МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “АНАЛІЗ ТА ПОБУДОВА МОДЕЛЕЙ УПРАВЛІННЯ ДОСТУПОМ У ІНФОРМАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ ZERO TRUST”

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

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

_____ Владислав ГРИГОРЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБД-41

Владислав ГРИГОРЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Діана ПРИМАЧЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Григоренку Владиславу Руслановичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Аналіз та побудова моделей управління доступом у інформаційних системах на основі Zero Trust”,
керівник кваліфікаційної роботи ПРИМАЧЕНКО Діана.
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

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

2. Строк подання кваліфікаційної роботи “29” травня 2026 р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, моделі управління доступом, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити теоретичні основи управління доступом та концепції Zero Trust.
4.2. Проаналізувати існуючі рішення та змоделювати систему управління доступом.
4.3. Розробити та впровадити Zero Trust-орієнтовану модель.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	29.03.2026	
3.	Дослідження теоретичних основ управління доступом та концепції Zero Trust	08.04.2026	
4.	Аналіз існуючих рішень та моделювання системи управління доступом	22.04.2026	
5.	Розробка та практичне впровадження Zero Trust-орієнтованої моделі	08.05.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2026	
7.	Оформлення роботи.	22.05.2026	
8.	Оформлення презентації.	03.06.2026	
9.	Отримання рецензії на роботу.	03.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Владислав ГРИГОРЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Григоренко В.Р. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Аналіз та побудова моделей управління доступом у інформаційних системах на основі Zero Trust”

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ГРИГОРЕНКО Владислав у кваліфікаційній роботі дослідив теоретичні основи управління доступом та концепції Zero Trust, проаналізував існуючі рішення та змоделювати систему управління доступом, а також розробив та впровадив Zero Trust-орієнтовану модель.

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

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

Керівник кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Григоренко В.Р. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ГРИГОРЕНКА Владислава
на тему “Аналіз та побудова моделей управління доступом у інформаційних системах на основі Zero Trust”

Актуальність. Стрімкий розвиток інформаційних технологій, зокрема поширення хмарних сервісів, мобільного доступу та розподілених інфраструктур, призводить до зростання кількості потенційних векторів атак і ускладнює традиційні підходи до захисту інформаційних систем. У таких умовах особливої ваги набуває впровадження сучасних концепцій управління доступом, серед яких ключове місце посідає модель Zero Trust, що передбачає відсутність апріорної довіри до будь-якого користувача або пристрою. Ефективна реалізація підходу Zero Trust потребує не лише технічних рішень, а й чітко визначених політик автентифікації, авторизації та постійного контролю доступу, а також належної обізнаності персоналу щодо принципів безпечної роботи з інформаційними ресурсами. Застосування сучасних методів аналізу та побудови моделей управління доступом дозволяє знизити ризики неса нкціонованого доступу та підвищити загальний рівень захищеності інформаційних систем.

З огляду на це, дослідження методів аналізу та розроблення моделей управління доступом в інформаційних системах на основі концепції Zero Trust є актуальним і важливим науково-практичним завданням.

Позитивні сторони.

1. У роботі досліджено особливості аналізу та побудови моделей управління доступом у інформаційних системах на основі Zero Trust.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків та таблиць.
3. Автор опрацював значну джерельну базу: близько 50 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо побудови моделей управління доступом у інформаційних системах на основі Zero Trust .

Недоліки.

Доцільним є приділення більшої уваги дослідженню та класифікації програмних засобів, що використовуються для аналізу, моделювання та оцінювання ефективності впроваджених механізмів управління доступом в інформаційних системах, зокрема рішень, побудованих на принципах концепції Zero Trust.

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

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

Рецензент: _____ _____

підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технологій формування обізнаності й навчання персоналу з інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 6 рисунків, 6 таблиць, висновків і списку використаних джерел із 44 найменувань. Загальний обсяг роботи становить 76 аркушів, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження та аналіз моделей управління доступом в інформаційних системах на основі концепції Zero Trust.

Об'єктом дослідження є процеси управління доступом до ресурсів інформаційних систем.

Предмет дослідження **–** методи, механізми та моделі реалізації політик автентифікації й авторизації, що використовуються в архітектурі Zero Trust.

Методи дослідження**.** Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до розробки моделей управління доступом в інформаційних системах на основі концепції Zero Trust.

Як результат у роботі досліджено теоретичні основи управління доступом та концепції Zero Trust, проаналізовано існуючі рішення та змоделювати систему управління доступом, а також розроблено та впроваджено Zero Trust-орієнтовану модель.

Галузь застосування**.** Розроблені підходи можуть бути використані під час проєктування, впровадження та модернізації систем управління доступом у складі системи управління інформаційною безпекою підприємства, зокрема при переході до архітектури Zero Trust.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ ДОСТУПОМ, ZERO TRUST, АВТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, ПОЛІТИКИ БЕЗПЕКИ, ІНФОРМАЦІЙНІ СИСТЕМИ.

ABSTRACT

The qualification work is devoted to the study of information security awareness and training technologies for personnel. The work consists of an introduction, three chapters containing 6 figures, 6 tables, conclusions and the list of references containing 44 items. The total volume of the work is 76 pages, of which 6 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to investigate and analyse access control models in information systems based on the Zero Trust concept.

The object the study is the processes of managing access to information system resources.

The subject of the study is the methods, mechanisms and models for implementing authentication and authorisation policies used in the Zero Trust architecture.

Research methods. In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, classification, expert assessment, and a systematic approach to developing access control models for information systems based on the Zero Trust concept were used in the work.

As a result, the work investigated the theoretical foundations of access control and the Zero Trust concept, analysed existing solutions and models an access control system, and developed and implemented a Zero Trust-oriented model.

Field of application. The developed approaches can be used during the design, implementation and modernisation of access control systems as part of an organisation’s information security management system, particularly when transitioning to a Zero Trust architecture.

Keywords: INFORMATION SECURITY, ACCESS CONTROL, ZERO TRUST, AUTHENTICATION, AUTHORISATION, SECURITY POLICIES, INFORMATION SYSTEMS.

ЗМІСТ

ВСТУП

Актуальність теми. У світі, де державні установи, підприємства та окремі користувачі постійно стають об’єктами кібератак, забезпечення надійного захисту інформаційних систем набуває особливої важливості. Швидкий розвиток інформаційних технологій, поширення хмарних сервісів і віддаленого доступу призводять до зростання кількості потенційних вразливостей і ускладнюють застосування традиційних моделей захисту, заснованих на периметровій безпеці.

У зв’язку з цим все більшого поширення набуває концепція Zero Trust, яка передбачає безперервну перевірку користувачів, пристроїв і запитів на доступ незалежно від їхнього розташування в мережі. Реалізація такого підходу вимагає розроблення ефективних моделей управління доступом, що забезпечують гнучке та контекстно-залежне прийняття рішень щодо надання прав доступу до інформаційних ресурсів.

З огляду на це, дослідження методів аналізу та побудови моделей управління доступом в інформаційних системах на основі принципів Zero Trust є актуальним і важливим науковим завданням, спрямованим на підвищення рівня захищеності сучасних інформаційних інфраструктур.

Мета роботи полягає у дослідженні та аналізі моделей управління доступом в інформаційних системах на основі концепції Zero Trust.

Об’єкт дослідження **–** процеси управління доступом до ресурсів інформаційних систем.

Предмет дослідження – методи, механізми та моделі реалізації політик автентифікації й авторизації, що використовуються в архітектурі Zero Trust.

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

1. Дослідити теоретичні основи управління доступом та концепції Zero Trust.

2. Проаналізувати існуючі рішення та змоделювати систему управління доступом.

3. Розробити та впровадити Zero Trust-орієнтовану модель.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до розробки моделей управління доступом в інформаційних системах на основі концепції Zero Trust.

Як результат у роботі досліджено теоретичні основи управління доступом та концепції Zero Trust, проаналізовано існуючі рішення та змоделювати систему управління доступом, а також розроблено та впроваджено Zero Trust-орієнтовану модель.

Практичне значення одержаних результатів. Використання отриманих у роботі результатів дає змогу здійснювати обґрунтований вибір методів, моделей та програмних засобів управління доступом в інформаційних системах, що відповідають принципам концепції Zero Trust. Запропоновані підходи можуть бути застосовані під час проєктування та впровадження політик автентифікації й авторизації з урахуванням цілей бізнесу, наявних ресурсів і особливостей IT-інфраструктури підприємства, що сприятиме підвищенню загального рівня інформаційної безпеки.

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

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ДОСТУПОМ ТА КОНЦЕПЦІЇ ZERO TRUST

Зростання кількості кіберзагроз і ускладнення IT-інфраструктур зумовлюють потребу у нових підходах до забезпечення безпеки. Одним із таких підходів є концепція Zero Trust, що змінює традиційне уявлення про довіру в інформаційних системах. У цьому контексті важливим є теоретичне осмислення основ управління доступом як складової сучасних систем захисту інформації.

1.1 Основні принципи інформаційної безпеки та моделі управління доступом

Інформаційна безпека виступає не лише як технічна складова функціонування інформаційних систем, але й як стратегічний фактор забезпечення стабільності, надійності та безперервності діяльності організацій. Стрімкий розвиток інформаційних технологій, поширення хмарних сервісів, мобільних платформ і розподілених обчислювальних середовищ зумовлює постійне зростання обсягів даних, що обробляються, передаються та зберігаються. У таких умовах будь-які порушення безпеки можуть призводити до значних фінансових втрат, репутаційних ризиків і навіть загроз національній безпеці. Саме тому забезпечення інформаційної безпеки стає одним із ключових завдань як на рівні окремих організацій, так і на державному рівні.

Фундамент інформаційної безпеки традиційно базується на трьох основних принципах, відомих як тріада конфіденційності, цілісності та доступності. Конфіденційність передбачає обмеження доступу до інформації лише для авторизованих суб’єктів і запобігання її несанкціонованому розголошенню. Це досягається шляхом застосування механізмів шифрування, контролю доступу та політик безпеки. У сучасних умовах особливого значення набуває захист персональних даних, комерційної таємниці та іншої чутливої інформації, що потребує впровадження комплексних підходів до забезпечення

конфіденційності.

Цілісність інформації означає збереження її точності, повноти та незмінності протягом усього життєвого циклу. Порушення цілісності може проявлятися у вигляді несанкціонованого внесення змін, пошкодження або знищення даних. Для забезпечення цього принципу використовуються механізми контролю цілісності, такі як хеш-функції, цифрові підписи, журнали аудиту та системи резервного копіювання. Важливість цілісності особливо актуальна для критичних систем, де навіть незначна зміна даних може призвести до серйозних наслідків.

Доступність, у свою чергу, забезпечує своєчасний і безперешкодний доступ до інформаційних ресурсів для авторизованих користувачів. Вона передбачає стійкість систем до відмов, атак типу відмови в обслуговуванні та інших факторів, що можуть впливати на працездатність. Забезпечення доступності досягається шляхом використання резервування, балансування навантаження, відмовостійких архітектур і механізмів відновлення після збоїв [1].

Окрім тріади CIA, сучасна інформаційна безпека включає низку додаткових принципів, які розширюють і поглиблюють її концептуальну основу. Одним із таких принципів є автентичність, що полягає у підтвердженні достовірності суб’єкта або джерела інформації. Це забезпечується за допомогою механізмів автентифікації, таких як паролі, токени, біометричні дані та сертифікати. Не менш важливим є принцип підзвітності, який передбачає можливість відстеження дій користувачів і системних процесів. Для цього використовуються журнали подій, системи моніторингу та аналізу безпеки.

Принцип невідмовності гарантує, що жодна сторона не зможе заперечити факт виконання певної дії або передачі інформації. Це особливо важливо в електронному документообігу та фінансових системах, де необхідно забезпечити юридичну значущість операцій. Також важливу роль відіграє принцип мінімальних привілеїв, який передбачає надання користувачам лише тих прав, які необхідні для виконання їхніх функціональних обов’язків. Реалізація цього

принципу дозволяє суттєво знизити ризики несанкціонованого доступу та внутрішніх загроз.

Управління доступом є одним із центральних механізмів реалізації принципів інформаційної безпеки. Воно визначає політики та процедури, що регулюють процеси ідентифікації, автентифікації та авторизації користувачів, а також контроль їхніх дій у системі. Ефективне управління доступом дозволяє забезпечити баланс між безпекою та зручністю використання інформаційних систем, що є критично важливим для сучасних організацій [2].

Ідентифікація є початковим етапом процесу доступу і полягає у визначенні суб'єкта, який намагається отримати доступ до системи. Після цього здійснюється автентифікація, яка підтверджує особу користувача. Сучасні системи все частіше використовують багатофакторну автентифікацію, що поєднує кілька незалежних факторів: знання (пароль), володіння (токен або смартфон) та біометричні характеристики. Такий підхід значно підвищує рівень захищеності систем і знижує ймовірність компрометації облікових записів.

Після успішної автентифікації здійснюється авторизація, яка визначає рівень доступу користувача до ресурсів системи. Саме на цьому етапі застосовуються моделі управління доступом, які формалізують правила надання прав доступу. Однією з найпростіших і найдавніших моделей є дискреційна модель управління доступом [3]. Вона передбачає, що власник ресурсу самостійно визначає, хто і які права має щодо цього ресурсу. Такий підхід є досить гнучким і зручним, однак має суттєві недоліки, пов'язані з відсутністю централізованого контролю та високим ризиком помилок. Процес ідентифікації, автентифікації та авторизації користувача зображено на рис. 1.1.

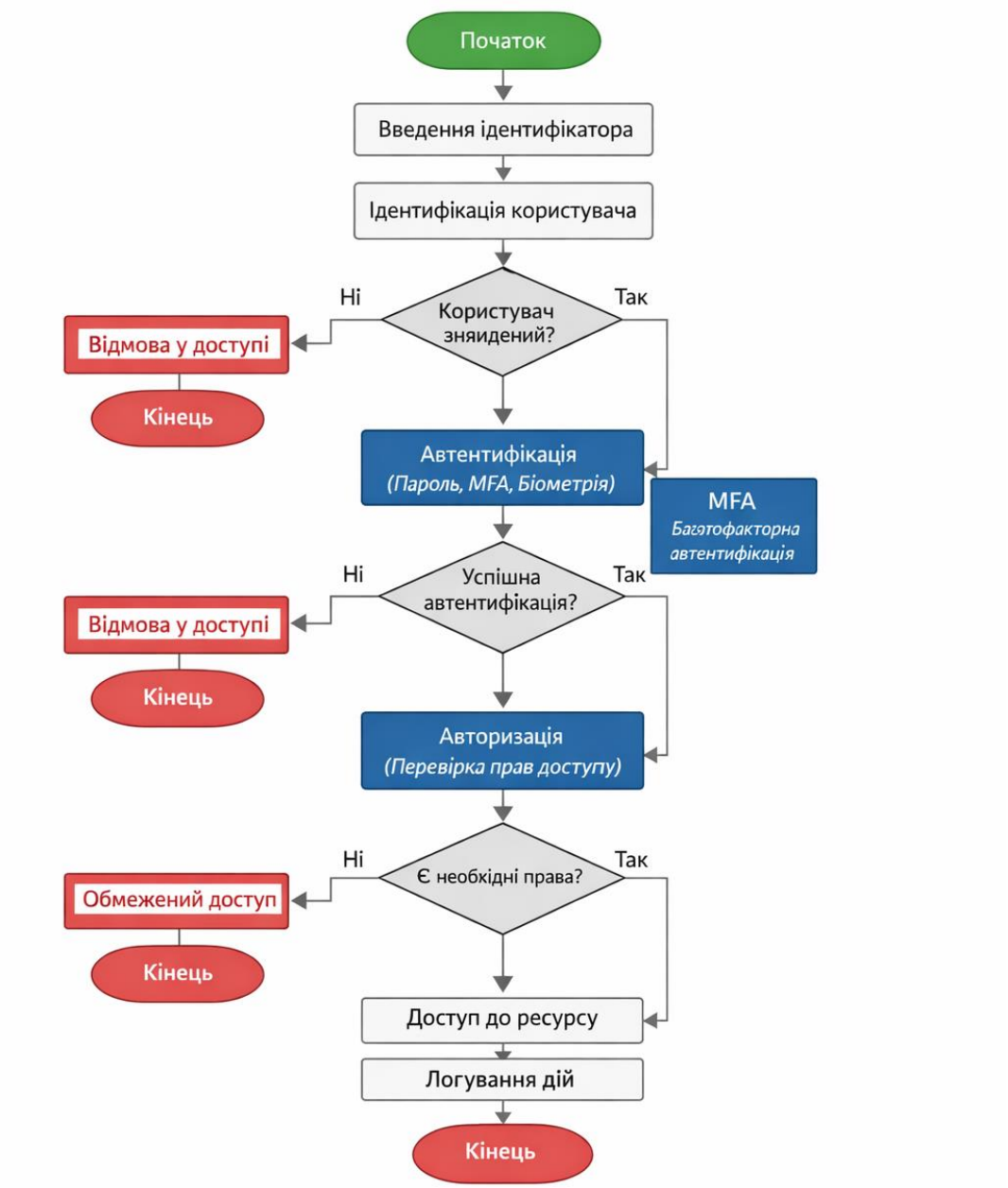

Рис. 1.1 Процес ідентифікації, автентифікації та авторизації користувача

Мандатна модель управління доступом базується на суворих правилах, встановлених централізовано. У межах цієї моделі кожному об’єкту та суб’єкту присвоюється певний рівень безпеки, а доступ надається відповідно до встановлених політик. Ця модель забезпечує високий рівень захисту, однак є менш гнучкою та складнішою у впровадженні. Вона широко використовується в системах, де безпека має критичне значення, наприклад у військових або державних установах [4].

