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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Данило ЮЖАКОВ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
ЮЖАКОВ Данило
(прізвище, ім'я)

Керівник д-р техн. наук, професор САВЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент к.т.н, доц. Щавинський Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

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

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
"___" жовтня 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

ЮЖАКОВУ Данилу Сергійовичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів»

керівник кваліфікаційної роботи САВЧЕНКО Віталій д-р техн. наук, професор
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « 30 » жовтня 2025 року № 467 .

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 25.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
набір рішень ESET;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти, звіти міжнародних компаній.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Проаналізувати теоретичні засади управління ідентифікацією та доступом користувачів.

2. Дослідити нормативно-правове забезпечення та стандарти у сфері управління доступом

3. Виконати аналіз загроз та вразливостей, пов'язаних з обліковими записами та доступом у корпоративному середовищі.

4. Розробити цільову архітектуру та технологію управління доступом на базі AD та ESET PROTECT Elite

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів.	01.10.2025 р.	
2.	Аналіз наукової та технічної літератури, нормативних документів і міжнародних стандартів з питань теми кваліфікаційної роботи.	12.10.2025 р.	
3.	Аналіз існуючих методів і засобів управління ідентифікацією та доступом користувачів на базі AD, ESET PROTECT Elite, Excalibur	27.10.2024 р.	
4.	Розроблення технології управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів	03.11.2025 р.	
5.	Розроблення практичних рекомендацій щодо впровадження та експлуатації запропонованої технології в організації	15.11.2025 р.	
6.	Оформлення результатів дослідження	26.11.2025 р.	
7.	Подання роботи на плагіат. Підготовка доповіді до захисту.	25.12.2025 р.	

Здобувач вищої освіти _____ Данило ЮЖАКОВ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Южакова Данила
на тему: «Технологія управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів»

Актуальність: Сучасні організації працюють у складних гібридних IT-середовищах, де одночасно використовуються локальні сервери, хмарні сервіси, віддалений доступ, велика кількість прикладних систем та облікових записів. Це впливає на ризики компрометації облікових записів, можуть з'являтись надмірні права доступу у користувачів, можлива відсутність належного контролю за життєвим циклом акаунтів. Це напряму підвищує ризики несанкціонованого доступу до корпоративних інформаційних ресурсів та призводить до значної частки успішних кібератак.

У таких умовах набуває значення впровадження цілісної технології управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі було встановлено зміст проблеми забезпечення безпечної роботи гібридних працівників організації та визначено мету та завдання даного виду забезпечення, а також його складові частини.
2. Досліджено можливості Active Directory, ESET PROTECT Elite та ESET Secure Authentication у контексті побудови цілісної технології управління доступом, зокрема реалізації рольової моделі, посиленого захисту облікових записів за допомогою MFA та контролю дій користувачів на кінцевих точках.
3. Розглянуто зміст цільової технології управління ідентифікацією та доступом користувачів, спроєктовано архітектуру на базі AD, ESA та ESET PROTECT

Недоліки:

1. У кваліфікаційній роботі бажано було б детальніше проаналізувати впровадження розробленої технології IAM на прикладі конкретної реальної організації з урахуванням її бізнес-процесів та обмежень.
2. Доцільно було б ширше розглянути інтеграцію запропонованої технології з хмарними сервісами та SaaS-додатками, а також провести кількісну оцінку ефективності (наприклад, за показниками зменшення надмірних привілеїв або невдалих спроб автентифікації).

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **"задовільно"**, а здобувач **ЮЖАКОВ Данило** – присвоєння кваліфікації магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім'я, прізвище)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач ЮЖАКОВ Данило до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів».
Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***ЮЖАКОВ Данило*** обрав тему роботи, метою якої було дослідити зміст технології забезпечення безпечної роботи гібридних працівників організації та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ЮЖАКОВ Данило*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ЮЖАКОВА Данила*** на оцінку **"задовільно"** та присвоїти йому кваліфікацію магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ЮЖАКОВ Данило** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)
_____ Галина Гайдур
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 75 сторінки, 29 джерел.

Об'єкт дослідження – процес управління ідентифікацією та доступом користувачів у гібридній корпоративній інформаційній системі на базі Active Directory.

Предмет дослідження – технологія побудови архітектури управління доступом на основі принципів найменших привілеїв, багатофакторної автентифікації та централізованого моніторингу.

Мета роботи – аналіз сучасних загроз для систем управління ідентичностями. Також вивчення міжнародних стандартів ISO/IEC 27001/27002 та рекомендацій NIST SP 800-207. Розроблення цільової архітектури управління доступом на основі Zero Trust [28]. Розроблення методики створення політик управління доступом та їх практичну реалізацію з використанням інтегрованого набору інструментів

Методи дослідження – аналіз наукових, технічних та нормативних джерел з управління інформаційною безпекою; вивчення стандартів ISO/IEC 27001:2022, ISO/IEC 27002:2022 та концепції Zero Trust (NIST SP 800-207); синтез звітів про кібератаки від провідних постачальників; аналіз типових ланцюгів атак на Windows-інфраструктури; моделювання цільової архітектури та формалізація вимог до контролів.

