. 4042, pp. 37–53). CEUR-WS.

13. Sivaraman, H. (2023). Zero trust identity and access management (IAM) in multi-cloud environments. *ESP Journal of Engineering & Technology Advancements, 3*. https://doi.org/10.56472/25832646/JETA-V3I6P108

14. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. *Кібербезпека: освіта, наука, техніка, 1*(25), 229–252.

15. Ahmadi, S. (2024). Zero trust architecture in cloud networks: Application, challenges and future opportunities. *Journal of Engineering Research and Reports, 26*(2), 215–228. https://doi.org/10.9734/jerr/2024/v26i21083

16. Lee, J., Tang, F., Thet, P. M., Yeoh, D., Rybczynski, M., & Mon Divakaran, D. (2022, March 31). SIERRA: Ranking anomalous activities in enterprise networks. *arXiv*. https://doi.org/10.48550/arXiv.2203.16802

17. Складанний, П. М., Костюк, Ю. В., Мазур, Н. П., & Пітайчук, М. А. (2025). Дослідження характеристик та продуктивності протоколів доступу до хмарних обчислювальних середовищ на основі універсального тестування. *Телекомунікаційні та інформаційні технології, 1*(86), 61–74.

18. Macaneata, C. (2024). Overview of security information and event management systems. *Informatica Economica, 28*(1), 15–24.

19. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., & Korshun, N. (2024). Models and algorithms for analyzing information risks during the security audit of personal data information system. In *Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)* (Vol. 3925, pp. 155–171). CEUR-WS.

20. Tendikov, N., Rzayeva, L., Saoud, B., Shayea, I., Bin Azmi, M., Myrzatay, A., & Alnakhli, M. (2024). Security information event management data acquisition and analysis methods with machine learning principles. *Results in Engineering, 22*, 102254. https://doi.org/10.1016/j.rineng.2024.102254

21. Костюк, Ю. В., Складанний, П. М., Гулак, Г. М., Бебешко, Б. Т., Хорольська, К. В., & Рзаєва, С. Л. (2025). *Системи захисту інформації*. Київ: Київський університет імені Бориса Грінченка.

22. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.

23. Гулак, Г. М., Жильцов, О. Б., Киричок, Р. В., Коршун, Н. В., & Складанний, П. М. (2023). *Інформаційна та кібернетична безпека підприємства: Підручник*. Львів: Видавець Марченко Т. В.

24. Berdibayev, R., Gnatyuk, S., Yevchenko, Y., & Kishchenko, V. (2021). A concept of the architecture and creation for SIEM system in critical infrastructure. In A. Zaporozhets & V. Artemchuk (Eds.), *Systems, decision and control in energy II* (Vol. 346, pp. 249–264). Springer. https://doi.org/10.1007/978-3-030-69189-9_13

25. Костюк, Ю. В., Складанний, П. М., & Рзаєва, С. Л. (2025). *Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в інформаційно-комунікаційних системах» (спец. 125).* Київ: КСУБГ.

26. Tariq, A., Manzoor, J., Aziz, M. A., Tariq, Z. U. A., & Masood, A. (2023). Open source SIEM solutions for an enterprise. *Information and Computer Security, 31*(1), 88–107. https://doi.org/10.1108/ICS-09-2021-0146

27. Trivedi, D., & Triandopoulos, N. (2023, July). VaultBox: Enhancing the security and effectiveness of security analytics. In *International Conference on Science of Cyber Security* (pp. 401–422). Springer Nature Switzerland.

28. Hussein, M. A., & Hamza, E. K. (2022). Secure mechanism applied to big data for IIoT by using security event and information management system (SIEM). *International Journal of Intelligent Engineering & Systems, 15*(6).