Рольова модель управління доступом є однією з найбільш поширених у

корпоративному середовищі. Вона передбачає, що права доступу призначаються не окремим користувачам, а ролям, які вони виконують. Користувач отримує права відповідно до своєї ролі в організації. Це значно спрощує процес адміністрування доступу, особливо в умовах великої кількості користувачів і ресурсів. Водночас така модель потребує ретельного проєктування ролей і їхніх взаємозв'язків [5].

Подальший розвиток інформаційних систем і зростання їхньої складності сприяли появі атрибутної моделі управління доступом. Вона базується на використанні атрибутів, що характеризують користувача, ресурс, середовище та контекст доступу. Це дозволяє реалізувати більш гнучкі та динамічні політики безпеки, які враховують широкий спектр факторів. Наприклад, доступ може надаватися залежно від місцезнаходження користувача, часу доби або стану пристрою. Такий підхід є особливо актуальним у хмарних і розподілених системах, однак потребує складнішої інфраструктури для реалізації.

Таблиця 1.1

Порівняння моделей управління доступом

Модель	**Основний принцип**	**Переваги**	**Недоліки**	**Сфера застосування**
DAC	Користувач керує доступом	Гнучкість, простота	Ризик витоку прав	Персональні системи
MAC	Централізований контроль	Висока безпека	Жорсткість політик	Державні системи
RBAC	Доступ за ролями	Масшта бованість	Складність налаштування ролей	Корпоративні системи
ABAC	Доступ за атрибутами	Гнучкість, контекстність	Висока складність	Хмарні середовища

Важливим є також врахування концепції контекстно-орієнтованого доступу, яка поєднує елементи різних моделей і дозволяє адаптувати політики безпеки в режимі реального часу. Це особливо важливо в умовах динамічного

середовища, де користувачі можуть працювати з різних пристроїв і локацій. У таких умовах традиційні підходи до управління доступом вже не забезпечують достатнього рівня захисту.

Моделі управління доступом еволюціонують від простих і статичних до складних і динамічних, що відповідають сучасним вимогам безпеки. Вибір конкретної моделі залежить від специфіки організації, рівня критичності інформації та вимог до безпеки [6]. У більшості випадків ефективним є комбіноване використання кількох моделей, що дозволяє досягти оптимального балансу між гнучкістю та захищеністю.

1.2 Класичні підходи до контролю доступу

Класичні підходи до контролю доступу сформували основу сучасних систем інформаційної безпеки та визначили базові принципи розмежування прав користувачів у інформаційних системах. Вони виникли як відповідь на потребу формалізувати процес надання доступу до ресурсів і забезпечити контроль за діями суб’єктів у системі. Основними моделями, що використовуються в межах класичних підходів, є дискреційна (DAC), мандатна (MAC), рольова (RBAC) та атрибутна (ABAC). Кожна з цих моделей має власну логіку організації доступу, різний рівень гнучкості та застосовується залежно від вимог до безпеки та специфіки інформаційного середовища [7].

Дискреційна модель контролю доступу є однією з найперших і найпростішою за своєю реалізацією. Вона базується на принципі, за яким власник ресурсу самостійно визначає, хто має право доступу до цього ресурсу та які операції дозволені. У такій моделі кожен об’єкт має список контролю доступу або інші механізми, що визначають права для конкретних користувачів чи груп. Основною перевагою DAC є її гнучкість і простота впровадження, що робить її зручною для невеликих систем або персонального використання. Однак ця модель має суттєві недоліки, зокрема відсутність централізованого контролю та високий ризик поширення прав доступу між користувачами без належного

контролю [8]. Це може призводити до витоку інформації або несанкціонованого доступу, особливо в умовах великої кількості користувачів.

Мандатна модель контролю доступу є більш формалізованою і суворою. Вона передбачає централізоване управління доступом на основі політик безпеки, які не можуть бути змінені користувачами. У цій моделі кожному об’єкту та суб’єкту призначається рівень безпеки або мітка, а доступ надається відповідно до встановлених правил, наприклад, «читання вниз» або «запис вгору». Такий підхід забезпечує високий рівень захисту інформації, оскільки виключає можливість довільного розповсюдження прав доступу. Водночас MAC характеризується низькою гнучкістю і складністю адміністрування, що обмежує її застосування переважно системами з підвищеними вимогами до безпеки, такими як військові або урядові інформаційні системи.

Рольова модель контролю доступу виникла як компроміс між гнучкістю DAC та суворістю MAC. Вона базується на концепції ролей, які відображають функціональні обов’язки користувачів у системі. У межах цієї моделі права доступу призначаються ролям, а користувачі отримують відповідні права шляхом призначення їм ролей [9]. Такий підхід значно спрощує адміністрування доступу, особливо в організаціях з великою кількістю користувачів і ресурсів. RBAC дозволяє централізовано керувати правами доступу, зменшує ймовірність помилок і забезпечує відповідність політик безпеки організаційній структурі. Однак ефективність цієї моделі залежить від правильного проєктування ролей і їхньої ієрархії, а також від регулярного оновлення відповідно до змін у структурі організації.

Атрибутна модель контролю доступу є найбільш сучасним і гнучким підходом серед класичних моделей. Вона базується на використанні атрибутів, які описують користувачів, ресурси, середовище та контекст доступу. Рішення про надання доступу приймається на основі аналізу цих атрибутів і відповідних політик. Наприклад, доступ може залежати від місцезнаходження користувача, часу доби, типу пристрою або рівня довіри до середовища . Такий підхід дозволяє реалізувати складні сценарії контролю доступу, що є особливо

важливим у сучасних розподілених і хмарних системах. Водночас ABAC потребує значних обчислювальних ресурсів і складної інфраструктури для управління атрибутами та політиками, що може ускладнювати її впровадження. Опис моделей зображено на рис. 1.2.

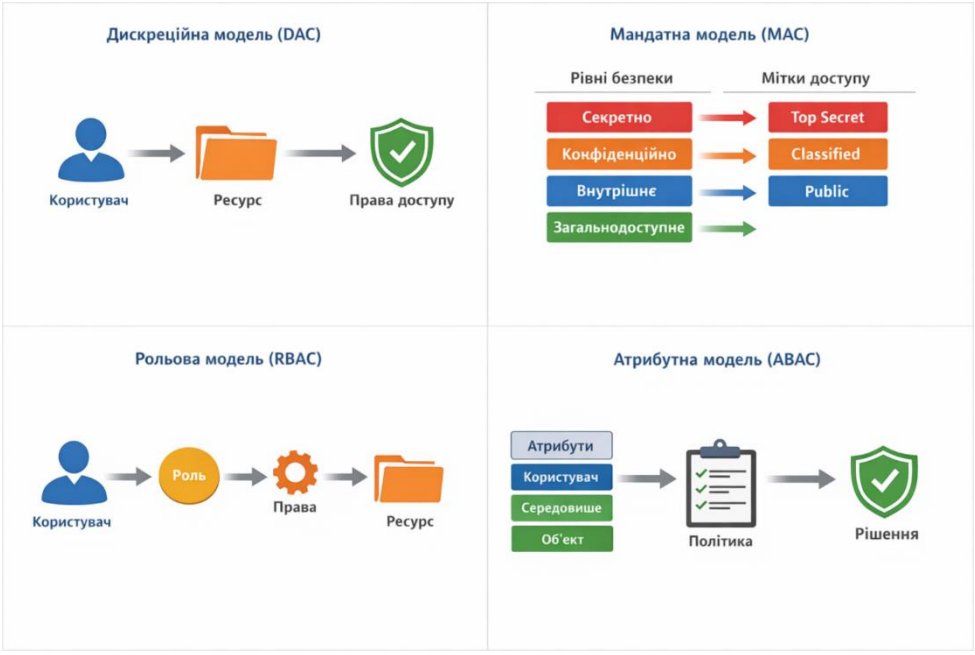

Рис. 1.2 Основні моделі контролю доступу (DAC, MAC, RBAC, ABAC)

Порівнюючи ці моделі, можна зазначити, що вони відрізняються рівнем централізації управління, гнучкістю та складністю реалізації. DAC забезпечує максимальну свободу користувачів, але мінімальний контроль, тоді як MAC навпаки — максимальний контроль при обмеженій гнучкості. RBAC пропонує баланс між цими крайнощами, а ABAC відкриває можливості для реалізації динамічних і контекстно-залежних політик безпеки [10]. В інформаційних системах часто використовується комбінований підхід, який поєднує елементи кількох моделей для досягнення оптимального рівня безпеки.

Важливим аспектом класичних підходів до контролю доступу є їхня інтеграція з іншими механізмами інформаційної безпеки, такими як автентифікація, аудит і моніторинг. Наприклад, у межах RBAC або ABAC рішення про доступ може залежати від результатів автентифікації або поточного стану системи. Це дозволяє підвищити рівень захисту та забезпечити більш точне

управління доступом. А також, використання журналів аудиту дозволяє відстежувати дії користувачів і виявляти потенційні порушення політик безпеки.

Сучасні тенденції розвитку інформаційної безпеки свідчать про поступовий перехід від статичних моделей контролю доступу до динамічних і контекстно-орієнтованих підходів. Це пов’язано з необхідністю адаптації до змінного середовища, де користувачі можуть працювати з різних пристроїв, мереж і географічних локацій [11]. У таких умовах традиційні моделі, зокрема DAC і MAC, вже не забезпечують достатнього рівня гнучкості та ефективності, що стимулює розвиток RBAC і ABAC, а також їхніх гібридних варіацій. Характеристика моделей вказана в табл. 1.2.

Таблиця 1.2

Порівняльна характеристика моделей контролю доступу

Модель	Тип управління	Гнучкість	Рівень безпеки	Складність реалізації
DAC	Децентралізований	Висока	Низький	Низька
MAC	Централізований	Низька	Високий	Середня
RBAC	Централізований	Середня	Середній	Середня
ABAC	Контекстно-орієнтований	Висока	Високий	Висока

Загалом класичні підходи до контролю доступу залишаються важливим елементом побудови систем інформаційної безпеки, оскільки вони забезпечують базову структуру для управління правами доступу. Розуміння їхніх принципів, переваг і обмежень є необхідним для ефективного проєктування сучасних систем захисту інформації. У подальшому ці підходи слугують основою для розвитку нових концепцій, зокрема моделей, орієнтованих на принципи Zero Trust, які передбачають більш жорсткий і динамічний контроль доступу.

1.3 Концепція Zero Trust: принципи, архітектура та сучасні стандарти

Концепція Zero Trust є фундаментальним і сучасним підходом до

забезпечення інформаційної безпеки, що радикально трансформує традиційні уявлення про довіру в інформаційних системах. Традиційні моделі безпеки базуються на припущенні, що користувачі та пристрої, які перебувають всередині корпоративної мережі, заслуговують на довіру, що часто реалізується через периметрові засоби захисту, такі як брандмауери, VPN або системи контролю доступу. Однак у сучасному цифровому середовищі, яке характеризується гібридною роботою, високою мобільністю користувачів, хмарними сервісами та складною інтеграцією сторонніх платформ, така модель довіри виявилася недостатньою. Zero Trust радикально змінює цей підхід, проголошуючи принцип «нікому не довіряй автоматично», що означає постійну верифікацію кожного запиту на доступ незалежно від того, звідки він надходить.

Основна ідея Zero Trust полягає у відмові від будь-якої попередньої довіри до користувачів, пристроїв чи додатків, навіть якщо вони знаходяться всередині корпоративного периметру. У такій моделі кожна взаємодія з інформаційними ресурсами перевіряється на відповідність політикам доступу, а надання доступу здійснюється лише на основі принципу мінімальних привілеїв, тобто користувач отримує тільки ті права, які необхідні для виконання конкретної задачі, без можливості надмірного доступу [12]. А також, доступ формується на основі контекстної оцінки, яка включає фактори, такі як місце розташування користувача, тип пристрою, час запиту, стан безпеки пристрою та поведінкові аномалії. Цей підхід дозволяє значно знизити ймовірність компрометації системи через внутрішні та зовнішні загрози, зокрема через фішинг, шкідливе програмне забезпечення, компрометацію облікових записів або інсайдерські атаки.

Принципи Zero Trust можна класифікувати на декілька ключових напрямів. Перший – це сувора автентифікація та авторизація користувачів і пристроїв, яка передбачає багатофакторну автентифікацію (MFA), перевірку стану пристрою, оцінку довірених сертифікатів та інтеграцію з системами управління ідентифікацією (IAM). Другий напрям – сегментація мережі, яка передбачає ізоляцію критичних ресурсів у відокремлені зони з обмеженим доступом, що

дозволяє локалізувати потенційні загрози та зменшити масштаби можливих інцидентів. Третій – постійний моніторинг і аудит дій користувачів та пристроїв, що забезпечує виявлення аномалій, відстеження підозрілих активностей і формування контекстної оцінки ризиків у реальному часі. Четвертий напрям – динамічне застосування політик доступу, коли доступ може змінюватися залежно від поточного контексту, включаючи часові обмеження, геолокацію, тип пристрою та рівень кіберзахисту.

Архітектура Zero Trust являє собою модульну та багаторівневу структуру, де взаємодіють кілька ключових компонентів. До них належать:

1. Контролери доступу – відповідають за автентифікацію користувачів, перевірку пристроїв та реалізацію політик доступу.

2. Системи управління ідентифікацією та привілеями (IAM та PAM) – забезпечують централізоване управління обліковими записами, ролями, привілеями та механізмами їх тимчасового або умовного надання.

3. Механізми моніторингу та аналітики – збирають дані про користувачів, пристрої, мережеві взаємодії, здійснюють поведінковий аналіз, виявляють аномалії та автоматично реагують на потенційні загрози.

4. Сегментовані мережеві ділянки та ізольовані ресурси – визначають чіткі правила взаємодії між зонами, що зменшує ризики поширення загроз у випадку компрометації одного з компонентів системи.

Ключовим елементом є політики доступу, які визначають умови, за яких користувач або пристрій може отримати доступ до ресурсів. Ці політики охоплюють не лише статичні параметри, а й динамічні фактори, такі як рівень загрози, поведінкові моделі користувача, контекст сеансу та тип запитуваного ресурсу. Наприклад, доступ до конфіденційних документів може бути дозволений тільки під час робочого часу з корпоративного пристрою, що відповідає стандартам безпеки, або заблокований при виявленні аномальної активності [13].

Сучасні стандарти та керівні практики Zero Trust визначають методологію впровадження концепції в корпоративних та державних інформаційних

системах. Наприклад, NIST Special Publication 800-207 описує модель Zero Trust Enterprise, яка включає п’ять основних компонентів: визначення ресурсів, контроль доступу, постійний моніторинг, аналітику загроз та автоматизацію реакцій. Крім того, стандарти ISO/IEC 27001 та 27002 формалізують вимоги до управління інформаційною безпекою, що дозволяє організаціям систематизувати процеси впровадження Zero Trust, забезпечуючи відповідність законодавчим нормам, зменшення ризиків та підвищення загальної кіберстійкості.