У роботі обґрунтовано застосовування концепції мінімуму привілеїв та явної перевірки доступу для організацій з гібридною моделлю роботи. Сформовано вимоги до безпеки, розроблена цільова архітектура на базі сегментації довіри, принципу найменших привілеїв та явного визначення дозволених взаємодій. Пропонується методика розроблення політик управління: контроль облікових записів та доступу, захист кінцевих точок, автентифікація та авторизація, мережевий моніторинг та реагування на інциденти. Наводиться приклад практичної реалізації з використанням Active Directory, ESET PROTECT Elite та інструментів для централізованого логування.

Галузь використання – кібербезпека та управління інформаційною безпекою в організаціях середнього масштабу, зокрема в середовищах із гібридною моделлю роботи та локальною доменною інфраструктурою.

Управління ідентичностями, IAM, Active Directory, MFA, RBAC, Zero Trust, політики безпеки, гібридна робота, Windows-інфраструктура, on-premises, ESET PROTECT, SIEM, моніторинг

ABSTRACT

Text part of the qualification work: 75 pages, 29 sources.
Object of research – the process of identity and access management in a hybrid corporate information system based on Active Directory.

Subject of research – technology for building access control architecture based on the Principle of Least Privilege, Multi-Factor Authentication, and centralized monitoring, adapted to Windows-oriented on-premises environment.

The aim of research – to analyze modern threats to identity management systems; to study international standards ISO/IEC 27001/27002 and NIST SP 800-207 recommendations; to develop a target access management architecture based on Zero Trust paradigm; to develop a methodology for creating access management policies and their practical implementation using an integrated set of tools.

Research methods – analysis of scientific, technical, and normative sources on information security management; study of standards ISO/IEC 27001:2022, ISO/IEC 27002:2022 and Zero Trust concept; synthesis of cyber threat reports from leading vendors (Verizon, Microsoft, IBM); systematic analysis of typical attack chains on Windows infrastructure; modeling of target architecture and formalization of control requirements.

The thesis substantiates the applicability of least privilege and explicit access verification principles for organizations with hybrid work model. Security requirements are formulated and a target architecture is designed based on trust segmentation, principle of least privilege, and explicit definition of allowed interactions. A methodology for policy development is proposed covering: account and access control, endpoint protection, authentication and authorization, network monitoring and incident response. An example of practical implementation is provided using Active Directory, ESET PROTECT Elite and centralized logging tools.

Field of application – cybersecurity and information security management in mid-sized organizations, particularly in environments with a hybrid work model and an on-premises domain infrastructure.

Identity and Access Management, IAM, Active Directory, MFA, RBAC, Zero Trust, security policies, hybrid work, Windows infrastructure, on-premises, ESET PROTECT, SIEM, monitoring

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

GPO — Group Policy Object

RBAC — Role-Based Access Control

VPN — Virtual Private Network

MFA — Multi-Factor Authentication

TOTP — Time-based One-Time Password

RADIUS — Remote Authentication Dial-In User Service

RDP — Remote Desktop Protocol

PAW — Privileged Access Workstation

EPP — Endpoint Protection Platform

EDR — Endpoint Detection and Response

XDR — Extended Detection and Response

AD — Active Directory

CVE — Common Vulnerabilities and Exposures

URL — Uniform Resource Locator

ВСТУП

Актуальність дослідження. Контроль доступу користувачів до інформаційних ресурсів, що забезпечується переважно за рахунок мережевого периметра та локальних облікових записів, уже не відповідає сучасним умовам функціонування корпоративних IT-систем. Масове впровадження хмарних сервісів, віддаленої роботи, мобільних пристроїв та SaaS-рішень призводить до розмивання периметра, збільшення кількості облікових записів і точок доступу, а також до ускладнення управління правами користувачів.

У результаті організації стикаються з проблемами надмірних привілеїв, відсутності єдиного уніфікованого підходу до управління ідентичністю, недостатнього контролю за життєвим циклом облікових записів, а також обмеженими можливостями аудиту дій користувачів та адміністраторів. Значна частина кіберінцидентів пов’язана саме з компрометацією облікових записів, зловживанням привілейованим доступом або помилками в налаштуванні прав доступу. Це визначає необхідність застосування цілісних технологій управління ідентифікацією та доступом, які поєднують організаційні політики, сучасні моделі доступу, такі як RBAC, ABAC, Zero Trust, та спеціалізовані програмні засоби.

Сучасні корпоративні середовища зазвичай використовують поєднання доменної інфраструктури, засобів захисту кінцевих точок і серверів, а також систем керування привілейованим доступом.

Вищезазначене зумовлює актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження та розроблення технології управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів на базі домену Active Directory та комплексу засобів захисту ESET PROTECT Elite.

Об’єкт дослідження – процес управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів.

Предмет дослідження – технологія управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів на базі Active Directory, комплексу засобів захисту ESET PROTECT Elite.

Мета роботи – розробити порядок застосування технології управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів та надати рекомендації щодо її реалізації в корпоративному середовищі.