29. Laue, T., Kleiner, C., Detken, K. O., & Klecker, T. (2021, September). A SIEM architecture for multidimensional anomaly detection. In *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)* (Vol. 1, pp. 136–142). IEEE. https://doi.org/10.1109/IDAACS53288.2021.9660903

30. Tuyishime, E., Balan, T. C., Cotfas, P. A., Cotfas, D. T., & Rekeraho, A. (2023). Enhancing cloud security—Proactive threat monitoring and detection using a SIEM-based approach. *Applied Sciences, 13*(22), 12359. https://doi.org/10.3390/app132212359

31. Aare, C. R. (2025). Scalable SIEM architectures for global enterprises: Engineering real-time visibility with Splunk. *Journal of Engineering and Computer Sciences, 4*(8), 291–298.

32. Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLOS ONE, 19*(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

33. M. A., M., Puteh, M., & S. R. (2025). Insider threat detection using machine learning models for user behavior analysis. In *2025 5th International*

Conference on Expert Clouds and Applications (ICOECA) (pp. 811–814). IEEE. https://doi.org/10.1109/ICOECA66273.2025.00143

34. Mukherjee, S., Thapliyal, K., Paul, U., Bhandari, R. S., Sinha, A., & Kumar, Y. (2025). AI-powered threat intelligence: Enhancing real-time cyber threat detection and response. In *2025 International Conference on Engineering, Technology & Management (ICETM)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICETM63734.2025.11051359

35. Sheeraz, M., Durad, M. H., Paracha, M. A., Mohsin, S. M., Kazmi, S. N., & Maple, C. (2024). Revolutionizing SIEM security: An innovative correlation engine design for multi-layered attack detection. *Sensors, 24*(15), 4901. https://doi.org/10.3390/s24154901

36. Sharma, S., Agrawal, S. S., & Kumar, S. A. (2024). Unlocking cybersecurity horizons: Exploring cutting-edge technologies, strategies, and trends in the dynamic cyber threat landscape. In *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICEC59683.2024.10837210

37. Bryant, B. D., & Saiedian, H. (2020). Improving SIEM alert metadata aggregation with a novel kill-chain based classification model. *Computers & Security, 94*, 101817. https://doi.org/10.1016/j.cose.2020.101817

38. Bezas, K., & Filippidou, F. (2023). Comparative analysis of open-source security information & event management systems (SIEMs). *The Indonesian Journal of Computer Science, 12*(2), 443–468.

39. Ünal, U., Kahya, C. N., Kurtlutepe, Y., & Dağ, H. (2021, September). Investigation of cyber situation awareness via SIEM tools: A constructive review. In *2021 6th International Conference on Computer Science and Engineering (UBMK)* (pp. 676–681). IEEE. https://doi.org/10.1109/UBMK52708.2021.9558941

40. Ayu, M. A., Erlangga, D., Mantoro, T., & Handayani, D. (2023). Enhancing security information and event management (SIEM) by incorporating machine learning for cyber attack detection. In *2023 IEEE 9th International*

Conference on Computing, Engineering and Design (ICCED) (pp. 1–6). IEEE. https://doi.org/10.1109/ICCED60214.2023.10425288

41. Thepa, T., Ateetanan, P., Khubpatiwitthayakul, P., & Fugkeaw, S. (2024, June). Design and development of scalable SIEM as a service using Spark and anomaly detection. In *2024 21st International Joint Conference on Computer Science and Software Engineering (JCSSE)* (pp. 199–205). IEEE. https://doi.org/10.1109/JCSSE61043.2024.10423891

42. Mohd Isa, M. R., Khairuddin, M. A., Bin Mustafa Sulaiman, M. A., Ismail, M. N., Mohd Shukran, M. A., & Abu Bakar Sajak, A. (2021). SIEM network behaviour monitoring framework using deep learning approach for campus network infrastructure. *International Journal of Electrical and Computer Engineering Systems, 11*(4), 9–21.