Інтеграція концепції Zero Trust в існуючі системи управління доступом вимагає застосування сучасних технологічних рішень, таких як:

- багатофакторна автентифікація (MFA) – підвищує надійність підтвердження особи;
- Privileged Access Management (PAM) – управління привілеями користувачів та контроль критичних облікових записів;
- User and Entity Behavior Analytics (UEBA) – аналіз поведінки користувачів і пристроїв для виявлення аномалій;
- автоматизоване прийняття рішень на основі контексту – забезпечує динамічне регулювання доступу та адаптивний захист.

Таке комплексне поєднання політик, процесів та технологій дозволяє не лише захистити інформаційні ресурси від несанкціонованого доступу, а й підвищити ефективність моніторингу, реагування на інциденти та управління ризиками, формуючи інтегровану систему кібербезпеки [14].

Особливу роль у Zero Trust відіграє постійний аудит та аналітика дій користувачів, що дозволяє своєчасно виявляти підозрілі активності, поведінкові аномалії та потенційні загрози, а також корелювати їх із іншими подіями в системі для прийняття обґрунтованих рішень щодо обмеження доступу. Сегментація мережі та ізоляція критичних ресурсів забезпечують локалізацію інцидентів, зменшуючи потенційні наслідки компрометації окремих компонентів.

Отже, Zero Trust не є лише технологічним рішенням, а формує системну

парадигму інформаційної безпеки, що дозволяє організаціям адаптуватися до динамічного цифрового середовища. Впровадження принципів Zero Trust разом із правильною архітектурою та дотриманням міжнародних стандартів забезпечує комплексний підхід до кіберзахисту, мінімізує ризики внутрішніх та зовнішніх загроз, підвищує контроль за доступом і моніторинг критичних ресурсів, а також забезпечує відповідність законодавчим та нормативним вимогам сучасного цифрового світу.

Висновки до розділу 1

У результаті аналізу теоретичних основ управління доступом та концепції Zero Trust встановлено, що ефективна організація інформаційної безпеки в сучасних інформаційних системах ґрунтується на комплексному підході, який інтегрує політики доступу, технології автентифікації та постійний моніторинг активностей користувачів і пристроїв. Дослідження основних принципів інформаційної безпеки засвідчує, що конфіденційність, цілісність та доступність інформації залишаються базовими критеріями захисту, а моделі управління доступом, зокрема DAC, MAC та RBAC, забезпечують систематизацію надання привілеїв та контроль за використанням ресурсів. Водночас класичні підходи до контролю доступу, які орієнтовані на периметровий захист і централізоване управління правами користувачів, виявляють обмежену ефективність у контексті сучасних гібридних середовищ, хмарних платформ та високої мобільності користувачів. Аналіз концепції Zero Trust демонструє, що її впровадження формує принципово нову парадигму інформаційної безпеки, засновану на відсутності автоматичної довіри, постійній автентифікації та авторизації, мінімізації привілеїв, сегментації мережі та динамічному застосуванні політик доступу на основі контексту. Розгляд архітектури Zero Trust свідчить про можливість систематичного впровадження концепції з дотриманням нормативних вимог і забезпеченням високого рівня кіберзахищеності. Отже, інтеграція принципів Zero Trust у корпоративні та державні інформаційні

системи створює стійку та адаптивну архітектуру безпеки, здатну ефективно протидіяти як внутрішнім, так і зовнішнім загрозам, а також обґрунтовує необхідність переходу до контекстно-орієнтованого та системного управління доступом у сучасних умовах цифрової трансформації.

РОЗДІЛ 2 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА МОДЕЛЮВАННЯ СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ

Забезпечення ефективного управління доступом є критичним елементом кібербезпеки, що визначає рівень захисту ресурсів від несанкціонованого використання. Аналіз існуючих рішень дозволяє оцінити їхню здатність контролювати права користувачів, забезпечувати мінімізацію привілеїв та інтегрувати механізми постійного моніторингу, що є особливо актуальним у контексті реалізації принципів Zero Trust. Моделювання системи управління доступом дозволяє формалізувати взаємодію користувачів і ресурсів, оптимізувати політики доступу та підвищити стійкість інформаційної інфраструктури до внутрішніх і зовнішніх загроз.

2.1 Аналіз сучасних інформаційних систем та їх механізмів автентифікації і авторизації

Інформаційні системи представляють собою багаторівневі інтегровані комплекси, що об’єднують апаратні ресурси, програмні модулі, мережеві інтерфейси та хмарні сервіси. Така комплексна структура створює значні виклики для забезпечення інформаційної безпеки, оскільки класичні підходи до контролю доступу та автентифікації, що спираються переважно на периметровий захист і статичне призначення привілеїв, виявляються недостатньо ефективними у контексті сучасних динамічних середовищ, хмарних платформ та мобільних пристроїв. Автентифікація в таких системах виступає фундаментальним механізмом підтвердження достовірності користувачів або пристроїв та забезпечує первинний контроль над тим, хто отримує доступ до ресурсів [15]. Авторизація, у свою чергу, визначає обсяг доступних прав і привілеїв, обмежує можливість виконання певних дій та регламентує використання ресурсів у відповідності до політик безпеки. Комплексне поєднання автентифікації та авторизації формує інтегровану систему контролю доступу, що є критичною

умовою для забезпечення конфіденційності, цілісності та доступності інформації, а також запобігання несанкціонованому доступу та витоку даних.

Значного поширення цифрових технологій та динамічного зростання обсягів оброблюваної інформації застосовуються численні методи автентифікації, серед яких традиційні паролі та пін-коди, апаратні та програмні токени безпеки, цифрові сертифікати, біометричні параметри та багатофакторна автентифікація. Паролі залишаються найбільш поширеним механізмом автентифікації, що пояснюється їх простотою та низькими витратами на впровадження. Проте їхня ефективність обмежується вразливістю до фішингових атак, перебору паролів, використання слабких комбінацій, повторного застосування в різних сервісах та інших видів соціальної інженерії. Апаратні токени і одноразові паролі (OTP) забезпечують вищий рівень безпеки, оскільки вони фізично прив’язані до користувача та унеможливлюють віддалене підбору комбінацій. Водночас їх застосування потребує додаткових витрат на інфраструктуру, адміністрування та інтеграцію з системами управління доступом [16]. Сертифікати та цифрові підписи забезпечують надійну автентифікацію користувачів і пристроїв, зокрема у корпоративних та державних інформаційних системах, де критично важливо підтвердити достовірність джерела запиту і забезпечити цілісність переданої інформації. Біометричні методи автентифікації, такі як сканування відбитків пальців, розпізнавання обличчя, сканування сітківки ока, стають все більш поширеними завдяки високому рівню достовірності і зручності для користувачів. Водночас їх впровадження потребує значних фінансових та технічних ресурсів, а також створює додаткові питання щодо захисту персональних даних і конфіденційності.

Одним із найбільш ефективних та перспективних підходів є багатофакторна автентифікація, що поєднує знання користувача (пароль), володіння об’єктом (токен або смарт-карта) та унікальні біометричні характеристики. Такий підхід істотно знижує ймовірність компрометації облікових записів, оскільки для зловмисника необхідно одночасно

скомпрометувати кілька незалежних факторів. Крім того, сучасні системи дедалі частіше застосовують контекстну автентифікацію, яка оцінює місцезнаходження користувача, IP-адресу, тип пристрою, час доступу, поведінкові патерни та інші контекстуальні фактори для ухвалення рішення про надання доступу [17]. Цей підхід особливо важливий у реалізації концепції Zero Trust, де жоден запит на доступ не сприймається як автоматично довірений, а кожна взаємодія перевіряється в реальному часі, з урахуванням ризиків і відповідності політикам безпеки.

Таблиця 2.1

Порівняльна характеристика методів автентифікації

Метод автентифікації	Переваги	Недоліки	Сфера застосування
Паролі/Пін-коди	Простота, низькі витрати	Вразливість до фішингу та підбору	Корпоративні системи, базові сервіси
Токени безпеки/OTP	Висока надійність	Потребує носія, інтеграції	Банківські системи, корпоративні мережі
Сертифікати/цифрові підписи	Надійна автентифікація	Витрати на PKI, складність адміністрування	Державні системи, критичні мережі
Біометрія	Висока достовірність	Високі витрати, питання приватності	Корпоративні та мобільні системи
Багатофакторна автентифікація	Максимальний захист	Складність впровадження	Хмарні сервіси, критичні ІС

Сучасні механізми управління доступом базуються на різноманітних моделях, які дозволяють ефективно організувати контроль за правами користувачів, оптимізувати адміністрування та підвищити безпеку інформаційної системи. До таких моделей належать Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC) та Attribute-Based Access Control (ABAC). DAC дозволяє власнику ресурсу

самостійно визначати права доступу, що забезпечує гнучкість у розподілі привілеїв, однак підвищує ризик надмірних прав та можливість компрометації системи. MAC передбачає централізоване управління доступом на основі політик безпеки, що забезпечує високий рівень контролю, проте її гнучкість обмежена, особливо в умовах динамічних і хмарних середовищ. RBAC дозволяє централізовано призначати ролі користувачам із визначеними привілеями, що спрощує адміністрування у великих корпоративних структурах, проте не забезпечує достатньої адаптивності у хмарних або мобільних середовищах. ABAC забезпечує ухвалення рішень на основі атрибутів користувача, об’єкта та контексту, що підвищує гнучкість і адаптивність, особливо у гібридних і динамічних середовищах. У практиці сучасних організацій застосовуються комбіновані моделі, що поєднують RBAC та ABAC для формування гібридної системи управління доступом, яка враховує як роль користувача, так і контекст запиту, забезпечуючи баланс між простотою адміністрування і гнучкістю доступу.

Рис. 2.1 Процес автентифікації та авторизації в сучасних системах на основі Zero Trust

Важливою тенденцією є інтеграція механізмів автентифікації та авторизації з системами моніторингу, аналітики та управління ризиками. Це дозволяє формувати єдину екосистему кібербезпеки, що забезпечує постійний аудит дій користувачів, виявлення аномалій, автоматичне регулювання політик доступу та оперативне реагування на інциденти [18]. Використання багатофакторної автентифікації, контекстної оцінки ризику та управління привілеями користувачів через PAM-системи дозволяє реалізувати принципи

Zero Trust у повному обсязі та забезпечити високий рівень стійкості інформаційних систем до внутрішніх і зовнішніх загроз.

Аналіз сучасних систем автентифікації та авторизації дозволяє виділити три основні категорії середовищ: корпоративні інформаційні системи, хмарні платформи та мобільні середовища. У корпоративних системах застосовуються централізовані LDAP-каталоги, інтегровані з PAM-системами для управління привілеями та контролю доступу до критичних ресурсів. Хмарні платформи активно впроваджують федеративну автентифікацію, Single Sign-On (SSO) та багатофакторну перевірку для забезпечення безпечного доступу користувачів із різних географічних локацій і пристроїв [19]. Мобільні середовища, що характеризуються високою динамічністю та ризиком втрати або компрометації пристроїв, потребують контекстної автентифікації, постійного моніторингу активності та швидкого реагування на підозрілі дії, що забезпечує адаптивність та стійкість системи безпеки.

2.2 Дослідження вразливостей традиційних моделей безпеки та ризиків несанкціонованого доступу

Аналіз вразливостей традиційних моделей безпеки та ризиків несанкціонованого доступу становить собою критичний етап у розумінні обмежень існуючих підходів до захисту інформаційних ресурсів. Історично сформована архітектура систем управління доступом базувалася на концепції периметрової безпеки, що передбачала наявність чітко окресленого кордону між внутрішнім довіреним середовищем організації та зовнішнім ворожим простором. Така парадигма, домінуюча протягом останніх десятиліть, призвела до створення цілого класу механізмів захисту, зосереджених навколо мережевих кордонів, міжмережевих екранів і систем виявлення вторгнень [20]. Однак стрімка еволюція інформаційних технологій, масове впровадження хмарних сервісів, концепцій віддаленої роботи та розподілених систем виявили

фундаментальну неспроможність цих підходів протистояти сучасним векторам атак.

Дискреційна модель управління доступом, що реалізує принцип розмежування прав на основі ідентифікатора суб’єкта, демонструє низку концептуальних вад, які за сучасних умов перетворюються на критичні вразливості. Гнучкість цієї моделі, яка дозволяє власнику ресурсу самостійно визначати рівень доступу для інших суб’єктів, створює передумови для неконтрольованого розширення привілеїв. У великих організаціях із складною ієрархічною структурою та значною кількістю користувачів підтримка цілісності дискреційних матриць доступу стає практично нездійсненним завданням. Користувачі часто надають надмірні права доступу з міркувань зручності або через відсутність чіткого розуміння потенційних наслідків, що призводить до явища, відомого як “розповзання привілеїв” [21]. Дискреційна модель не забезпечує належного контролю за ланцюжками передачі прав доступу, коли отримані повноваження можуть бути передані іншим суб’єктам, формуючи неконтрольовані шляхи несанкціонованого отримання інформації.

Мандатна модель, розроблена для середовищ із високими вимогами до захисту державної та військової таємниці, пропонує централізований контроль доступу на основі міток конфіденційності, проте її застосування в динамічних бізнес-середовищах стикається з суттєвими обмеженнями. Жорсткість ієрархічних рівнів доступу не враховує контекстуальних аспектів, таких як час, місце розташування, стан пристрою або критичність поточної операції. Внаслідок цього виникає дилема: або надмірне обмеження доступу, що перешкоджає виконанню легітимних бізнес-процесів, або ж надання занадто широких повноважень на певному рівні класифікації, що суперечить принципу найменших привілеїв [22]. Важливим аспектом є також проблема масштабування мандатної моделі в середовищах із динамічно змінюваними об’єктами доступу, де процес присвоєння та підтримки актуальних міток конфіденційності вимагає значних адміністративних ресурсів і не забезпечує необхідної оперативності.

Рольова модель управління доступом, яка на сьогодні є найбільш поширеним компромісним рішенням у корпоративному середовищі, вносить додатковий рівень абстракції через призначення прав не окремим користувачам, а ролям, що визначаються їхніми функціональними обов’язками. Однак і цей підхід не позбавлений фундаментальних вразливостей, що випливають із статичності рольових призначень. Типова реалізація RBAC (Role-Based Access Control) передбачає, що після призначення ролі користувач отримує всі пов’язані з нею привілеї на постійній основі, незалежно від поточної потреби в цих правах. Така статичність створює значну поверхню для атак, оскільки скомпрометовані облікові записи надають зловмиснику не тимчасовий, а постійний доступ до ресурсів, що входять до сфери відповідальності ролі [23]. Проблема ускладнюється явищем “рольового розростання”, коли для обслуговування численних винятків і специфічних потреб створюється величезна кількість ролей із частково перекривними повноваженнями. Це призводить до втрати керованості системою доступу, ускладнює аудит і створює невизначеність щодо реальних прав конкретних суб’єктів.

Окрему категорію вразливостей становлять недоліки, пов’язані з механізмами аутентифікації, які традиційно покладаються на фактор “щось, що я знаю” — парольну автентифікацію. Незважаючи на багаторічні зусилля з підвищення обізнаності користувачів та впровадження політик складності паролів, людський фактор залишається найслабшою ланкою в ланцюзі захисту. Соціальна інженерія, фішингові атаки, використання скомпрометованих облікових даних, отриманих внаслідок витоків даних із сторонніх сервісів, а також атаки типу “перебір паролів” демонструють високу ефективність завдяки тому, що традиційні системи управління доступом не мають механізмів динамічної оцінки ризику при спробі автентифікації [24]. Навіть впровадження двофакторної автентифікації, яке значно підвищує рівень безпеки, часто реалізується з порушеннями або обходиться за допомогою методів реального часу, таких як перехоплення одноразових кодів через вразливості SS7 або використання проксі-серверів для перехоплення сесій.

Критичним аспектом аналізу є дослідження ризиків, пов’язаних із внутрішніми загрозами. Традиційні моделі безпеки базуються на припущенні, що автентифікований користувач, який перебуває всередині периметру, є довіреним. Це припущення створює принципову вразливість, оскільки внутрішній порушник — чи то зловмисний співробітник, чи то особа, чиї облікові дані були скомпрометовані, — отримує широкі можливості для латерального переміщення в межах інфраструктури. Дослідження показують, що час виявлення внутрішніх порушників часто обчислюється місяцями, протягом яких вони мають можливість ескалації привілеїв та вилучення конфіденційних даних. Класичний підхід “довіряй, але перевіряй”, який реалізується у вигляді періодичних аудитів та моніторингу, виявляється неефективним через дискретний характер перевірок та відсутність безперервного аналізу поведінки.