Наукові завдання:

- Дослідити сутність проблеми управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів;
- Проаналізувати моделі та підходи до управління доступом у корпоративних системах;
- Проаналізувати існуючі рішення та технології управління ідентифікацією та доступом користувачів;
- Проаналізувати методи та засоби реалізації технології управління ідентифікацією та доступом користувачів у типовому корпоративному середовищі;
- Розкрити порядок реалізації технології управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів і сформулювати практичні рекомендації щодо її впровадження.

Додано примітку [DY1]: Поки не знаю, шо тут аналізувати

Методи дослідження – опрацювання наукової та технічної літератури за даною тематикою, аналіз експлуатаційної документації програмно-апаратних засобів, міжнародних стандартів та нормативних документів, їх порівняння; методи системного та структурно-функціонального аналізу для дослідження процесів управління доступом; елементи моделювання для побудови цільової технології IAM.

Практичне значення одержаних результатів: запропоновано порядок застосування технології управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації на базі Active Directory та комплексу засобів захисту ESET PROTECT Elite.

1 ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1. Поняття та місце систем управління ідентифікацією та доступом у забезпеченні кібербезпеки

Сучасні корпоративні інформаційні системи характеризуються значною кількістю користувачів, сервісів, застосунків та пристроїв, між якими постійно відбувається обмін даними. За таких умов ключовим завданням стає забезпечення контрольованого доступу до інформаційних ресурсів – від файлових сховищ і баз даних до хмарних сервісів і корпоративних застосунків. Від того, наскільки коректно організовано управління обліковими записами та правами доступу, безпосередньо залежить рівень кібербезпеки організації.

Базовими поняттями у цій сфері є ідентифікація, автентифікація та авторизація. Ідентифікація полягає у встановленні тотожності суб'єкта певному запису в системі. Автентифікація підтверджує, що суб'єкт справді є тим, за кого себе видає . Авторизація визначає, які саме дії суб'єкт має право виконувати щодо певних ресурсів: читання, запис, адміністрування, доступ до конфіденційних даних тощо. Часто до цієї трійки додають облік та аудит , коли всі критичні операції фіксуються в журналах подій для подальшого аналізу та розслідування інцидентів.

Комплексний підхід до цих процесів реалізується в рамках концепції Identity and Access Management. Під IAM розуміють сукупність політик, процесів, організаційних заходів та програмно-апаратних засобів, спрямованих на централізоване управління життєвим циклом облікових записів і контролем доступу до інформаційних ресурсів. Системи IAM забезпечують створення, модифікацію та видалення облікових записів, призначення ролей і прав, реалізацію багатофакторної автентифікації, а також ведення журналів подій, пов'язаних із доступом.

Місце IAM у системі кібербезпеки визначається тим, що більшість кіберінцидентів так чи інакше пов'язані з обліковими записами: компрометація облікових даних, використання слабких або повторно застосованих паролів,

надмірні привілеї, спільні акаунти, несвоєчасне блокування доступу звільнених співробітників. За відсутності централізованої технології управління ідентичністю організація втрачає можливість ефективно застосовувати принцип «найменших привілеїв», контролювати відповідність доступів службовим обов'язкам та забезпечувати повноцінний аудит дій користувачів і адміністраторів.

Окремим напрямом є управління привілейованим доступом (Privileged Access Management, PAM), що розглядається як складова або доповнення до IAM. Системи PAM забезпечують захист і контроль облікових записів з підвищеними правами , які у разі компрометації можуть бути використані для повного захоплення інфраструктури. PAM-рішення дозволяють централізовано зберігати паролі та ключі, видавати тимчасові права, записувати та контролювати сесії привілейованих користувачів.

Таким чином, системи IAM та PAM відіграють ключову роль у побудові сучасної системи кібербезпеки, забезпечуючи контроль над тим, хто, до яких ресурсів і на яких умовах має доступ, а також даючи змогу відстежувати й аналізувати дії користувачів. Для корпоративних середовищ, що активно використовують доменні служби, засоби захисту кінцевих точок і спеціалізовані рішення класу PAM, питання інтеграції цих компонентів у єдину технологію управління доступом набуває особливої важливості.

1.2. Моделі та принципи управління доступом до корпоративних ресурсів

Організація доступу до інформаційних ресурсів базується на певних моделях управління доступом, які визначають, хто і за якими правилами може отримати доступ до тієї чи іншої інформації. Вибір моделі суттєво впливає на складність адміністрування, гнучкість системи прав та її відповідність вимогам безпеки.

Однією з найстаріших моделей є дискреційна модель управління доступом. У ній власник ресурсу має право самостійно визначати, кому надається доступ і на яких правах. Такий підхід забезпечує гнучкість, однак створює ризики хаотичного розподілу прав, коли користувачі можуть делегувати доступ іншим без централізованого контролю. У великих організаціях це призводить до накопичення надмірних привілеїв та ускладнює аудит.

Мандатна модель передбачає жорстке централізоване управління правами на основі рівнів конфіденційності та допусків. Кожному об’єкту і суб’єкту призначається певний рівень, і правила доступу визначаються політикою безпеки. Такий підхід традиційно застосовується в системах з підвищеними вимогами до захисту державної або військової інформації, однак є менш гнучким для динамічних комерційних середовищ.