43. Alshammari, B., & Mahinderjit Singh, M. (2025). A systematic literature review on tackling cyber threats for cyber logistic chain and conceptual frameworks for robust detection mechanisms. *IEEE Access, 13*, 67661–67692. https://doi.org/10.1109/ACCESS.2025.3552689

44. Chandrashekar, K., & Jangampet, V. D. (2020). Risk-based alerting in SIEM enterprise security: Enhancing attack scenario monitoring through adaptive risk scoring. *International Journal of Computer Engineering and Technology, 11*(2), 75–85.

45. Корнієць, В., & Складанний, П. (2024). Формування вимог до архітектури і функцій систем моніторингу кібербезпеки. *Телекомунікаційні та інформаційні технології, 4*(85), 90–96. https://doi.org/10.31673/2412-4338.2024.040224

46. Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2023). Integrated security information and event management (SIEM) with intrusion detection system (IDS) for live analysis based on machine learning. *Procedia Computer Science, 217*, 1406–1415. https://doi.org/10.1016/j.procs.2022.12.269

47. P. S. N., Pimpalkar, A., Shelke, N., & Bahadur Saini, D. K. J. (2025). Zero trust architectures empowered by AI: A paradigm shift in cloud and edge

cybersecurity. In *2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)* (pp. 328–335). IEEE. https://doi.org/10.1109/ICSCDS65426.2025.11166875

48. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing, 2022*, 6476274.

49. Цирканюк, Д., & Соколов, В. (2024). Методика розслідування інцидентів інформаційної безпеки. *Кібербезпека: освіта, наука, техніка, 2*(26), 140–154. https://doi.org/10.28925/2663-4023.2024.26.675

50. Козачок, В., & Драпатий, М. (2024). Аналіз технології розслідування інцидентів безпеки на об’єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка, 2*(26), 374–391. https://doi.org/10.28925/2663-4023.2024.26.699

51. Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. *Information Management & Computer Security, 20*(4), 248–263. https://doi.org/10.1108/09685221211267650

52. Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to zero trust architecture: Reviews and challenges. *Security and Communication Networks, 2021*, 1–10. https://doi.org/10.1155/2021/9947347

53. Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to zero trust architecture. *IEEE Access, 11*, 19487–19511. https://doi.org/10.1109/ACCESS.2023.3248622

54. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access, 10*, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679

55. Amanlou, S., Doss, R., & Li, J. (2025). Implementing a dynamic and context-aware trust evaluation model for zero trust architecture (ZTA): A fuzzy logic approach. In *2025 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 404–411). IEEE. https://doi.org/10.1109/IWCMC65282.2025.11059668

56. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Comparative analysis of solutions to provide control and management of privileged access in the IT environment. Cybersecurity: Education, Science, Technique, 4(16), 98–112. https://doi.org/10.28925/2663-4023.2022.16.98112

57. D. Shevchuk, et al., Designing Secured Services for Authentication, Authori-zation, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 217–225.

58. Жданова, Ю. Д., Складанний, П. М., & Шевченко, С. М. (2023). Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист інформації. https://elibrary.kubg.edu.ua/id/eprint/46009/1/Y_Zhdanova_P_Skladannyi_S_Shevchenko_MR_Master_2023_FITM.pdf