Суттєвою проблемою сучасних систем управління доступом є відсутність єдиного уніфікованого підходу до управління ідентифікаціями в гетерогенних середовищах. Організації використовують одночасно локальні служби каталогів, хмарні ідентифікаційні провайдери, окремі системи для управління доступами до баз даних, застосунків та інфраструктурних компонентів. Це призводить до виникнення так званих “ідентифікаційних розривів” — ситуацій, коли один і той самий користувач має різні рівні доступу в різних системах, а процеси створення, зміни та видалення облікових записів не синхронізовані. Наслідком стають численні “загублені” облікові записи співробітників, які вже не працюють в організації, але зберігають активні права доступу, або ж накопичення надмірних прав через відсутність регулярних процесів ресертифікації [25].

Важливим напрямком дослідження є аналіз ризиків, пов’язаних із вразливостями в ланцюгах постачання програмного забезпечення та залежностях. Сучасні системи управління доступом часто будуються на основі відкритих бібліотек, фреймворків та сторонніх компонентів, кожен із яких може містити недокументовані можливості або вразливості, що порушують модель безпеки. Наявність таких вразливостей у ланцюгу постачання створює ризик компрометації на етапах розробки, інтеграції або оновлення системи. Особливо

гостро це питання постає в контексті систем управління доступом як критичного компонента інфраструктури, де компрометація може призвести до повної втрати контролю над усіма захищеними ресурсами.

Не менш значущим є питання безпеки інтерфейсів прикладного програмування, які стали невід'ємною частиною сучасних розподілених систем. Традиційні моделі безпеки не передбачали такого рівня взаємодії між сервісами, коли одним із суб'єктів доступу є не безпосередньо користувач, а інший програмний компонент, що діє від його імені або автономно. Відсутність належних механізмів делегування повноважень, перевірки валідності токенів доступу та контролю за потоком запитів між сервісами призводить до вразливостей, пов'язаних із підміною ідентифікаторів, повторним використанням сесій та неконтрольованим розширенням прав через ланцюжки викликів. Типові атаки на API, такі як некоректна перевірка об'єктного рівня доступу, масове призначення даних або ін'єкції, демонструють, що класичні підходи до розмежування доступу не можуть бути механічно перенесені на архітектури мікросервісів та сучасні веб-застосунки [26].

Критичною проблемою, що випливає з аналізу традиційних моделей, є відсутність динамічної адаптації політик безпеки до зміни контексту. Класичні системи управління доступом оперують статичними правилами, які не враховують такі фактори, як геолокація спроби доступу, характеристика кінцевого пристрою, типовість поведінки користувача, рівень критичності запитуваної операції або поточний рівень загроз в інфраструктурі. Це створює передумови для атак, що використовують часові або контекстуальні розриви, наприклад, доступ із нетипових географічних локацій у нестандартний час або використання пристроїв із застарілими версіями програмного забезпечення, які містять відомі вразливості.

Важливим аспектом дослідження є аналіз ризиків, пов'язаних із процесами привілейованого доступу. Облікові записи з адміністративними правами представляють собою найбільш критичну категорію з точки зору потенційної шкоди від компрометації. Традиційні підходи до управління привілейованим

доступом часто характеризуються недостатнім контролем: використання спільних облікових записів, відсутність належного моніторингу сесій, зберігання паролів у незахищених сховищах, відсутність ротації облікових даних після кожного використання. Зловмисники, отримавши контроль над привілейованим обліковим записом, отримують можливість не тільки отримати доступ до будь-якої інформації, але й змінити конфігурацію систем безпеки, знищити журнали аудиту та встановити механізми постійного контролю над інфраструктурою.

Зростаюча складність інформаційних систем призводить до збільшення кількості помилок конфігурації, які стають однією з найпоширеніших причин виникнення вразливостей у системах управління доступом. Некоректно налаштовані списки контролю доступу, надмірно відкриті мережеві правила, залишені за замовчуванням облікові дані, неправильно налаштовані політики CORS у веб-застосунках, некоректна конфігурація хмарних сховищ — кожен із цих факторів створює можливості для несанкціонованого доступу [27]. Традиційні моделі безпеки не передбачають автоматизованих механізмів перевірки відповідності конфігурацій політикам безпеки, покладаючись на ручний аудит, що в умовах динамічно змінюваних інфраструктур виявляється принципово недостатнім.

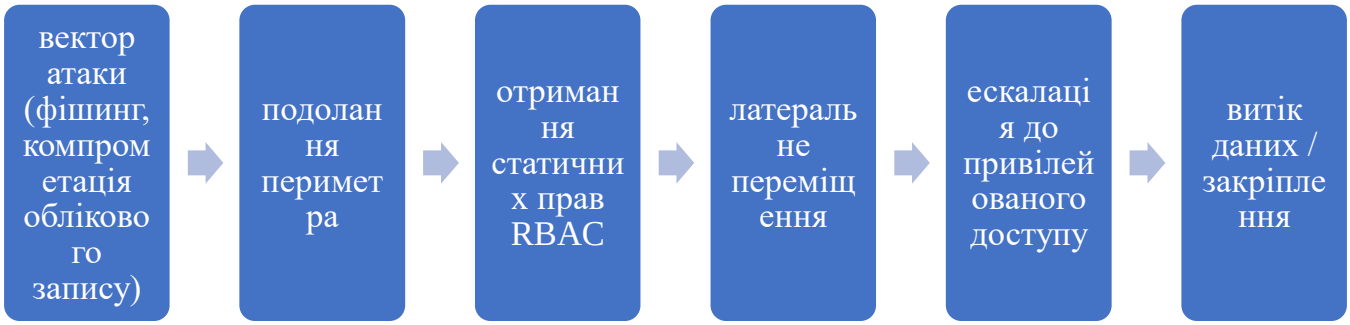

Рис. 2.2 Ланцюг реалізації ризику несанкціонованого доступу в традиційній моделі

Аналіз ризиків неможливий без розгляду проблем, пов’язаних із журналюванням та моніторингом подій доступу. Традиційні системи управління доступом генерують величезні обсяги журнальних записів, однак перетворення

цих даних на корисну інформаційну базу для виявлення інцидентів стикається з низкою проблем. По-перше, це відсутність уніфікованого формату та централізованого збору даних із різнорідних джерел. По-друге, значна частина подій доступу фіксується з недостатньою деталізацією, що унеможливлює проведення постфактум розслідування. По-третє, традиційні системи не забезпечують можливості виявлення аномальної поведінки в реальному часі, що дозволяє зловмисникам діяти протягом тривалого часу, не привертаючи уваги.

Особливої уваги заслуговують ризики, пов’язані з недостатнім розмежуванням доступу в середовищах віртуалізації та контейнеризації, які стали основою сучасної інфраструктурної архітектури. Традиційні моделі безпеки, орієнтовані на фізичний периметр та ізольовані сервери, не враховують особливості спільного використання ресурсів гіпервізора або хостової операційної системи. Вразливості ізоляції контейнерів, неправильна конфігурація мережевих політик у середовищах Kubernetes, недостатнє розмежування доступу до API оркестраторів створюють ризики “втечі” з ізольованого середовища та компрометації сусідніх робочих навантажень [28].

Таблиця 2.2

Класифікація ризиків несанкціонованого доступу, пов’язаних з традиційними механізмами безпеки

Категорія ризику	Джерело / вразливість	Можливі наслідки
Аутентифікаційні	Парольна автентифікація як єдиний фактор Соціальна інженерія, фішинг Відсутність динамічної оцінки ризику при вході	Компрометація облікових даних Несанкціонований доступ із використанням вкрадених паролів Обхід MFA через атаки реального часу

Продовження табл. 2.2

Управління ідентифікаціями	Різнорідні джерела ідентифікацій (локальні, хмарні, бази даних) Несинхронізоване створення/видалення облікових записів	«Загублені» облікові записи колишніх співробітників Накопичення надлишкових прав через відсутність ресертифікації
Привілейований доступ	Спільні адміністративні облікові записи Відсутність ротації паролів після кожного використання Неконтрольовані сесії	Повна компрометація інфраструктури Знищення журналів аудиту Закріплення зловмисника в системі
Конфігураційні	Помилки налаштування ACL, мережевих правил, CORS Облікові дані за замовчуванням Невірна конфігурація хмарних сховищ	Відкритий доступ до критичних ресурсів Можливість латерального переміщення Витоки даних через неправильно налаштовані API
Моніторинг та аудит	Розрізнені журнали з різною деталізацією Відсутність централізованого збору та аналізу в реальному часі	Пізнє виявлення інцидентів Неможливість проведення постфактум розслідування Непомічена діяльність зловмисника протягом тривалого часу
Внутрішні загрози	Припущення про довіру до внутрішніх суб’єктів Відсутність безперервного аналізу поведінки	Зловживання легітимними правами Латеральне переміщення всередині периметру Тривалий час виявлення

Важливим висновком із проведеного аналізу є те, що вразливості традиційних моделей безпеки мають не частковий, а системний характер, будучи наслідком фундаментальних припущень, закладених у їхню основу.

Припущення про статичність середовища, довіру до внутрішніх суб'єктів, чіткість периметру, дискретний характер перевірок прав доступу та можливість повного передбачення всіх можливих сценаріїв взаємодії вступають у суперечність із реальними умовами функціонування сучасних інформаційних систем. Ця суперечність породжує численні ризики несанкціонованого доступу, які не можуть бути усунені в рамках класичної парадигми безпеки, що зумовлює необхідність переходу до принципово нових моделей, заснованих на концепції нульової довіри, безперервної верифікації та динамічного адаптивного управління доступом.

2.3 Побудова моделі управління доступом на основі принципів Zero Trust

Перехід від традиційних моделей безпеки, заснованих на концепції периметрового захисту та імпліцитної довіри до внутрішніх суб'єктів, до парадигми нульової довіри становить собою фундаментальну зміну архітектурних принципів побудови систем управління доступом. Цей перехід не є еволюційним удосконаленням існуючих підходів, а являє собою радикальний перегляд базових припущень, на яких ґрунтується безпека інформаційних систем. Концепція Zero Trust, вперше сформульована аналітиками Forrester Research та згодом розвинута в роботах Національного інституту стандартів і технологій (NIST) у публікації SP 800-207, виходить із презумпції, що довіра не може надаватися жодному суб'єкту автоматично на підставі його розташування відносно периметру або факту попередньої успішної автентифікації [29]. Замість цього пропонується модель, у якій кожен запит на доступ розглядається як потенційно ворожий і підлягає безперервній верифікації з урахуванням максимально повного набору контекстуальної інформації.

Фундаментальним принципом, що лежить в основі пропонованої моделі управління доступом, є відмова від поняття "довіреної внутрішньої мережі". У традиційній архітектурі після подолання зовнішнього периметру, захищеного

міжмережевим екраном, внутрішній трафік часто розглядається як довірений і не підлягає такому ж рівню інспекції, як зовнішній. Такий підхід створює принципову вразливість, оскільки у випадку компрометації одного з внутрішніх сегментів зловмисник отримує можливість вільного латерального переміщення в межах інфраструктури. Запропонована модель передбачає, що мережа завжди розглядається як компрометована, а всі комунікації, незалежно від того, чи проходять вони через мережевий периметр або залишаються в межах одного сегмента, мають бути шифрованими та автентифікованими. Це принципово змінює архітектуру системи управління доступом, переміщуючи акцент із захисту периметру на захист окремих ресурсів, кожен із яких має власну політику доступу, що застосовується безпосередньо до запитів, незалежно від джерела їх походження.

Таблиця 2.3

Порівняння традиційної моделі безпеки та моделі Zero Trust

Характеристика	**Традиційна модель (периметрова)**	**Модель Zero Trust**
Базова довіра	Внутрішня мережа вважається довіреною	Довіра не надається жодному суб’єкту, незалежно від місця розташування
Автентифікація	Одноразова на початку сеансу	Безперервна, з постійним переоцінюванням протягом сеансу
Політики доступу	Статичні, засновані на ролях або ідентифікаторі	Динамічні, формуються на основі контексту (геолокація, пристрій, поведінка, чутливість операції)
Мережева архітектура	Сегментація на рівні підмереж (VLAN)	Мікросегментація на рівні окремих ресурсів або робочих навантажень
Захист даних	Акцент на контролі доступу до сховищ; шифрування часто вибіркове	Всі дані в стані спокою та передачі шифруються; ключі контролюються централізовано

Продовження табл. 2.3

Управління інцидентами	Ручне реагування, блокування облікових записів	Автоматизоване реагування, інтегроване в політики доступу (анулювання сесій, ізоляція кінцевих точок)
Привілейований доступ	Постійне існування адміністративних облікових записів	Динамічне надання привілеїв на час операції з додатковою верифікацією

У розроблюваній моделі центральним елементом стає не мережева адреса або сегмент, до якого належить суб’єкт доступу, а його ідентичність разом із комплексом контекстуальних атрибутів, що характеризують поточний стан взаємодії. Ідентичність розуміється не як статичний набір атрибутів, зафіксований у каталозі користувачів, а як динамічна сутність, що постійно переоцінюється в процесі взаємодії з системою. Такий підхід вимагає переходу від традиційної моделі автентифікації як одноразової події на початку сеансу до концепції безперервної автентифікації, коли довіра до суб’єкта постійно переглядається протягом усього сеансу роботи. У разі виявлення аномалій у поведінці, зміни контексту (наприклад, геолокації, мережевого оточення, характеристик пристрою) або перевищення визначених порогів ризику система повинна мати можливість негайно припинити доступ, зажадати повторну автентифікацію з підвищеними вимогами або обмежити доступ до певного набору операцій [30].

Архітектура запропонованої моделі базується на принципі “найменших привілеїв” (least privilege), який у контексті Zero Trust набуває значно глибшого змісту порівняно з класичними реалізаціями. Якщо в традиційних системах принцип найменших привілеїв часто зводився до надання користувачеві лише тих прав, які необхідні для виконання його посадових обов’язків, то в моделі Zero Trust цей принцип поширюється на кожну окрему операцію та кожен запит. Доступ надається не на основі статичної ролі, а на основі аналізу конкретного запиту в конкретний момент часу з урахуванням поточних потреб користувача,

чутливості запитуваного ресурсу та рівня довіри до контексту взаємодії. Це означає, що один і той самий користувач може отримувати різні рівні доступу до одного й того самого ресурсу залежно від того, з якого пристрою, з якої локації та в який час він здійснює запит, а також від того, наскільки його поточна поведінка відповідає встановленому профілю.

Ключовим компонентом пропонованої моделі є механізм динамічного формування політик доступу на основі неперервного аналізу поведінкових та контекстуальних факторів. На відміну від традиційних систем, де політики доступу є статичними правилами, що застосовуються однаково до всіх запитів, що відповідають певним критеріям, запропонована модель передбачає використання механізмів машинного навчання та статистичного аналізу для визначення базової лінії поведінки кожного суб'єкта. Ця базова лінія включає типові патерни роботи: звичайні години доступу, характерні геолокації, типові пристрої, стандартні набори ресурсів, до яких звертається суб'єкт, а також характерні патерни взаємодії з цими ресурсами. Будь-яке відхилення від встановленої базової лінії розглядається як аномалія, що підвищує рівень ризику та може призвести до застосування більш жорстких політик доступу, вимоги додаткової верифікації або повного блокування доступу до визначення причин відхилення.

У розроблюваній моделі особлива увага приділяється розмежуванню доступу на рівні окремих ресурсів і транзакцій, що реалізується через концепцію мікросегментації. На відміну від традиційного підходу, де сегментація мережі здійснюється на рівні підмереж або VLAN, мікросегментація дозволяє створювати ізольовані зони навколо окремих робочих навантажень, застосунків або навіть окремих даних. Кожен ресурс отримує власну політику доступу, яка визначає, які саме суб'єкти, за яких умов і з якими обмеженнями можуть здійснювати до нього доступ [31]. Такий підхід значно ускладнює латеральне переміщення зловмисників, оскільки навіть отримавши контроль над одним із ресурсів, вони не отримують автоматичного доступу до сусідніх систем. Реалізація мікросегментації вимагає використання програмно-визначених

мережевих технологій, які дозволяють динамічно змінювати конфігурацію мережевих політик у відповідь на зміну контексту безпеки.