У більшості сучасних корпоративних систем використовується рольова модель управління доступом . У цій моделі права прив'язуються не до конкретних користувачів, а до ролей. Наприклад у якості ролей можуть виступати посади, функціональні обов’язки. Користувачеві призначаються одна або кілька ролей, які визначають його доступ до ресурсів. Це спрощує адміністрування, оскільки при зміні посади або переході співробітника між підрозділами достатньо змінити набір ролей замість ручного коригування доступів до кожного ресурсу.

Подальшим розвитком є атрибутивна модель управління доступом де рішення про доступ приймається на основі набору атрибутів: властивостей користувача , ресурсу , контексту та політики безпеки. ABAC забезпечує високу гнучкість та дає можливість реалізовувати складні правила доступу, наприклад: «дозволити доступ до фінансових звітів лише співробітникам фінансового відділу з корпоративного пристрою в робочий час».

У сучасних концепціях кібербезпеки важливу роль відіграє підхід Zero Trust, відповідно до якого жодному користувачеві або пристрою не можна повністю довіряти лише на підставі їхнього розташування в мережі. Доступ до ресурсів надається на основі постійної перевірки ідентичності, контексту запиту та відповідності встановленим політикам безпеки. Це означає, що моделі управління доступом мають бути інтегровані з механізмами багатофакторної автентифікації, перевірки стану пристрою, контролю сесій та постійного моніторингу ризиків.

Незалежно від обраної моделі, в управлінні доступом виділяється низка базових принципів:

- Принцип найменших привілеїв (Least Privilege) – кожен користувач повинен мати лише той мінімально необхідний набір прав, який потрібен для виконання його службових обов’язків.
- Принцип необхідності знання (Need-to-Know) – доступ до конфіденційної інформації надається лише в разі обґрунтованої службової потреби.
- Розподіл обов'язків (Separation of Duties) – критичні операції повинні вимагати участі двох і більше користувачів, щоб запобігти шахрайству та зловживанням.
- Централізоване управління та аудит – усі зміни прав доступу мають виконуватись контрольовано, з фіксацією в журналах подій.
- Керування життєвим циклом доступу – доступи мають надаватись, змінюватись та анульовуватись відповідно до життєвого циклу співробітника в організації (прийом, зміна посади, звільнення).

У реальних корпоративних системах, зокрема на базі домену Active Directory, засоби рольового доступу, груп безпеки та політик можна комбінувати з атрибутивним підходом і концепцією Zero Trust. Це створює передумови для побудови узгодженої технології IAM, яка враховує як формальні моделі, так і практичні обмеження інфраструктури.

1.3. Підходи до створення політик на основі моделі нульової довіри

Поширення гібридної моделі роботи та зростання використання хмарних сервісів зумовлюють ситуацію, за якої співробітники організацій дедалі частіше здійснюють доступ до корпоративних ресурсів із різних мереж, географічних локацій і з використанням різнорідних пристроїв. За таких умов традиційна модель захисту, що ґрунтується на мережевому периметрі та припущенні про довірений характер внутрішнього середовища, втрачає ефективність. Практика сучасних кібератак, орієнтованих на компрометацію облікових записів, механізмів віддаленого доступу, VPN-шлюзів і хмарних ідентичностей, демонструє, що сам факт розміщення ресурсу в межах внутрішньої мережі не може гарантувати належного рівня захисту. Сукупність цих чинників сприяла формуванню та

поширенню підходів до забезпечення інформаційної безпеки, об’єднаних у межах концепції Zero Trust.

Базова ідея Zero Trust [28] полягає в тому, що довіра не надається автоматично жодному користувачу, пристрою або сервісу лише на підставі їхнього розташування у мережі. Кожен запит на доступ розглядається як потенційно небезпечний і підлягає окремій перевірці. У цьому контексті принцип найменших привілеїв набуває практичного значення, користувач отримує тільки ті права, які є необхідними для виконання його службових функцій, і лише на той час, коли ці права необхідні. Для об’єктів інфраструктури це означає відмову від надмірно широких груп доступу та перехід до більш гнучких, у тому числі тимчасових, моделей надання прав.

Іншим важливим елементом є перевірка стану пристрою. Рішення про доступ приймається не тільки на основі того, хто звертається до ресурсу, але й з урахуванням того, з якого саме пристрою здійснюється цей запит і чи відповідає цей пристрій мінімальним вимогам безпеки. У загальному випадку йдеться про актуальність оновлень операційної системи, наявність та працездатність антивірусного рішення, налаштовані механізми блокування робочого столу, увімкнене шифрування дисків та інші заходи, які зменшують ймовірність успішної атаки на кінцеву точку. У низці сучасних рішень для віддаленого доступу, зокрема VPN клієнтів, така перевірка стану кінцевої точки реалізується як невід’ємна частина політик доступу, перед встановленням захищеного тунелю клієнт виконує тестування відповідності пристрою заданому профілю безпеки (posture check), а у разі невідповідності доступ або повністю блокується, або обмежується лише мінімально необхідним набором ресурсів. У гібридній моделі, де один і той самий співробітник може чергувати роботу з корпоративного ноутбука та особистого пристрою, значення цього принципу особливо велике.