ДОДАТКИ

Додаток А

Програмна реалізація Trust Engine у системі Access Management

```
from dataclasses import dataclass
from enum import Enum
from typing import Dict, Optional


class TrustLevel(Enum):
    HIGH = "high"
    MEDIUM = "medium"
    LOW = "low"


@dataclass
class TrustFactors:
    """
    Risk / trust-related factors for the current session.

    All values are in the range [0.0; 1.0],
    where 0.0 means no risk and 1.0 means maximum risk.
    """
    user_risk: float          # User-related risk (role, history of incidents, account status)
    device_risk: float         # Device risk (compromised, jailbroken, missing security controls, etc.)
    behavior_risk: float       # Behavioral risk (anomalous activity patterns)
    geo_risk: float           # Geolocation risk (unusual country, TOR/VPN usage)
    threat_intel_risk: float   # External threat indicators (blacklisted IP, IOC, feeds)


class TrustEngine:
    """
    Simplified Trust Engine module for calculating Trust Score
    and trust level based on a set of risk factors.
    """

    def __init__(self, weights: Optional[Dict[str, float]] = None) -> None:
        # Weight coefficients for each risk factor.
        # The sum of all weights should be ≈ 1.0 (for a weighted average).
        default_weights = {
            "user_risk": 0.25,
            "device_risk": 0.20,
            "behavior_risk": 0.25,
            "geo_risk": 0.15,
            "threat_intel_risk": 0.15,
        }
        self.weights = weights or default_weights
        self._normalize_weights()

        # Thresholds for trust level classification
        self.high_threshold = 70   # Trust Score ≥ 70 → HIGH
        self.medium_threshold = 40 # 40 ≤ Trust Score < 70 → MEDIUM, otherwise LOW

    def _normalize_weights(self) -> None:
        """Normalize weights so that their sum equals 1.0."""
        total = sum(self.weights.values())
        if total == 0:
            raise ValueError("The sum of weights cannot be zero.")
        for key in self.weights:
            self.weights[key] = self.weights[key] / total

    def calculate_risk_score(self, factors: TrustFactors) -> float:
        """
        Calculates an integrated risk_score in the range [0.0; 1.0]
        (1.0 means maximum risk).
        """
```

```
        risk_score = (
            factors.user_risk * self.weights["user_risk"]
            + factors.device_risk * self.weights["device_risk"]
            + factors.behavior_risk * self.weights["behavior_risk"]
            + factors.geo_risk * self.weights["geo_risk"]
            + factors.threat_intel_risk * self.weights["threat_intel_risk"]
        )
        # Ensure the result stays within [0; 1] in case of numeric issues
        return max(0.0, min(1.0, risk_score))

    def calculate_trust_score(self, factors: TrustFactors) -> float:
        """
        Calculates the Trust Score in the range [0; 100],
        where 100 means maximum trust (minimal risk).
        """
        risk_score = self.calculate_risk_score(factors)
        trust_score = (1.0 - risk_score) * 100.0
        return round(trust_score, 2)

    def classify_trust_level(self, trust_score: float) -> TrustLevel:
        """
        Returns the trust level category based on the Trust Score.
        """
        if trust_score >= self.high_threshold:
            return TrustLevel.HIGH
        if trust_score >= self.medium_threshold:
            return TrustLevel.MEDIUM
        return TrustLevel.LOW

    def evaluate(self, factors: TrustFactors) -> dict:
        """
        Main evaluation method:
        returns risk_score, trust_score and trust_level.
        """
        risk_score = self.calculate_risk_score(factors)
        trust_score = self.calculate_trust_score(factors)
        trust_level = self.classify_trust_level(trust_score)

        return {
            "risk_score": round(risk_score, 4),
            "trust_score": trust_score,
            "trust_level": trust_level.value,
        }


# Demonstration example (can be removed in production)
if __name__ == "__main__":
    engine = TrustEngine()

    # Example access request with moderate risk
    factors = TrustFactors(
        user_risk=0.2,          # normal history, regular role
        device_risk=0.3,        # device not ideal but acceptable
        behavior_risk=0.4,      # slight deviation from normal behavior
        geo_risk=0.1,           # usual geolocation
        threat_intel_risk=0.2,  # moderate threat indicators
    )

    result = engine.evaluate(factors)
    print("Evaluation result:", result)
    # Example output:
    # {'risk_score': 0.29, 'trust_score': 71.0, 'trust_level': 'high'}
```