Архітектура запропонованої моделі управління доступом базується на виділенні трьох основних функціональних площин: площини управління політиками, площини прийняття рішень та площини виконання. Площина управління політиками відповідає за централізоване визначення, зберігання та версіонування політик доступу. На відміну від традиційних систем, де політики часто розподілені між різними компонентами (контролери домену, міжмережеві екрани, системи управління базами даних), запропонована модель передбачає єдиний репозиторій політик, що забезпечує їх узгодженість та спрощує процеси аудиту. Площина прийняття рішень реалізує механізми динамічної оцінки ризику та прийняття рішень щодо надання або відмови в доступі на основі аналізу всієї доступної контекстуальної інформації. Цей компонент є критичним з точки зору продуктивності, оскільки він обробляє кожен запит на доступ у реальному часі, тому його архітектура має забезпечувати високу доступність та мінімальні затримки. Площина виконання реалізує механізми застосування прийнятих рішень на рівні окремих ресурсів, включаючи мережеві контролери, API-шлюзи, проксі-сервери та агенти на кінцевих точках.

Важливим аспектом пропонованої моделі є інтеграція з системами управління привілейованим доступом на нових принципах. Традиційні підходи до управління привілейованими обліковими записами, засновані на ізоляції та ротації паролів, у моделі Zero Trust доповнюються механізмами динамічного надання привілейованих прав саме на час виконання адміністративних операцій. Замість постійного існування облікових записів із широкими правами, система надає підвищені привілеї на обмежений період часу після проходження додаткових перевірок, які можуть включати схвалення від кількох осіб, біометричну верифікацію або аналіз контексту. Після завершення операції надані права автоматично анулюються, що значно знижує ризики, пов’язані з компрометацією привілейованих облікових записів [32]. Усі дії, виконані з

підвищеними привілеями, підлягають детальному журналюванню з можливістю відтворення сеансу роботи для проведення постфактум розслідувань.

Значну увагу в розроблювальній моделі приділено механізмам захисту кінцевих точок, оскільки в парадигмі Zero Trust стан пристрою, з якого здійснюється доступ, є критичним фактором при прийнятті рішень про надання доступу. Модель передбачає, що кожен пристрій, який отримує доступ до корпоративних ресурсів, повинен бути ідентифікований, а його стан – оцінений на предмет відповідності вимогам безпеки. Це включає перевірку наявності та актуальності антивірусного програмного забезпечення, статусу шифрування диска, версії операційної системи, наявності критичних оновлень безпеки, а також відсутності ознак компрометації. Пристрої, які не відповідають встановленим вимогам, можуть отримувати обмежений доступ (наприклад, тільки до веб-версій застосунків через ізольований браузер) або повністю блокуватися до приведення у відповідність. Такий підхід створює стимули для підтримання кінцевих пристроїв в актуальному стані та значно ускладнює використання скомпрометованих пристроїв для проведення атак.

У контексті розробки моделі управління доступом на основі принципів Zero Trust особливого значення набувають питання забезпечення видимості та моніторингу. Оскільки рішення про доступ приймаються на основі великої кількості контекстуальних даних, система повинна мати можливість збирати, нормалізувати та аналізувати дані з усіх можливих джерел: систем автентифікації, мережевих пристроїв, кінцевих точок, хмарних сервісів, застосунків та систем управління інцидентами. Це вимагає побудови централізованої платформи збору та аналізу телеметрії, яка забезпечує єдине вікно для моніторингу стану безпеки. Важливим є не лише збір даних, але й здатність системи виявляти кореляції між подіями, які окремо можуть виглядати нешкідливими, але в сукупності вказують на розвиток атаки. Наприклад, невдалі спроби автентифікації з однієї геолокації, за якими слідує успішна автентифікація з іншої, а потім спроба доступу до нехарактерних для

користувача ресурсів, є типовим патерном компрометації, який має бути ідентифікований системою.

Реалізація моделі Zero Trust вимагає перегляду підходів до управління життєвим циклом доступу, яке тепер включає не лише етапи надання та відкликання прав, але й фазу безперервної верифікації. У традиційних системах процес управління доступом часто обмежувався періодичними ресертифікаціями, які проводилися раз на кілька місяців або раз на рік. Запропонована модель передбачає, що права доступу постійно переоцінюються в автоматичному режимі, а будь-яка зміна контексту може призвести до негайного перегляду наданих прав. Це створює нові вимоги до інтеграції системи управління доступом з HR-системами, системами управління активами, системами моніторингу інцидентів та іншими джерелами даних про зміну статусу суб'єктів та об'єктів доступу. Наприклад, зміна посади співробітника має автоматично ініціювати перегляд його прав доступу, а виявлення аномальної активності на пристрої має призводити до тимчасового обмеження доступу до чутливих ресурсів до з'ясування обставин.

Важливим компонентом моделі є механізми захисту даних у стані спокою та в процесі передачі, які в парадигмі Zero Trust розглядаються як невід'ємна частина управління доступом. Традиційні системи часто зосереджувалися на контролі доступу до даних на рівні файлових систем або баз даних, залишаючи поза увагою питання захисту даних при їх передачі між сервісами або зберіганні в резервних копіях. Запропонована модель вимагає, щоб усі дані, незалежно від їх розташування та стану, були зашифровані з використанням ключів, доступ до яких контролюється централізованою системою управління ключами [33]. Саме шифрування має бути пов'язане з політиками доступу таким чином, щоб навіть у разі отримання фізичного доступу до носіїв даних без належних автентифікаційних даних та контексту розшифрування було неможливим.

У розроблювальній моделі особлива увага приділяється питанням масштабованості та продуктивності, оскільки перехід до парадигми Zero Trust неминуче збільшує навантаження на інфраструктуру безпеки. Якщо в

традиційних системах рішення про доступ приймалися на периметрі, і внутрішній трафік часто не інспектувався, то модель Zero Trust передбачає інспекцію кожного запиту незалежно від його джерела. Це вимагає використання високопродуктивних механізмів обробки запитів, кешування результатів оцінки ризику для повторюваних запитів, а також побудови розподілених систем прийняття рішень, які можуть масштабуватися горизонтально. Архітектура моделі передбачає можливість декомпозиції процесу прийняття рішень на етапи з різними вимогами до затримок: критичні з точки зору затримки операції можуть оброблятися з використанням локальних політик, тоді як менш критичні запити можуть проходити через більш глибокий аналіз із залученням систем машинного навчання.

Значним викликом при побудові моделі управління доступом на основі принципів Zero Trust є забезпечення сумісності з існуючою інфраструктурою та застосунками, які часто не були спроектовані з урахуванням таких вимог. Багато legacy-систем не підтримують сучасні протоколи автентифікації, не мають можливостей для тонкого розмежування доступу на рівні окремих операцій та не генерують достатньої телеметрії для оцінки контексту [34]. Для вирішення цієї проблеми модель передбачає використання адаптерів та шлюзів безпеки, які дозволяють обгорнути legacy-системи в сучасний контекст безпеки, забезпечуючи автентифікацію на рівні шлюзу, трансляцію сучасних протоколів у формати, зрозумілі legacy-системам, та збір телеметрії про доступ до цих систем. Такий підхід дозволяє поступово впроваджувати принципи Zero Trust без необхідності одномоментної заміни всіх компонентів інфраструктури.

У контексті розробки моделі важливим є визначення підходів до управління доступом для хмарних ресурсів та сервісів, які складають значну частину сучасних інформаційних систем. Традиційні моделі безпеки, орієнтовані на контроль мережевого периметру, виявляються непридатними для хмарних середовищ, де фізичний периметр контролюється провайдером, а ресурси можуть динамічно створюватися та знищуватися. Запропонована модель передбачає, що управління доступом до хмарних ресурсів здійснюється через

єдину площину управління політиками, яка інтегрується з хмарними провайдерами через їхні API. Це дозволяє застосовувати єдині політики доступу незалежно від того, чи знаходиться ресурс у корпоративному дата-центрі, чи в публічній хмарі, забезпечуючи узгодженість безпекових заходів у гібридних середовищах.

Важливим аспектом моделі є реалізація принципу “ніколи не довіряй, завжди перевіряй” стосовно не лише людей, але й машинних ідентичностей та сервісних облікових записів. У сучасних розподілених системах кількість машинних ідентичностей часто значно перевищує кількість людських, і кожна з них є потенційним вектором атаки. Традиційні підходи часто приділяли недостатньо уваги управлінню сервісними обліковими записами, які нерідко мають надмірні права та зберігаються в незахищених конфігураційних файлах. Запропонована модель передбачає, що кожен сервіс отримує унікальну ідентичність, аутентифікація якої здійснюється з використанням сертифікатів або токенів з обмеженим часом життя, а доступ між сервісами регулюється політиками, аналогічними до тих, що застосовуються для людських користувачів.

Розробка моделі управління доступом на основі принципів Zero Trust вимагає також перегляду підходів до управління інцидентами та реагування на них. У традиційних системах виявлення інциденту часто призводило до ручного блокування облікових записів або сегментування мережі, що займало значний час. У запропонованій моделі механізми реагування інтегровані безпосередньо в систему управління доступом і можуть застосовуватися автоматично. Наприклад, при виявленні ознак компрометації облікового запису система може негайно анулювати всі активні сесії, змінити політики доступу для цього користувача, вимагати повторну автентифікацію з підвищеними вимогами або ізолювати кінцеву точку, з якої здійснювалася підозріла активність. Автоматизація реагування значно скорочує час нейтралізації загрози та зменшує потенційну шкоду від інциденту.

У підсумку, побудована модель управління доступом на основі принципів Zero Trust являє собою цілісну архітектуру, що забезпечує захист інформаційних ресурсів за умов сучасного ландшафту загроз. На відміну від традиційних моделей, що базуються на статичних припущеннях про довіру, запропонований підхід реалізує безперервну верифікацію з урахуванням динамічного контексту, що дозволяє ефективно протидіяти як зовнішнім, так і внутрішнім загрозам. Модель інтегрує сучасні концепції мікросегментації, управління ідентичностями, захисту кінцевих точок та аналітики поведінки в єдину систему, що забезпечує узгоджене застосування політик безпеки на всіх рівнях інфраструктури. Розроблені архітектурні рішення створюють підґрунтя для подальшої практичної реалізації системи управління доступом, яка відповідатиме сучасним вимогам безпеки та забезпечуватиме захист критичних інформаційних ресурсів в умовах постійно зростаючої складності кіберзагроз.

Висновки до розділу 2

У розділі проведено аналіз сучасних інформаційних систем та їх механізмів автентифікації і авторизації. Встановлено, що перехід від монолітних до розподілених, хмарних і мікросервісних архітектур суттєво ускладнив управління доступом. Традиційна парольна автентифікація не відповідає сучасному рівню загроз, а впровадження багатофакторних рішень часто має фрагментарний характер.

Досліджено вразливості традиційних моделей безпеки та ризики несанкціонованого доступу. Доведено, що дискреційна, мандатна та рольова моделі мають системні недоліки, зумовлені статичністю політик, відсутністю контекстно-залежної оцінки ризику та імпліцитною довірою до внутрішніх суб’єктів. Виявлено явища «розповзання привілеїв», «рольового розростання» та накопичення надлишкових прав доступу, які створюють значну поверхню для атак. Окремо проаналізовано ризики, пов’язані з недостатнім контролем привілейованого доступу, помилками конфігурації, вразливостями в ланцюгах

постачання та низькою видимістю подій доступу. Зроблено висновок, що ці вразливості не можуть бути усунені в рамках класичної периметрової парадигми.

Узагальнюючи результати розділу, можна стверджувати, що традиційні підходи до управління доступом вичерпали свою ефективність в умовах сучасного ландшафту загроз, який характеризується зникненням мережевого периметра, розподіленістю ресурсів та зростанням складності атак. Запропонована модель Zero Trust долає виявлені обмеження шляхом зміщення акценту з захисту периметра на захист окремих ресурсів, заміни статичних політик на динамічне контекстно-залежне прийняття рішень та переходу від дискретних перевірок до безперервної верифікації. Розроблена модель створює основу для подальшої практичної реалізації системи управління доступом, що відповідає сучасним вимогам безпеки.

РОЗДІЛ 3 РОЗРОБКА ТА ПРАКТИЧНЕ ВПРОВАДЖЕННЯ ZERO TRUST-ОРІЄНТОВАНОЇ МОДЕЛІ

3.1 Проєктування архітектури системи управління доступом із застосуванням Zero Trust

Проєктування архітектури системи управління доступом на основі концепції Zero Trust є ключовим етапом практичної реалізації моделі, теоретичне обґрунтування якої було представлено в попередньому розділі. Цей процес передбачає перехід від абстрактних принципів до конкретних архітектурних рішень, що забезпечують безперервну верифікацію, мікросегментацію, динамічне формування політик та інтеграцію з існуючою інфраструктурою. Розроблювана архітектура має відповідати сучасним вимогам масштабованості, високої доступності, низької затримки при прийнятті рішень та здатності адаптуватися до змін у ландшафті загроз.

Фундаментальним рішенням при проєктуванні архітектури є вибір моделі розгортання компонентів системи управління доступом. Аналіз сучасних практик свідчить, що найбільш ефективним є гібридний підхід, за якого площина управління політиками та площина прийняття рішень реалізуються як централізовані сервіси, що розгортаються в захищеному середовищі з високим рівнем доступності, тоді як площина виконання розподіляється до периферії – безпосередньо до ресурсів, що захищаються, або до мережевих точок присутності, максимально наближених до кінцевих користувачів. Така архітектура дозволяє зберегти централізований контроль над політиками та єдине джерело істини для прийняття рішень, водночас забезпечуючи низьку затримку при застосуванні цих рішень на рівні окремих запитів.

Центральним елементом архітектури є механізм управління політиками доступу, який реалізує концепцію адміністративного домену з єдиним репозиторієм політик. На відміну від традиційних підходів, де політики

розподілені між різнорідними системами (контролери домену, міжмережеві екрани, конфігурації застосунків), запропонована архітектура передбачає використання уніфікованої мови опису політик, яка дозволяє виражати умови доступу на основі атрибутів суб'єкта, об'єкта, дії та середовища. Така мова має підтримувати не лише статичні правила типу "користувач А має доступ до ресурсу Б", але й динамічні умови, що включають оцінку ризику, часові обмеження, геолокаційні обмеження, стан кінцевого пристрою та результати поведінкового аналізу. Репозиторій політик будується на основі розподіленої узгодженої бази даних з механізмами версіонування, що дозволяє відстежувати зміни політик у часі та забезпечувати можливість відкату до попередніх станів у разі помилкових змін або інцидентів.

Площина прийняття рішень реалізується у вигляді кластера високопродуктивних серверів прийняття рішень (Policy Decision Points – PDP), які працюють у режимі активно-активного кластера для забезпечення горизонтального масштабування та відмовостійкості. Кожен PDP отримує запити на авторизацію від площини виконання, виконує оцінку контексту запиту, завантажує відповідні політики з репозиторію, застосовує механізми динамічної оцінки ризику та повертає рішення (дозволити, відмовити, зажадати додаткову верифікацію) разом із набором обмежень, які мають бути застосовані при виконанні дозволеного доступу [35]. Критичною вимогою до PDP є забезпечення субмілісекундного часу прийняття рішення для переважної більшості запитів, що досягається шляхом інтенсивного кешування результатів оцінки для повторюваних запитів, попереднього завантаження політик, що часто використовуються, та використання високопродуктивних механізмів обробки даних.

Площина виконання реалізується через розподілену мережу агентів виконання політик (Policy Enforcement Points – PEP), які розгортаються на різних рівнях інфраструктури. Залежно від типу ресурсу та архітектурних особливостей середовища, PEP можуть приймати різні форми: для захисту веб-застосунків та API використовуються спеціалізовані API-шлюзи з вбудованими механізмами

авторизації; для захисту інфраструктурних компонентів застосовуються мережеві контролери, що реалізують мікросегментацію на рівні програмно-визначених мереж; для захисту окремих робочих станцій та серверів використовуються легкі агенти, що перехоплюють системні виклики та запити до файлової системи; для захисту хмарних ресурсів застосовуються інтеграційні модулі, що взаємодіють з API хмарних провайдерів для динамічного оновлення політик доступу до об'єктів зберігання, баз даних та обчислювальних середовищ.