Суттєве місце в архітектурі Zero Trust займає багатофакторна автентифікація. Вона розглядається як базовий компонент безпеки для більшості сервісів, корпоративної пошти, внутрішніх веб-ресурсів, VPN доступу, хмарних платформ і адміністративних інтерфейсів. З огляду на те, що більшість цільових атак

починається із фішингових листів та викрадення облікових даних, повсюдне впровадження MFA дозволяє суттєво ускладнити подальший розвиток атаки, навіть у випадку компрометації пароля.

Ще один принцип стосується контекстно-орієнтованого доступу. Доступ до одного і того самого ресурсу може бути дозволений або заборонений залежно від додаткових обставин. Такими обставинами можуть бути дані про географічне розташування користувача, час доби, тип мережі, історія попередніх підключень, обсяг чи характер запитуваних даних. Наприклад, спроба підключення до внутрішньої системи обліку з IP-адреси, яка географічно не відповідає звичній країні чи регіону перебування користувача, може вимагати додаткової перевірки або повністю блокуватися. Таким чином, контекст стає невід'ємним елементом процесу авторизації.

Реалізація Zero Trust неможлива без розвиненого моніторингу та телеметрії. Рішення про доступ, виявлення аномалій, реакція на інциденти спираються на дані про події автентифікації та авторизації, дії користувачів, поведінку пристроїв, мережеві з'єднання, DNS-запити тощо. Ці дані збираються, нормалізуються, корелюються і аналізуються, у тому числі за допомогою систем класу SIEM та поведінкового аналізу. Для гібридної моделі особливо важливо, щоб моніторинг охоплював як внутрішню інфраструктуру, так і хмарні сервіси, які активно використовуються працівниками.

У документі NIST SP 800-207 [1] запропоновано узагальнену референсну архітектуру Zero Trust. Її ядро складають компоненти, відповідальні за прийняття та застосування рішень щодо доступу. Політики й правила безпеки реалізуються у вигляді логіки Policy Engine, який, отримуючи від поінформованих джерел дані про користувача, пристрій, ресурс і контекст, визначає, чи має бути дозволено, обмежено чи заборонено певний запит. Policy Administrator забезпечує технічне втілення цих рішень, трансформуючи їх у конкретні дії для мережевих пристроїв, проксі-серверів, агентів на кінцевих точках та інших засобів контролю. Безпосереднє ж застосування рішень відбувається на рівні точок примусового виконання політики, це можуть бути VPN шлюзи, веб-проксі, мережеві екрани або

програмні агенти, що контролюють доступ до ресурсів на робочих станціях.

Робота такої архітектури може бути описана послідовністю дій. Коли користувач із певного пристрою звертається до корпоративного ресурсу, трафік перехоплюється засобом, який виконує роль точки примусового виконання. До компонента прийняття рішень передається інформація про ідентичність користувача, належність до груп, стан пристрою, тип і чутливість запитуваного сервісу, а також поточний контекст підключення. На підставі заздалегідь визначених політик Policy Engine формує рішення, яке або дозволяє повний доступ, або вводить ті чи інші обмеження, або повністю блокує запит. Це рішення через Policy Administrator доводиться до відповідних технічних засобів. Важливо, що оцінка не обмежується моментом початкової автентифікації: у разі зміни контексту, наприклад, появи аномальної активності, підозрілих мережевих з’єднань чи зміни геолокації, рішення щодо доступу може бути переглянуто вже в ході активної сесії.

У межах корпоративної інформаційної інфраструктури впровадження принципів Zero Trust, як правило, здійснюється поетапно та з урахуванням наявного рівня зрілості системи безпеки. На початковому етапі основна увага зосереджується на переосмисленні ролі ідентичності, яка починає виконувати функцію ключового контрольного елемента доступу, фактично замінюючи традиційний мережевий периметр. Це передбачає централізацію управління обліковими записами, уніфікацію вимог до автентифікації та забезпечення широкого застосування багатофакторної автентифікації для користувачів і привілейованих ролей. На наступному етапі реалізується мікросегментація середовища, у межах якої внутрішня мережа поділяється на логічно ізольовані зони, а взаємодія між ними регламентується правилами, побудованими за принципом найменших привілеїв. Такий підхід істотно обмежує можливості горизонтального переміщення зловмисника в разі компрометації окремих компонентів інфраструктури та підвищує загальну стійкість системи до складних багатовекторних атак.

Наступним кроком стає поглиблення контекстно-орієнтованого доступу.

Якщо на початковому етапі рішення про доступ приймалися здебільшого на основі ролі користувача, то поступово до уваги береться все ширший набір атрибутів, таких як географія, тип і стан пристрою, тип мережі, звичайні патерни поведінки. Паралельно розвиваються засоби моніторингу й аналітики, що дозволяють не лише фіксувати факти доступу, а й виявляти аномалії та автоматично реагувати на них, наприклад, шляхом примусової повторної автентифікації або блокування деяких дій.