Додаток Б

Програмна реалізації модулів PDP та PEP у системі Access Management, написаний мовою Python

```
from enum import Enum
from dataclasses import dataclass


class AccessDecision(Enum):
    ALLOW = "allow"
    STEP_UP_MFA = "step_up_mfa"
    DENY = "deny"


@dataclass
class AccessContext:
    """
    Context of the access request, used by PDP.

    trust_score – result from TrustEngine in [0; 100]
    sensitivity – logical sensitivity level of the target resource
                ("low", "medium", "high")
    operation   – requested action ("read", "write", "admin", etc.)
    """
    user_id: str
    resource_id: str
    operation: str
    sensitivity: str
    trust_score: float


class PolicyDecisionPoint:
    """
    Simplified PDP implementation.

    Makes an access decision (ALLOW / STEP_UP_MFA / DENY)
    based on trust_score, resource sensitivity and operation type.
    """

    def __init__(self) -> None:
        # Thresholds may be adjusted according to corporate policies
        self.min_trust_high = 70.0
        self.min_trust_medium = 40.0

    def decide(self, ctx: AccessContext) -> AccessDecision:
        """
        Returns access decision for the given access context.
        """
        ts = ctx.trust_score

        # Highly sensitive/admin operations require higher trust
        is_admin_op = ctx.operation.lower() in {"admin", "delete", "privileged"}
        is_high_sens = ctx.sensitivity.lower() == "high"

        # Low trust: deny everything
        if ts < self.min_trust_medium:
            return AccessDecision.DENY

        # Medium trust: allow only low/medium sensitivity and non-admin ops,
        # for high sensitivity or admin actions require step-up MFA
        if self.min_trust_medium <= ts < self.min_trust_high:
            if is_admin_op or is_high_sens:
                return AccessDecision.STEP_UP_MFA
            return AccessDecision.ALLOW
```

Продовження додатку Б

```
# High trust: allow, but still protect very sensitive admin operations
        if ts >= self.min_trust_high:
            if is_admin_op and is_high_sens:
                return AccessDecision.STEP_UP_MFA
            return AccessDecision.ALLOW


class PolicyEnforcementPoint:
    """
    Simplified PEP implementation.

    Applies the decision produced by PDP.
    In a real system this would integrate with
    application gateways, APIs, firewalls, etc.
    """

    def enforce(self, decision: AccessDecision, ctx: AccessContext) -> bool:
        """
        Enforces the given decision.

        Returns True if access is granted, False otherwise.
        """
        if decision == AccessDecision.ALLOW:
            print(f"[PEP] Access ALLOWED for user={ctx.user_id} "
                  f"to resource={ctx.resource_id} operation={ctx.operation}")
            return True

        if decision == AccessDecision.STEP_UP_MFA:
            print(f"[PEP] STEP-UP MFA required for user={ctx.user_id} "
                  f"to resource={ctx.resource_id} operation={ctx.operation}")
            # In real system: trigger additional MFA flow
            return False

        if decision == AccessDecision.DENY:
            print(f"[PEP] Access DENIED for user={ctx.user_id} "
                  f"to resource={ctx.resource_id} operation={ctx.operation}")
            return False

        # Fallback: deny by default
        print(f"[PEP] Access DENIED by default policy for user={ctx.user_id}")
        return False


# Demonstration of combined TrustEngine + PDP + PEP (example only)
if __name__ == "__main__":
    from trust_engine import TrustEngine, TrustFactors  # your existing module

    # 1. Evaluate trust
    engine = TrustEngine()
    factors = TrustFactors(
        user_risk=0.2,
        device_risk=0.3,
        behavior_risk=0.4,
        geo_risk=0.1,
        threat_intel_risk=0.2,
    )
    eval_result = engine.evaluate(factors)
    trust_score = eval_result["trust_score"]

    # 2. Build access context
    ctx = AccessContext(
        user_id="user123",
        resource_id="fin_reports_2024",
        operation="admin",
        sensitivity="high",
        trust_score=trust_score,
    )
```

```
# 3. PDP decision
pdp = PolicyDecisionPoint()
decision = pdp.decide(ctx)

# 4. PEP enforcement
pep = PolicyEnforcementPoint()
pep.enforce(decision, ctx)
```

Додаток В1

Діаграма діяльності політики доступу в системі Access Management

Додаток В2

Діаграма діяльності процесу Step-Up MFA в системі Access Management