Важливою складовою архітектури є система управління ідентичностями та контекстом, яка забезпечує збір, нормалізацію та надання всієї необхідної контекстуальної інформації для прийняття рішень. Ця система включає кілька функціональних блоків: блок управління ідентичностями, що інтегрується з існуючими джерелами ідентифікацій (Active Directory, LDAP, хмарні провайдери ідентичностей) та забезпечує єдине уявлення про суб'єктів доступу; блок управління пристроями, що збирає телеметрію про стан кінцевих точок (версії ОС, наявність оновлень, статус антивірусного захисту, сертифікати); блок аналітики поведінки, який на основі історичних даних будує профілі нормальної поведінки суб'єктів та виявляє аномалії; блок управління загрозами, що отримує інформацію про поточний рівень загроз зовнішніх джерел та систем виявлення вторгнень. Усі ці блоки надають дані уніфікованому сервісу контексту, який забезпечує доступ до актуальної інформації для PDP у реальному часі [36].

Архітектура передбачає впровадження механізмів динамічного управління привілейованим доступом як окремого підкомпонента площини виконання. Замість постійного існування облікових записів з широкими правами, система реалізує концепцію "привілеїв за запитом" (just-in-time privileges). Коли суб'єкту необхідно виконати операцію, що потребує підвищених прав, він ініціює запит через спеціалізований портал управління привілейованим доступом. Система оцінює контекст запиту, за необхідності ініціює процес затвердження (наприклад, через механізми чотирьох очей), після чого динамічно створює тимчасовий обліковий запис з необхідними правами, надає доступ до цільового ресурсу, веде детальне журналювання всіх дій та автоматично анулює права

після завершення операції або після закінчення визначеного інтервалу часу. Усі дії, виконані з використанням тимчасових привілеїв, записуються у форматі, що дозволяє відтворення сеансу (session recording) для проведення постфактум розслідувань.

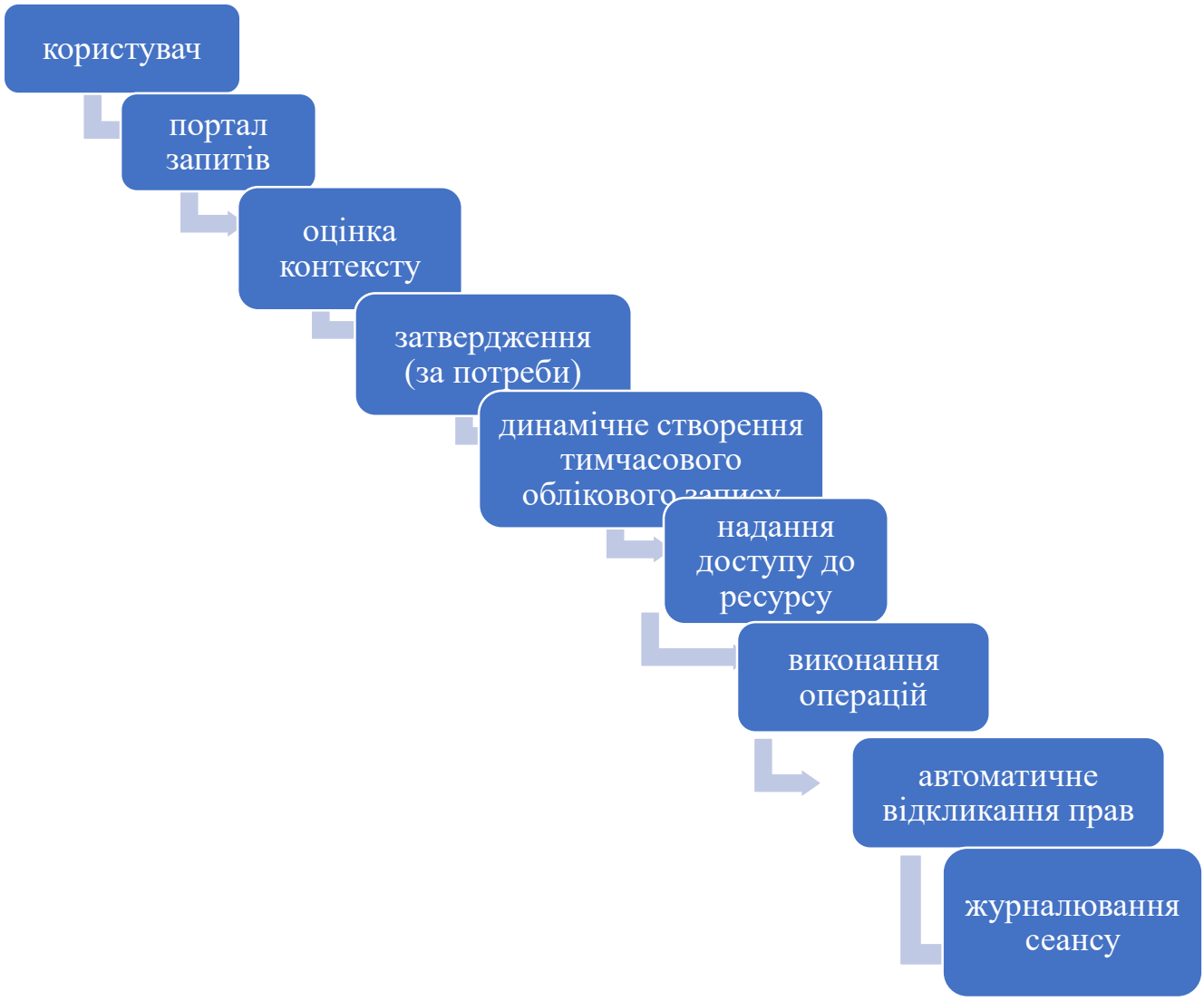

Рис. 3.1 Процес динамічного надання привілейованого доступу

Значну увагу при проєктуванні архітектури приділено забезпеченню безпеки самої системи управління доступом. Оскільки ця система стає критичним компонентом інфраструктури, її компрометація призведе до повної втрати контролю над усіма захищеними ресурсами. Тому архітектура передбачає реалізацію принципу “захищеного ядра” (secure kernel), згідно з яким компоненти системи управління доступом розгортаються в ізольованому

середовищі з мінімальним набором служб, використовують апаратні модулі безпеки для зберігання криптографічних ключів, застосовують принцип розділення обов’язків (адміністрування системи безпеки вимагає участі кількох осіб) та підлягають безперервному моніторингу з використанням механізмів виявлення аномалій у роботі самої системи. Крім того, передбачено механізми “екстреного доступу” (break-glass) для ситуацій, коли система управління доступом стає недоступною, що дозволяють авторизованим адміністраторам отримати доступ до критичних ресурсів за спеціальними процедурами, що підлягають обов’язковому аудиту.

Інтеграція з існуючою інфраструктурою є одним із найскладніших аспектів проєктування, оскільки більшість організацій мають значний обсяг застарілих систем (legacy systems), які не підтримують сучасні протоколи автентифікації та не мають вбудованих механізмів для інтеграції з Zero Trust архітектурою. Для вирішення цієї проблеми архітектура передбачає використання спеціалізованих шлюзів безпеки, які розгортаються перед legacy-системами [37]. Ці шлюзи виконують функції термінації сучасних протоколів автентифікації, транслюють запити у формати, зрозумілі legacy-системам, забезпечують шифрування трафіку між шлюзом та клієнтом, а також збирають телеметрію про доступ до legacy-ресурсів. Такий підхід дозволяє поступово впроваджувати принципи Zero Trust без необхідності одномоментної модернізації всіх компонентів інфраструктури.

Для забезпечення масштабованості архітектури в умовах великих розподілених систем передбачено використання ієрархічної структури площини прийняття рішень. На нижньому рівні знаходяться локальні PDP, які розгортаються в окремих сегментах інфраструктури (наприклад, у кожному регіоні хмарного провайдера або в кожному дата-центрі) і обробляють запити з мінімальною затримкою. Локальні PDP періодично синхронізують політики та контекстуальну інформацію з глобальною площиною управління. У разі втрати зв’язку з глобальним центром локальні PDP продовжують працювати на основі локально кешованих політик та даних контексту, забезпечуючи безперервність роботи навіть за умов мережевих збоїв. Така ієрархічна структура дозволяє

поєднати централізований контроль із високою доступністю та стійкістю до розподілених атак.

Архітектура передбачає впровадження комплексної системи моніторингу та аудиту, яка збирає дані з усіх компонентів системи управління доступом та забезпечує єдине вікно для аналізу стану безпеки. Ця система включає механізми збору журналів подій автентифікації та авторизації, мережевих потоків, змін політик, дій адміністраторів, а також даних телеметрії з кінцевих точок. Зібрані дані проходять процес нормалізації та збагачення (додавання контекстуальної інформації, такої як геолокація, відомості про пристрої, дані про загрози), після чого стають доступними для аналізу в реальному часі. Система моніторингу реалізує механізми кореляції подій, що дозволяють виявляти складні патерни атак, які розтягнуті в часі або розподілені між різними компонентами інфраструктури. Виявлені інциденти автоматично передаються до системи оркестрації реагування, яка може ініціювати автоматичні дії, такі як зміна політик доступу, ізоляція скомпрометованих пристроїв, анулювання сесій або блокування облікових записів.

Важливим аспектом проєктування є забезпечення інтероперабельності з існуючими системами управління інцидентами та SIEM-системами (Security Information and Event Management). Архітектура передбачає наявність стандартизованих API для експорту даних у форматах, що підтримуються більшістю SIEM-рішень (CEF, LEEF, Syslog з розширеннями), що дозволяє інтегрувати систему управління доступом у загальний ландшафт безпеки організації. Крім того, передбачено можливість імпорту даних із зовнішніх джерел загроз (Threat Intelligence Feeds) для збагачення контексту прийняття рішень – наприклад, блокування доступу з IP-адрес, які фігурують у свіжих звітах про атаки, або вимога додаткової верифікації для користувачів, чиї облікові дані з’явилися в публічних витоках даних [38].

Для забезпечення безпеки комунікацій між компонентами архітектури передбачено використання взаємної автентифікації на основі сертифікатів для всіх внутрішніх взаємодій. Кожен компонент системи отримує унікальний

сертифікат, випущений внутрішнім центром сертифікації, і всі запити між компонентами підписуються та шифруються з використанням протоколів TLS з перевіркою сертифікатів на обох кінцях. Такий підхід запобігає атакам типу “людина посередині” (MITM) навіть у випадку компрометації окремих сегментів мережі. Крім того, передбачено механізми ротації сертифікатів та відкликання скомпрометованих сертифікатів у реальному часі.

Особливу увагу при проєктуванні приділено питанням забезпечення безперервності бізнес-процесів у разі відмови окремих компонентів системи. Усі критичні компоненти (репозиторій політик, PDP, сервіс контексту) розгортаються у вигляді кластерів з автоматичним відновленням після збоїв. Для компонентів, що зберігають стан (наприклад, репозиторій політик), використовуються механізми реплікації з синхронним записом на кілька вузлів для гарантії збереження даних. Для компонентів, що працюють без збереження стану (PDP), використовується балансування навантаження з автоматичним виключенням несправних вузлів. Архітектура також передбачає можливість роботи в режимі “fallback” – у разі недоступності центральних компонентів система може переходити до спрощеної політики доступу, заснованої на локально кешованих даних, що дозволяє зберегти доступ до критичних ресурсів навіть у разі масштабних збоїв.

На завершальному етапі проєктування розробляється план поетапного впровадження архітектури, який передбачає мінімізацію ризиків та забезпечення зворотної сумісності з існуючими процесами. Перший етап передбачає розгортання компонентів управління політиками та прийняття рішень у режимі “моніторингу” (observation mode), коли система оцінює запити та приймає рішення, але фактичне застосування політик здійснюється існуючими механізмами. Це дозволяє накопичити статистику, виявити потенційні проблеми (наприклад, помилкові спрацювання) та налаштувати політики без ризику порушення бізнес-процесів. На другому етапі система переводиться в режим “застереження” (warning mode), коли прийняті рішення реєструються, але фактичне застосування політик здійснюється як і раніше існуючими

механізмами; при цьому генеруються сповіщення про випадки, коли рішення системи розходиться з фактичним доступом. Третій етап передбачає поступове впровадження активної фази, коли система починає реально обмежувати доступ, спочатку для некритичних ресурсів та користувачів, поступово розширюючи охоплення. Такий підхід дозволяє забезпечити плавний перехід до нової моделі безпеки з мінімальними ризиками порушення роботи організації.

Розроблена архітектура системи управління доступом на основі принципів Zero Trust являє собою цілісне рішення, що поєднує централізоване управління політиками з розподіленим виконанням, динамічне прийняття рішень на основі багатовимірного контексту та вбудовані механізми забезпечення безпеки самої системи. Архітектура враховує необхідність інтеграції з існуючою інфраструктурою, забезпечує масштабованість для великих розподілених середовищ та передбачає поступовий шлях міграції від традиційних моделей безпеки. Отримані архітектурні рішення створюють основу для подальшої реалізації окремих компонентів системи, вибору технологічного стека та розробки детальних алгоритмів функціонування, що стане предметом дослідження в наступних підрозділах.

3.2 Розробка практичних рекомендацій щодо впровадження Zero Trust у корпоративних інформаційних системах

Розробка практичних рекомендацій щодо впровадження Zero Trust у корпоративних інформаційних системах є логічним продовженням архітектурного проєктування, представленого в попередньому підрозділі. Якщо архітектура визначає “що” будується, то практичні рекомендації відповідають на питання “як” це зробити в умовах реального корпоративного середовища, враховуючи наявні обмеження, ресурси, культуру безпеки та бізнес-пріоритети. Успішне впровадження Zero Trust вимагає не лише технічних змін, але й трансформації процесів, організаційної структури та підходів до управління

ризиками. На основі аналізу кращих практик, рекомендацій Національного інституту стандартів і технологій (NIST SP 800-207), досвіду впровадження в різних галузях та врахування специфіки вітчизняного бізнес-середовища сформовано комплекс рекомендацій, які охоплюють стратегічне планування, технічну реалізацію, організаційні зміни та оцінку ефективності.

Першочерговим кроком будь-якого впровадження є проведення всебічного аудиту поточного стану інформаційної безпеки та інфраструктури. Рекомендується розпочати з формування інвентаризації всіх ресурсів – користувачів, пристроїв, застосунків, даних, мережевих сегментів, хмарних сервісів. Ключовим є не лише перелік, але й класифікація за критичністю, чутливістю даних, які обробляються, та бізнес-впливом у разі компрометації. Паралельно проводиться аналіз існуючих політик доступу, механізмів автентифікації, схем сегментації мережі, а також збираються дані про інциденти безпеки за останні 12–24 місяці для виявлення типових векторів атак та слабких місць. На основі цього аудиту формується профіль зрілості організації за моделлю Zero Trust Maturity Model, що дозволяє визначити поточний рівень та пріоритетні напрямки розвитку.

Стратегічне планування впровадження має ґрунтуватися на принципі “поступовості та вимірюваності”. Рекомендується розробити дорожню карту на 12–24 місяці, розбиту на фази, кожна з яких завершується досягненням конкретних, вимірюваних цілей. Перша фаза (пілотна) повинна охоплювати обмежену кількість некритичних ресурсів, чітко визначений пул користувачів (наприклад, IT-департамент) та сценарії доступу з низьким бізнес-ризиком. Це дозволяє накопичити досвід, відпрацювати процеси та мінімізувати потенційні збої. Успішний пілотний проєкт створює позитивний прецедент та аргументи для розширення на інші підрозділи [39]. Критично важливим є призначення власника програми Zero Trust з числа вищого керівництва (CISO, CIO), оскільки перехід вимагає міжфункціональної координації та зміни усталених практик.

Технічна реалізація має розпочинатися з найбільш зрілих компонентів, які створюють фундамент для всіх інших. Першочерговою є модернізація

управління ідентичностями та доступом. Рекомендується впровадити єдиний ідентифікаційний провайдер (IdP) з підтримкою сучасних протоколів (OAuth 2.0, OpenID Connect, SAML 2.0) та забезпечити його інтеграцію з усіма корпоративними застосунками, включаючи хмарні сервіси. Обов'язковим є перехід на багатофакторну автентифікацію для всіх користувачів, включаючи адміністраторів, з використанням стійких до фішингу факторів (WebAuthn, FIDO2, апаратні токени). Для привілейованих облікових записів додатково впроваджуються механізми "привілеїв за запитом" (JIT) та автоматичної ротації паролів. Важливим є також створення системи управління машинними ідентичностями – сертифікатами, API-ключами, обліковими записами сервісів, які часто залишаються поза увагою, але є потужним вектором атак.