Узагальнюючи, можна зробити висновок, що сучасні рішення із забезпечення безпечної роботи гібридних працівників втілюють принципи Zero Trust [28] незалежно від конкретних технологічних платформ. Вони поєднують жорстке управління ідентичностями, оцінку стану пристроїв, багатофакторну автентифікацію, контекстно-орієнтований доступ та розвинений моніторинг. Для подальших розділів ці принципи виступають методологічною основою, на якій будуватиметься опис конкретних технологій та технологічних рішень щодо захисту гібридної роботи.

1.3. Нормативно-правова та стандартна база у сфері управління ідентифікацією та доступом

Управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів не може розглядатися виключно як технічна задача. Воно жорстко прив’язане до вимог нормативно-правових актів, міжнародних та національних стандартів, галузевих регламентів і внутрішніх політик організації. Саме ці документи визначають допустимий рівень ризику, вимоги до аутентифікації та авторизації, правила обробки персональних даних, вимоги до журналювання дій та зберігання цих журналів, а також відповідальність за порушення встановлених правил доступу.

Умовно нормативно-правову та стандартну базу, що стосується IAM та PAM, можна поділити на три рівні:

- міжнародні стандарти та рекомендації;
- наднаціональні та галузеві регламенти ;
- національне законодавство та стандарти

- внутрішні нормативні документи організації.

Міжнародні стандарти інформаційної безпеки

Фундаментом для побудови систем управління інформаційною безпекою, у тому числі процесів IAM, є стандарти родини ISO/IEC 27000.

- ISO/IEC 27001 [8] визначає загальні вимоги до системи управління інформаційною безпекою (СУІБ). У контексті IAM важливими є вимоги щодо управління доступом, розподілу ролей і відповідальності, управління активами, кадрової безпеки, а також контролю змін. Процеси управління обліковими записами та правами доступу розглядаються як частина життєвого циклу активів та управління ризиками.
- ISO/IEC 27002 [9] містить деталізований набір заходів , у тому числі розділ, присвячений управлінню доступом: політика управління доступом, управління правами користувачів, управління привілейованими доступами, контроль доступу до систем та застосунків, управління паролями, використання багатофакторної автентифікації, журналювання тощо. Ці рекомендації фактично задають перелік вимог до технології управління ідентифікацією та доступом.
- ISO/IEC 27005 регламентує управління ризиками інформаційної безпеки. Для IAM це означає, що вибір конкретних механізмів аутентифікації, політик паролів, рівнів доступу тощо має базуватися на оцінці ризиків: загроз компрометації облікових даних, зловживання привілеями, внутрішніх порушень, помилок персоналу.
- ISO/IEC 27035 описує процес управління інцидентами інформаційної безпеки. IAM у цьому контексті виступає як один із ключових джерел даних для виявлення та розслідування інцидентів (журнали автентифікації, підвищення привілеїв, створення/видалення акаунтів, зміна прав).

Окреме значення для управління ідентифікацією має стандарт ISO/IEC 29115, присвячений рівням гарантії електронної автентифікації. Він вводить поняття рівнів довіри до механізмів автентифікації (наприклад, від простих паролів до багатофакторних схем із криптографічними токенами) та може використовуватись

як методична основа при виборі того чи іншого методу автентифікації для різних категорій користувачів і операцій.

Суттєвим джерелом вимог і рекомендацій є документи Національного інституту стандартів і технологій США . Зокрема:

- серія NIST SP 800-63 описує цифрову ідентичність, рівні гарантії автентифікації, керування цифровими ідентичностями та механізми автентифікації;
- NIST SP 800-53 містить каталог контролів безпеки для федеральних інформаційних систем, включаючи вимоги до ідентифікації, автентифікації, управління доступом, журналювання дій та аудиту;
- інші публікації NIST дають рекомендації щодо управління привілейованим доступом, принципу найменших привілеїв, побудови Zero Trust-архітектур.

Ці стандарти не є обов'язковими до виконання в усіх країнах, однак широко використовуються як кращі практики при побудові корпоративних систем IAM.

Наднаціональні та галузеві регламенти

Для європейського простору, а також організацій, які працюють із громадянами ЄС, важливе значення має Регламент (ЄС) 2016/679 (GDPR) про захист персональних даних. Хоча GDPR не є стандартом IAM, він містить низку вимог, безпосередньо пов'язаних із управлінням доступом:

- мінімізація персональних даних і обмеження доступу до них лише тим працівникам, яким це дійсно необхідно;
- забезпечення цілісності та конфіденційності обробки, включаючи технічні та організаційні заходи контролю доступу;
- журналювання операцій обробки та можливість довести законність доступу.

У низці галузей, таких як фінансовий сектор, енергетика, охорона здоров'я, можуть діяти окремі регуляторні документи й настанови, які посилюють вимоги до аутентифікації, сегментації доступу, журналювання та управління привілейованими акаунтами. Усе це прямо впливає на вибір архітектури IAM та політик доступу.

Національна нормативна база та внутрішні документи організації

У національних правових системах, у тому числі в Україні, питання ідентифікації, захисту інформації та доступу до інформаційних ресурсів регламентуються:

- законами про інформацію, захист інформації в інформаційно-телекомунікаційних системах, кібербезпеку;
- підзаконними актами та нормативними документами, що встановлюють порядок створення комплексних систем захисту інформації, вимоги до доступу, автентифікації, управління обліковими записами;
- державними стандартами , які регламентують термінологію, загальні принципи захисту інформації, вимоги до підсистем управління доступом, використання криптографічних засобів тощо.

Для конкретної організації ці вимоги транслюються у внутрішні нормативні документи:

- політику інформаційної безпеки;
- політику управління доступом;
- регламент управління обліковими записами та правами;
- положення про використання привілейованих облікових записів;
- інструкції щодо використання засобів автентифікації (паролі, токени, сертифікати, MFA);
- процедури аудиту, перегляду прав доступу, розслідування інцидентів.

Таким чином, нормативно-правова та стандартна база задає «рамки», у межах яких має бути розроблена технологія управління ідентифікацією та доступом. При проєктуванні конкретної реалізації управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів необхідно забезпечити відповідність ключовим вимогам: наявність формалізованих політик, застосування принципу найменших привілеїв, життєвий цикл облікових записів, аудит і контроль доступу, захист від несанкціонованих змін і компрометації облікових даних.

1.4. Сучасні технології та рішення IAM

Реалізація концепцій IAM у корпоративному середовищі базується на поєднанні низки технологій і програмних засобів, кожен з яких виконує свою роль

у загальній архітектурі управління ідентичністю та доступом. У цілому можна виділити такі основні класи рішень:

1. Служби каталогів та репозиторії ідентичностей
2. Системи управління життєвим циклом облікових записів (Identity Lifecycle Management)
3. Системи керування доступом та єдиного входу (Access Management, SSO)
4. Засоби багатофакторної автентифікації
5. Системи управління привілейованим доступом
6. Допоміжні засоби контролю та моніторингу

Служби каталогів та репозиторії ідентичностей

Більшість корпоративних систем базуються на службах каталогів, які зберігають відомості про користувачів, групи, комп'ютери, служби та інші об'єкти. Типовими прикладами є каталоги на основі протоколу LDAP та реалізації на кшталт Active Directory.

Служба каталогів забезпечує:

- централізоване зберігання облікових записів і груп;
- механізми автентифікації користувачів (наприклад, Kerberos у AD);
- прив'язку користувачів до організаційних одиниць (OU);
- реалізацію групових політик (GPO), у тому числі політик доступу;
- інтеграцію з іншими системами через LDAP або федераційні протоколи.

У контексті технології IAM саме служба каталогів є «ядром» інфраструктури ідентичностей: усі інші системи повинні або використовувати її як джерело істини (source of truth), або бути з нею синхронізовані.

Системи управління життєвим циклом облікових записів

Identity Lifecycle Management (ILM) відповідає за автоматизацію процесів створення, зміни та видалення облікових записів відповідно до кадрових подій: прийом на роботу, зміна посади, переведення, відпустка, звільнення.

Такі системи:

- інтегруються з HR-системами;
- дозволяють описувати робочі процеси (workflow) погодження доступу;

- автоматично створюють облікові записи в каталозі та прикладних системах;
- забезпечують своєчасне відключення доступів при звільненні;
- періодично проводять перегляд (recertification) доступів, дозволяючи керівникам підтверджувати або відкликати права своїх підлеглих.

У невеликих та середніх організаціях частина цих задач часто виконується вручну засобами самої служби каталогу, однак із зростанням масштабу без ILM-систем зберегти керованість прав доступу практично неможливо.

Системи керування доступом та єдиного входу (SSO)

Системи Access Management забезпечують реалізацію механізмів єдиного входу (Single Sign-On, SSO), федерації ідентичності та централізованого керування сесіями доступу до веб-застосунків і сервісів. Вони:

- виступають як постачальник ідентичності (IdP), який автентифікує користувача один раз і видає токени доступу;
- підтримують сучасні протоколи авторизації та федерації: SAML, OAuth 2.0, OpenID Connect;
- надають можливість централізовано застосовувати політики доступу до різних веб- та хмарних сервісів;
- реалізують додаткові механізми безпеки: step-up authentication (підвищення рівня автентифікації для критичних операцій), контроль геолокації, обмеження за типом пристрою тощо.

У ролі таких систем можуть виступати як комерційні продукти (хмарні та on-premises, які дозволяють організації будувати власну SSO-інфраструктуру.

Засоби сильної автентифікації та MFA

З огляду на вразливість паролів до підбору, фішингу та інших атак, стандартною вимогою сучасних систем IAM є використання багатофакторної автентифікації (MFA). MFA поєднує щонайменше два фактори з різних категорій:

- «знання» (пароль, PIN);
- «володіння» (токен, смарт-карта, мобільний пристрій);
- «біометрія» (відбиток пальця, розпізнавання обличчя тощо).

Технологічно MFA може реалізовуватися через:

- одноразові паролі (OTP) у мобільних додатках або апаратних токенах;
- push-повідомлення в мобільний застосунок;
- смарт-карти та криптографічні токени;
- біометричні системи.

Такі засоби інтегруються як із службами каталогів, так і з SSO-платформами, VPN-шлюзами, системами віддаленого доступу, критичними адміністраторськими консолями.