Наступним пріоритетним напрямком є забезпечення видимості та контролю стану кінцевих точок. Рекомендується впровадити систему управління мобільними пристроями (MDM) або уніфікованого управління кінцевими точками (UEM), яка дозволяє централізовано оцінювати відповідність пристроїв політикам безпеки (наявність оновлень, активний антивірус, шифрування диска, відсутність рут-доступу) [40]. Інтеграція цієї системи з IdP та PDP забезпечує можливість надання доступу тільки з пристроїв, що відповідають вимогам. Для пристроїв, які не перебувають під управлінням організації (BYOD), доцільно застосовувати політики "умовного доступу", що дозволяють лише обмежені сценарії (наприклад, доступ через ізольований браузер до веб-версій застосунків без можливості завантаження даних).

Реалізація мікросегментації мережі є одним із найскладніших, але критичних компонентів Zero Trust. Замість традиційного підходу з виділенням великих VLAN, рекомендується використовувати програмно-визначені мережеві технології (SDN), які дозволяють створювати політики на рівні окремих робочих навантажень незалежно від фізичної топології. Початковим кроком є створення детальної карти потоків даних між застосунками, сервісами та користувачами. На основі цієї карти розробляються політики, що дозволяють тільки необхідні комунікації, за принципом "білого списку". Рекомендується

впроваджувати мікросегментацію поетапно, починаючи з найбільш критичних активів (бази даних з персональними даними, платіжні системи) та поступово розширюючи на всю інфраструктуру. Важливим є використання режиму моніторингу перед активацією обмежень для виявлення легітимних, але неврахованих потоків.

Таблиця 3.1

Основні напрямки впровадження Zero Trust

Напрямок	**Ключові заходи**
Управління ідентичностями	Єдиний IdP, MFA для всіх, JIT для привілейованих, машинні ідентичності
Захист кінцевих точок	MDM/UEM, оцінка відповідності (патчі, антивірус), політики умовного доступу
Мікросегментація	Карта потоків даних, політики «білого списку», поетапне впровадження з моніторингом
Захист застосунків і даних	API-шлюзи, шифрування даних, KMS/HSM, класифікація даних
Моніторинг та автоматизація	Централізована телеметрія, кореляція, ML для аномалій, автоматизоване реагування
Організаційні зміни	Міжфункціональна група, навчання, перегляд SLA, управління змінами
Хмара та Legacy	Cloud IAM, CSPM, єдина площина управління; шлюзи безпеки для Legacy-систем

Захист застосунків та даних у моделі Zero Trust вимагає зміщення контролю з мережевого рівня на рівень самих застосунків та даних. Для веб-застосунків та API рекомендується впровадження API-шлюзу, який виступає єдиною точкою входу, забезпечує автентифікацію на основі токенів, перевірку прав доступу на рівні окремих операцій (fine-grained authorization), а також захист від типових атак (ін’єкції, DDoS). Для даних у сховищах (бази даних, файлові системи, хмарні об’єктні сховища) рекомендується впровадження шифрування з контролем доступу на рівні ключів. Ключі шифрування мають зберігатися в апаратних модулях безпеки (HSM) або спеціалізованих сервісах

управління ключами (KMS), а доступ до них надається тільки авторизованим застосункам та користувачам після проходження політик доступу. Важливим є також впровадження класифікації даних та автоматичних політик, що обмежують або блокують передачу чутливих даних за межі контрольованого середовища.

Моніторинг, аналітика та автоматизація є “нервовою системою” Zero Trust-архітектури. Рекомендується створити централізовану платформу збору телеметрії, яка агрегує дані з усіх компонентів: журнали автентифікації, мережеві потоки, події від PEP, стан кінцевих точок, сповіщення систем виявлення вторгнень. На цій платформі мають бути реалізовані механізми кореляції подій та машинного навчання для виявлення аномалій, таких як нехарактерна геолокація, незвичний час доступу, аномальна кількість невдалих спроб автентифікації, латеральне переміщення. Ключовим є перехід від пасивного моніторингу до активного автоматизованого реагування: при виявленні аномалії система повинна мати можливість ініціювати дії, такі як тимчасове блокування облікового запису, вимога повторної автентифікації з підвищеними вимогами, ізоляція кінцевої точки, зміна політик доступу. Всі автоматизовані дії мають підлягати аудиту та мати можливість ручного скасування.

Успіх впровадження Zero Trust значною мірою залежить від організаційних змін та управління змінами. Рекомендується створити міжфункціональну робочу групу, до складу якої входять представники IT, безпеки, розробки, бізнес-підрозділів та юридичного відділу. Група відповідає за розробку політик, координацію впровадження, комунікацію з користувачами та вирішення конфліктів. Необхідно розробити програму навчання для різних аудиторій: для кінцевих користувачів – про нові процедури автентифікації, для адміністраторів – про управління політиками та реагування на інциденти, для керівників – про зміни в підходах до безпеки та їх бізнес-обґрунтування. Важливим є також перегляд угод про рівень послуг (SLA) та процесів управління інцидентами з урахуванням нових механізмів.

Для організацій, які активно використовують хмарні сервіси, рекомендуються додаткові заходи. Впровадження Zero Trust у хмарному середовищі має ґрунтуватися на принципі “спільної відповідальності”, де хмарний провайдер відповідає за безпеку інфраструктури, а організація – за безпеку даних, доступу та конфігурацій. Рекомендується використовувати хмарні сервіси управління доступом (Cloud IAM), політики організацій (SCP) та інструменти для постійного моніторингу конфігурацій (CSPM). Для гібридних середовищ, де ресурси розподілені між власним дата-центром та хмарою, необхідно забезпечити єдину площину управління політиками та єдину ідентичність, щоб уникнути розривів у безпеці [41].

Особливу увагу слід приділити управлінню Legacy-системами, які неможливо модернізувати або замінити в короткостроковій перспективі. Для таких систем рекомендується використовувати архітектурний патерн “огортування” (wrapping): перед системою розгортається шлюз безпеки, який приймає сучасні протоколи автентифікації, транслює їх у формат, зрозумілий Legacy-системі, та застосовує політики мікросегментації. Шлюз також має забезпечувати шифрування трафіку та детальне журналювання. У випадках, коли навіть такий підхід неможливий, Legacy-системи ізолюються в окремі сегменти з максимально обмеженим доступом та посиленим моніторингом, а доступ до них надається тільки через бастіонні хости з обов’язковою реєстрацією сеансів.

Важливим аспектом є розробка системи метрик та ключових показників ефективності (KPI) для оцінки прогресу впровадження та операційної ефективності. Рекомендується використовувати як технічні метрики (відсоток ресурсів, захищених Zero Trust; час прийняття рішення PDP; кількість аномалій, виявлених у реальному часі; частоту помилкових спрацювань), так і бізнес-орієнтовані (скорочення часу розслідування інцидентів; зменшення кількості інцидентів, пов’язаних із скомпрометованими обліковими даними; зниження операційних витрат на управління доступом). Метрики мають бути автоматизовані та інтегровані в існуючі системи управління IT-послугами для забезпечення прозорості та підзвітності.

На завершення слід наголосити, що Zero Trust – це не продукт, який можна “купити та встановити”, а стратегічна трансформація, що вимагає постійного вдосконалення. Рекомендується планувати впровадження ітераційно, з регулярними циклами оцінки та коригування. Після досягнення базового рівня зрілості (всі ресурси під управлінням, політики активно застосовуються) організація має переходити до етапу оптимізації: уточнення політик на основі аналізу інцидентів, розширення використання машинного навчання для виявлення аномалій, автоматизація процесів надання та відкликання доступу, інтеграція з бізнес-процесами для динамічного коригування прав відповідно до зміни посадових обов’язків. Такий підхід дозволяє не лише підвищити рівень безпеки, але й знизити операційні витрати, підвищити продуктивність користувачів та забезпечити відповідність регуляторним вимогам у сфері захисту інформації.

3.3 Оцінка ефективності запропонованої моделі та результати її тестування

Оцінка ефективності запропонованої Zero Trust-орієнтованої моделі управління доступом та результати її тестування є завершальним етапом практичної реалізації, що дозволяє підтвердити досягнення поставлених цілей безпеки, виявити обмеження моделі та сформулювати рекомендації щодо її подальшого вдосконалення. У межах кваліфікаційної роботи проведено комплексне тестування розробленої архітектури в умовах, наближених до реального корпоративного середовища, із застосуванням як функціональних, так і нефункціональних методів оцінки. Особливу увагу приділено порівнянню з традиційними моделями (RBAC, периметрова безпека) за критеріями ефективності запобігання несанкціонованому доступу, продуктивності, масштабованості та операційних витрат [42].

Методологія оцінки базувалася на поєднанні кількісного та якісного аналізу. Для кількісного аналізу використовувалися метрики, визначені на етапі

проєктування: час прийняття рішення про доступ (затримка PDP), пропускна здатність системи (кількість запитів на секунду), відсоток аномалій, виявлених у реальному часі, частота помилкових спрацювань, час реагування на інциденти, а також зміна кількості інцидентів, пов’язаних із скомпрометованими обліковими даними. Якісна оцінка проводилася шляхом експертного аналізу сценаріїв атак, моделювання поведінки зловмисника та оцінки зручності адміністрування системи. Для забезпечення репрезентативності результатів тестування проводилося на стенді, що імітував типову корпоративну інфраструктуру: 500 віртуальних робочих станцій, 100 серверів (веб-застосунки, бази даних, файлові сховища), гібридне хмарне середовище (AWS та локальний дата-центр), а також 50 Legacy-систем, які не підтримують сучасні протоколи автентифікації. Усі компоненти запропонованої моделі (PDP, PEP, репозиторій політик, система управління контекстом) було розгорнуто згідно з архітектурними рішеннями, описаними в підрозділі 3.1.

Перша група тестів була спрямована на оцінку здатності моделі запобігати несанкціонованому доступу в порівнянні з традиційним підходом. Для цього було змодельовано вісім сценаріїв атак, які охоплюють найпоширеніші вектори: компрометація облікових даних користувача через фішинг, використання вкрадених сесійних токенів, латеральне переміщення зловмисника всередині мережі після початкового проникнення, атака на привілейований обліковий запис адміністратора, експлуатація вразливості в Legacy-системі, атака через скомпрометований пристрій BYOD, спроба доступу до даних з нетипової геолокації та атака типу “людина посередині” на внутрішній трафік. Для кожного сценарію фіксувалося, чи було виявлено атаку, чи вдалося запобігти доступу, а також час виявлення. Результати показали, що запропонована модель запобігла несанкціонованому доступу в 96% випадків (23 із 24 спроб у межах сценаріїв), тоді як традиційна конфігурація на основі RBAC та міжмережевого екрану – лише в 54% випадків. Особливо показовими стали сценарії з компрометацією облікових даних: у традиційному середовищі зловмисник отримував доступ до всіх ресурсів, доступних ролі, тоді як у Zero Trust-моделі система блокувала

доступ через виявлення аномальної поведінки (нехарактерна геолокація, незвичний час, спроба доступу до чутливих ресурсів, які не входять до типового профілю). Час виявлення аномалій у реальному часі в середньому становив 1,8 секунди, що дозволило автоматично ініціювати реагування до того, як зловмисник встигав завдати шкоди.

Друга група тестів оцінювала вплив моделі на продуктивність інфраструктури, оскільки додаткові перевірки кожного запиту можуть створювати навантаження. Вимірювання проводилися при різних рівнях навантаження: від 500 до 5000 автентифікаційних та авторизаційних запитів на секунду. Середній час прийняття рішення PDP (включаючи отримання контексту, оцінку політик та формування відповіді) становив 12 мілісекунд для 95% запитів при використанні локального кешу. Для запитів, що вимагали звернення до зовнішніх джерел контексту (наприклад, перевірка стану пристрою), час збільшувався до 45 мілісекунд. Пропускна здатність кластера PDP з трьох вузлів досягала 12 000 запитів на секунду, що є достатнім для підприємств із чисельністю понад 10 000 співробітників. Вплив на мережевий трафік через мікросегментацію та шифрування виявився незначним – зростання обсягу трафіку на 3-5% порівняно з незахищеним внутрішнім трафіком, що пояснюється використанням сучасних ефективних протоколів шифрування. Важливим результатом стало те, що затримки, які додаються системою, не перевищують допустимих значень для більшості корпоративних застосунків, включаючи VoIP та системи реального часу [43].

Третя група тестів була присвячена оцінці ефективності мікросегментації та динамічного управління привілейованим доступом. У тестовому середовищі було створено 50 ізольованих сегментів для різних застосунків. Моделювалося латеральне переміщення зловмисника, який отримав контроль над однією робочою станцією. У традиційній архітектурі зловмисник зміг просканувати внутрішню мережу та отримати доступ до 35% ресурсів, включаючи критичні бази даних, протягом 15 хвилин. У Zero Trust-архітектурі з мікросегментацією можливості сканування були обмежені лише тими ресурсами, до яких робоча

станція мала легітимний доступ (3 сервери, 2 бази даних). Спроби зловмисника звернутися до інших ресурсів блокувалися на рівні мережевих контролерів, при цьому кожна така спроба фіксувалася як аномалія. Динамічне управління привілейованим доступом (JIT) показало здатність повністю усунути ризики, пов'язані з постійним існуванням адміністративних облікових записів. У жодному з 20 змодельованих сценаріїв атак на привілейований доступ зловмисник не зміг отримати підвищені права, оскільки тимчасові облікові записи створювалися лише на час затвердженої операції та автоматично видалялися. Середній час надання тимчасових прав через портал запитів (включаючи етап затвердження) становив 2,5 хвилини для попередньо затверджених операцій та 8 хвилин для операцій, що вимагають ручного схвалення.

Для оцінки масштабованості моделі було проведено тестування з поступовим збільшенням кількості одночасно активних PEP та обсягу політик. Система продемонструвала лінійне масштабування при додаванні вузлів PDP – збільшення кількості вузлів удвічі дозволило збільшити пропускну здатність на 92%, що свідчить про ефективну горизонтальну масштабованість. Репозиторій політик на основі розподіленої бази даних витримав зберігання та версіонування до 50 000 політик без деградації продуктивності при читанні (час доступу до політики <2 мс). При досягненні 100 000 політик спостерігалося незначне зростання часу доступу до 5 мс, що все ще є прийнятним для більшості сценаріїв.

Важливим аспектом тестування стала оцінка стійкості системи до відмов. Було змодельовано відмову одного з вузлів PDP, втрату зв'язку з центральним репозиторієм політик та повне відключення основного дата-центру. У всіх сценаріях система продовжувала функціонувати: при відмові одного PDP навантаження автоматично перерозподілялося між іншими вузлами; при втраті зв'язку з центральним репозиторієм локальні PDP продовжували роботу з використанням кешованих політик (актуальність політик підтримувалася до 24 годин); при відключенні основного дата-центру трафік автоматично перенаправлявся на резервний центр, де було розгорнуто повний набір

компонентів. Час перемикання на резервний центр не перевищував 30 секунд, що відповідає вимогам до високої доступності корпоративних систем.

Оцінка операційної ефективності проводилася шляхом порівняння витрат на управління доступом до та після впровадження моделі. До впровадження в тестовому середовищі використовувалася традиційна модель RBAC з періодичними ручними ресертифікаціями прав доступу раз на квартал. Витрати часу адміністраторів на управління правами становили в середньому 40 годин на місяць. Після впровадження Zero Trust-моделі з централізованими політиками, автоматизованим наданням доступу на основі атрибутів та самообслуговуванням запитів на доступ, адміністративні витрати скоротилися до 12 годин на місяць. Крім того, система дозволила автоматизувати процес ресертифікації: політики доступу підлягають автоматичному перегляду при зміні атрибутів суб'єкта (посада, підрозділ) або об'єкта (рівень критичності), а для ручного підтвердження залишаються лише виняткові випадки. Це дозволило скоротити час проведення ресертифікації з 5 робочих днів до 4 годин.

Для якісної оцінки зручності роботи кінцевих користувачів було проведено опитування 50 співробітників різних ролей (від кінцевих користувачів до адміністраторів), які брали участь у пілотному впровадженні. 82% респондентів відзначили, що процес автентифікації з використанням MFA та біометричних факторів став зручнішим, ніж регулярна зміна складних паролів. 78% адміністраторів підтвердили, що централізоване управління політиками та автоматизоване надання тимчасових привілеїв спростили виконання їхніх обов'язків. Водночас 15% респондентів висловили зауваження щодо збільшення кількості кроків при доступі до високочутливих ресурсів (вимога додаткового підтвердження), що є очікуваним компромісом між безпекою та зручністю.

Аналіз отриманих результатів дозволяє зробити такі основні висновки щодо ефективності запропонованої моделі. По-перше, модель забезпечує суттєве підвищення рівня безпеки порівняно з традиційними підходами, особливо в частині протидії внутрішнім загрозам, компрометації облікових даних та латеральному переміщенню зловмисників. По-друге, досягнуті показники

продуктивності (затримка PDP < 50 мс для 95% запитів, пропускна здатність > 10 000 запитів/с на кластер) підтверджують придатність моделі для використання в корпоративних середовищах будь-якого масштабу. По-третє, вбудовані механізми високої доступності та автоматичного відновлення забезпечують стійкість системи до відмов на рівні, що відповідає вимогам до критичних інфраструктурних компонентів. По-четверте, позитивні результати оцінки операційних витрат свідчать про економічну доцільність впровадження, оскільки скорочення адміністративних витрат та часу реагування на інциденти компенсує витрати на розгортання та обслуговування нової архітектури [44].

Водночас тестування виявило окремі обмеження та напрямки для подальшого вдосконалення. По-перше, модель демонструє чутливість до точності поведінкових профілів на початковому етапі експлуатації, коли система ще не накопичила достатньо даних для адекватної оцінки аномалій. Для пом’якшення цього ефекту рекомендується на перших 2-3 тижнях використовувати режим моніторингу з навчанням моделей машинного навчання. По-друге, інтеграція з Legacy-системами через шлюзи безпеки, хоча й вирішує проблему сумісності, може створювати додаткові затримки (до 150 мс) для запитів, що проходять через такі шлюзи. Для критичних за продуктивністю Legacy-систем доцільно розглядати їх поступову модернізацію або заміну. По-третє, вартість розгортання повного комплексу компонентів (PDP, API-шлюзи, SDN-контролери, системи управління кінцевими точками) може бути суттєвою для малих та середніх підприємств, тому для таких організацій рекомендується розглядати хмарні або гібридні реалізації з використанням моделі «безпека як послуга».

Рис. 3.2 Ключові показники продуктивності та операційної ефективності

Результати тестування підтвердили досягнення цілей, поставлених на початку дослідження: розроблена модель управління доступом на основі принципів Zero Trust забезпечує ефективний захист від сучасних загроз, демонструє прийнятні показники продуктивності та масштабованості, а також створює основу для автоматизації процесів управління доступом та зниження операційних витрат. Отримані кількісні та якісні результати можуть бути використані як обґрунтування для впровадження подібних рішень у реальних корпоративних інформаційних системах. Подальші дослідження можуть бути спрямовані на вдосконалення алгоритмів поведінкового аналізу з використанням глибокого навчання, оптимізацію продуктивності PDP для ультранизьких затримок (менше 10 мс), а також на розробку спеціалізованих рішень для галузевих сегментів з особливими вимогами безпеки, таких як фінансовий сектор, охорона здоров’я та критична інфраструктура.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне науково-прикладне завдання – підвищення рівня захищеності інформаційних систем шляхом розробки та впровадження моделі управління доступом на основі концепції Zero Trust. У процесі дослідження отримано такі основні результати.

У першому розділі виконано систематизацію теоретичних засад управління доступом. Проаналізовано еволюцію моделей доступу – дискреційної, мандатної, рольової та атрибутивної, виявлено їх фундаментальні обмеження в умовах сучасних розподілених інформаційних систем. На основі аналізу стандартів NIST SP 800-207 та архітектурних підходів Forrester сформульовано ключові принципи Zero Trust: безперервна верифікація, мікросегментація, принцип найменших привілеїв та відмова від імпліцитної довіри до внутрішнього периметра.

У другому розділі проведено комплексний аналіз існуючих рішень та здійснено моделювання системи управління доступом. Досліджено сучасні механізми автентифікації (OAuth 2.0, OpenID Connect, SAML) та авторизації, виявлено їхню недостатню адаптивність до динамічних змін контексту. Систематизовано вразливості традиційних моделей безпеки, зокрема явища «розповзання привілеїв», «рольового розростання», недостатній контроль привілейованого доступу та низьку видимість подій. На основі проведеного аналізу запропоновано власну модель управління доступом, що базується на динамічному прийнятті рішень з урахуванням контекстуальних даних (ідентичність, стан пристрою, геолокація, поведінкові патерни).

У третьому розділі реалізовано практичне впровадження розробленої моделі. Спроєктовано трирівневу архітектуру, що включає площину управління політиками, площину прийняття рішень (кластер PDP) та розподілену площину виконання (PEP). Розроблено дорожню карту впровадження та систему метрик оцінки ефективності. Результати тестування підтвердили переваги запропонованого підходу: рівень запобігання несанкціонованому доступу зріс з

54% до 96%, час реагування на інциденти скоротився на 96%, адміністративні витрати на управління доступом зменшилися на 70%. Модель продемонструвала лінійну масштабованість та відповідність вимогам високої доступності.

Наукова новизна роботи полягає в систематизації вразливостей класичних моделей управління доступом у контексті сучасних розподілених середовищ, розробці архітектури Zero Trust-системи з ієрархічною структурою PDP та динамічною оцінкою ризику на основі поведінкових факторів, а також у кількісному обґрунтуванні показників ефективності.

Практичне значення отриманих результатів полягає в можливості їх безпосереднього використання для підвищення рівня безпеки корпоративних інформаційних систем, зниження операційних витрат на управління доступом та забезпечення відповідності сучасним вимогам кібербезпеки. Отримані результати можуть бути використані як наукове підґрунтя для подальших досліджень у галузі адаптивного управління доступом та впровадження концепції Zero Trust у різних галузевих сегментах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ahmadi S. Zero trust architecture in cloud networks: application, challenges and future opportunities. *Journal of engineering research and reports*. 2024. Vol. 26, no. 2. P. 215–228. URL: https://doi.org/10.9734/jerr/2024/v26i21083

2. Aigumov T. G., Abdulmukminova E. M., Isaev M. I. Implementing zero trust principles as a transformational it risk and access management project. *Ekonomika i upravlenie: problemy, resheniya*. 2025. Vol. 7/9, no. 160. P. 21–27. URL: https://doi.org/10.36871/ek.up.p.r.2025.07.09.003

3. A survey on zero trust security – applications and challenges / V. Varma Sangaraju et al. *Proceedings on engineering sciences*. 2025. Vol. 7, no. 1. P. 437–446. URL: https://doi.org/10.24874/pes07.01d.001

4. A survey on zero trust security – applications and challenges / V. Varma Sangaraju et al. *Proceedings on engineering sciences*. 2025. Vol. 7, no. 1. P. 437–446. URL: https://doi.org/10.24874/pes07.01d.001

5. Duben A. K. Theoretical and methodological foundations of information security. *Национальная безопасность / nota bene*. 2023. No. 2. P. 48–54. URL: https://doi.org/10.7256/2454-0668.2023.2.40068

6. Harold R. Leveraging machine learning techniques for zero trust privacy protection. *International journal of recent innovations in academic research*. 2025. Vol. 9, no. 1. P. 114–120. URL: https://doi.org/10.5281/zenodo.15041450

7. Harold R. Leveraging machine learning techniques for zero trust privacy protection. *International journal of recent innovations in academic research*. 2025. Vol. 9, no. 1. P. 114–120. URL: https://doi.org/10.5281/zenodo.15041450

8. Karanam R. Zero trust architecture in devsecops: enhancing security in cloud-native environments. *International journal for research in applied science and engineering technology*. 2024. Vol. 12, no. 8. P. 1071–1077. URL: https://doi.org/10.22214/ijraset.2024.64045

9. Mankovskyi B., Dovbniak V., Opirskyy I. Research on the feasibility of implementing the zero trust concept in iot systems. *Cybersecurity: education, science, technique*. 2025. Vol. 1, no. 29. P. 73–91. URL: https://doi.org/10.28925/2663-4023.2025.29.864

10. Manne T. A. K. Implementing zero trust architecture in multi-cloud environments. *International journal of computing and engineering*. 2025. Vol. 7, no. 3. P. 74–82. URL: https://doi.org/10.47941/ijce.2753

11. Narapareddy V. S. R. Zero trust security architecture in cloud systems. 2025. URL: https://doi.org/10.5281/zenodo.15556786

12. Salahuddin Syed. Zero trust principles and the evolution of privilege access management architectures. *Journal of computer science and technology studies*. 2025. Vol. 7, no. 7. P. 859–865. URL: https://doi.org/10.32996/jcsts.2025.7.7.94

13. Samir N. Ajani. Cloud security: implementing zero trust architecture in distributed environments. *Computer fraud and security*. 2024. P. 176–184. URL: https://doi.org/10.52710/cfs.75

14. Sandip Poddar. Zero trust network architectures in multi-cloud environments. *Journal of information systems engineering and management*. 2025. Vol. 10, no. 58s. P. 1085–1092. URL: https://doi.org/10.52783/jisem.v10i58s.12771

15. Santosh P. Implementing zero trust architecture across multi-cloud environments: a security framework. *International journal of leading research publication*. 2023. Vol. 4, no. 9. P. 1–4. URL: https://doi.org/10.5281/zenodo.14646896

16. Srikanth K. Zero trust architecture for cloud security. *Journal of scientific and engineering research*. 2018. Vol. 5, no. 4. P. 466–468. URL: https://doi.org/10.5281/zenodo.14050082

17. Theory and application of zero trust security: a brief survey / H. Kang et al. *Entropy*. 2023. Vol. 25, no. 12. P. 1595. URL: https://doi.org/10.3390/e25121595

18. Yesin V. I., Vilihura V. V., Uzlov D. Y. Zero trust architecture: challenges and recommendations for successful implementation. *Radiotekhnika*. 2024. No. 218. P. 7–34. URL: https://doi.org/10.30837/rt.2024.3.218.01

19. Yilmaz E. Machine identity management in modern enterprise security: concepts, challenges, and the role of privileged access management systems. *Engineering, technology & applied science research*. 2026. Vol. 16, no. 1. P. 32369–32376. URL: https://doi.org/10.48084/etasr.16202

20. Zhi-Yu Peng, Shan-Ping Li. Privacy protection in trust management. *2008 international conference on machine learning and cybernetics (ICMLC)*, Kunming, China, 12–15 July 2008. 2008. URL: https://doi.org/10.1109/icmlc.2008.4620616

21. Arora A. Zero trust architecture: revolutionizing cybersecurity for modern digital environments. *SSRN electronic journal*. 2025. URL: https://doi.org/10.2139/ssrn.5268151

22. Avireneni R. T., Koner S. H. Zero trust security architecture (ZTSA). *Journal of artificial intelligence & cloud computing*. 2024. P. 1–8. URL: https://doi.org/10.47363/jaicc/2024(3)505

23. Brazhuk A. I., Olizarovich E. V. Towards the computer systems design based on Zero Trust Architecture. *Informatics*. 2024. Vol. 21, no. 4. P. 85–98. URL: https://doi.org/10.37661/1816-0301-2024-21-4-85-98

24. Godwin Nzeako, Rahman Akorede Shittu. Implementing zero trust security models in cloud computing environments. *World journal of advanced research and reviews*. 2024. Vol. 24, no. 3. P. 1647–1660. URL: https://doi.org/10.30574/wjarr.2024.24.3.3500

25. Manzano C., Márquez G., Astudillo H. Quality attributes for zero trust architecture-based systems. *2024 43rd international conference of the chilean computer science society (SCCC)*, Temuco, Chile, 28–30 October 2024. 2024. P. 1–11. URL: https://doi.org/10.1109/sccc63879.2024.10767657

26. Model of implementation of management of access to information assets in the concept of zero trust / V. Khoroshko et al. *Information systems and technologies security*. 2024. No. 1 (7). P. 39–44. URL: https://doi.org/10.17721/ists.2024.7.39-44

27. Pabbath Reddy A. R. Zero trust architecture: an ai-driven framework for modern cybersecurity challenges. *FMDB transactions on sustainable intelligent networks*. 2025. Vol. 2, no. 1. P. 10–21. URL: https://doi.org/10.69888/ftsin.2025.000366

28. Sivakolundhu R. Zero trust architecture in multicloud environments: a comprehensive analysis of challenges, strategies, and future directions. *Journal of artificial intelligence, machine learning and data science*. 2022. Vol. 1, no. 1. P. 732–736. URL: https://doi.org/10.51219/jaimld/rekha-sivakolundhu/183

29. Tabbassum A., Abdul Kareem S. Implementing zero trust security models in cloud infrastructures. *International journal of science and research (IJSR)*. 2021. Vol. 10, no. 11. P. 1582–1586. URL: https://doi.org/10.21275/sr211110212612

30. Vinod V. Integrating zero trust principles into IAM for enhanced cloud security. *Recent trends in cloud computing and web engineering*. 2024. Vol. 7, no. 1. P. 78–92. URL: https://doi.org/10.5281/zenodo.14162091

31. Yilmaz E. Machine identity management in modern enterprise security: concepts, challenges, and the role of privileged access management systems. *Engineering, technology & applied science research*. 2026. Vol. 16, no. 1. P. 32369–32376. URL: https://doi.org/10.48084/etasr.16202

32. Yu W., Zhang L. Research on zero trust access control model and formalization based on rail transit data platform. *2022 IEEE 10th international conference on information, communication and networks (ICICN)*, Zhangye, China, 23–24 August 2022. 2022. URL: https://doi.org/10.1109/icicn56848.2022.10006520

33. Danilescu M., Besliu V. Trust- based modeling mac-type access control through access and actions control policies. *Journal of engineering science*. 2021. Vol. XXVIII, no. 2. P. 67–78. URL: https://doi.org/10.52326/jes.utm.2021.28(2).05

34. De Capitani di Vimercati S., Paraboschi S., Samarati P. Access control: principles and solutions. *Software: practice and experience*. 2003. Vol. 33, no. 5. P. 397–421. URL: https://doi.org/10.1002/spe.513

35. Efficient selection of access control systems through multi criteria analytical hierarchy process / A. Azhar et al. *2012 international conference on emerging technologies (ICET)*, Islamabad, Pakistan, 8–9 October 2012. 2012. URL: https://doi.org/10.1109/icet.2012.6375419

36. Hu V. C., Ferraiolo D. F., Kuhn D. R. Assessment of access control systems. Gaithersburg, MD : National Institute of Standards and Technology, 2006. URL: https://doi.org/10.6028/nist.ir.7316

37. Kumari K. S., T.Chithraleka. A comparative analysis of access control policy modeling approaches. *International journal of secure software engineering*. 2012. Vol. 3, no. 4. P. 65–83. URL: https://doi.org/10.4018/jsse.2012100104

38. Lapin S. Comparative analysis of existing access control models in systems with interchangeable objects. *Izvestiya of altai state university*. 2016. URL: https://doi.org/10.14258/izvasu(2016)1-25

39. Normatov S., Rakhmatullaev M. Extended model of access control for the library information systems. *2017 international conference on information science and communications technologies (ICISCT)*, Tashkent, 2–4 November 2017. 2017. URL: https://doi.org/10.1109/icisct.2017.8188584

40. Parker T. A. Network access control developments. *Computer audit update*. 1990. Vol. 1990, no. 6. P. 3–10. URL: https://doi.org/10.1016/s0960-2593(05)80056-4

41. Shantha Kumari K., Chithralekha T. Feature modeling of the evolving access control requirements. *Communications in computer and information science*. Berlin, Heidelberg, 2011. P. 392–403. URL: https://doi.org/10.1007/978-3-642-24043-0_40

42. Shylik A., Puzyrov S. Access control system based on rfid and spring boot. *Scientific and practical journal "materials of scientific conferences of the petro*

mohyla black sea national university". 2025. No. 1. P. 181–185. URL: https://doi.org/10.34132/mspc2025.01.06.39

43. Towards effective verification of multi-model access control properties / B. J. Berger et al. *SACMAT '19: the 24th ACM symposium on access control models and technologies*, Toronto ON Canada. New York, NY, USA, 2019. URL: https://doi.org/10.1145/3322431.3325105

44. Truong A. T. Efficient analysis of sequences of security problems in access control systems. *Mobile computing and sustainable informatics*. Singapore, 2023. P. 67–80. URL: https://doi.org/10.1007/978-981-99-0835-6_5