Системи управління привілейованим доступом (PAM)

Окремий клас рішень – PAM-системи, які зосереджені на захисті та контролі привілейованих облікових записів. Вони реалізують:

- сховище секретів (vault), у якому зберігаються паролі, ключі, облікові дані адміністраторів та сервісних акаунтів;
- проксі-доступ до критичних систем (адміністратор підключається не напряму, а через PAM-платформу);
- запис сесій (відео- чи текстовий лог усіх дій привілейованого користувача);
- динамічні паролі (password rotation), коли система автоматично змінює паролі після кожного використання;
- Just-in-Time (JIT) доступ, коли привілеї надаються тимчасово, на час вирішення задачі, після чого автоматично відкликаються.

PAM-системи інтегруються з каталогом (для ідентифікації адміністраторів), з операційними системами, СУБД, мережевим обладнанням, засобами віртуалізації та іншими компонентами інфраструктури. У загальній технології IAM вони відповідають за найкритичніший сегмент – керування обліковими записами з максимальними правами.

Допоміжні засоби контролю та моніторингу

Для повноцінної реалізації IAM/PAM важливу роль відіграють засоби:

- Endpoint Detection and Response (EDR/XDR) – забезпечують додатковий контекст щодо дій користувача на кінцевій точці, дозволяють виявляти підозрілу активність від імені законних облікових записів;

- SIEM-системи – збирають журнали автентифікації, авторизації, зміни прав доступу та інші події безпеки, на основі яких будуються кореляційні правила та сценарії виявлення інцидентів;
- User and Entity Behavior Analytics – аналізують поведінку користувачів і виявляють аномалії, які можуть свідчити про компрометацію облікового запису або зловживання привілеями.

У результаті формується багаторівнева архітектура, де:

- служба каталогів виступає центральним сховищем ідентичностей;
- ILM-системи забезпечують керування життєвим циклом облікових записів;
- SSO/Access Management платформи керують автентифікацією та авторизацією у веб- і хмарних сервісах;
- MFA-платформи підвищують рівень довіри до автентифікації;
- PAM-системи контролюють привілейований доступ;
- EDR/SIEM/UEBA здійснюють моніторинг, журналювання та аналітику.

У контексті даної кваліфікаційної роботи особливий інтерес становить побудова такої архітектури на основі поєднання доменної інфраструктури Active Directory як служби каталогів, комплексу засобів захисту кінцевих точок і серверів (з можливостями політик, ролей і моніторингу) та спеціалізованої PAM-системи, доповнених за потреби open-source компонентами для реалізації SSO або додаткових функцій IAM. Саме це поєднання дозволяє створити цілісну технологію управління ідентифікацією та доступом, яка буде розкрита в наступних розділах роботи.

У межах даної роботи практична реалізація повноцінного PAM-рішення не виконується; основна увага приділяється засобам багатофакторної автентифікації (MFA) для захисту облікових записів та доступу.

ВИСНОВКИ ДО РОЗДІЛУ 1

У першому розділі були розглянуті теоретичні основи управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів. Проаналізовано сутність та призначення систем IAM (Identity and Access Management) і PAM (Privileged Access Management), їх роль у сучасній архітектурі

кібербезпеки, а також ключові принципи – централізація управління ідентичністю, принцип найменших привілеїв, розділення обов'язків, рольовий підхід до доступу, атрибутивний підхід та концепція Zero Trust.

Додано примітку [DY2]: (RBAC)

Додано примітку [DY3]: (ABAC)

Було розглянуто можливості доменної інфраструктури Active Directory [11] як базової платформи для централізованої автентифікації користувачів, побудови груп безпеки, делегування повноважень і застосування групових політик. Визначено, що AD є природним ядром для реалізації IAM в організаціях, які використовують середовище Windows.

Окрему увагу приділено проблематиці управління привілейованими обліковими записами та загрозам, пов'язаним із їхнім використанням: компрометація адміністративних акаунтів, ескалація привілеїв, використання спільних облікових даних, недостатній аудит дій. Показано, що для зниження цих ризиків потрібні спеціалізовані PAM-рішення, які забезпечують зберігання секретів у захищеному сховищі, проксі-доступ, запис сесій та Just-in-Time привілеї. Таким чином, у першому розділі сформовано теоретичне підґрунтя для подальшої розробки технології IAM, окреслено ключові поняття, моделі та підходи, на яких базуватиметься практична частина роботи

На основі стандартів ISO/IEC 27001:2022 [8] та ISO/IEC 27002:2022 [9] і концепції Zero Trust [1] обґрунтовано, що ефективна безпека в умовах гібридної роботи потребує не формального набору документів, а узгодженої системи політик і процедур, які реально відображені в архітектурі та конфігураціях середовища. Це визначає методологічну основу подальших розділів: формування цільової архітектури та розроблення політик, орієнтованих на керування ідентичностями й доступом, мікросегментацію, контроль стану пристроїв, централізоване журналювання та готовність до реагування на інциденти.

2 АНАЛІЗ СУЧАСНОГО СТАНУ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

2.1. Характеристика корпоративного середовища та інформаційних ресурсів

Для проведення дослідження в даній кваліфікаційній роботі розглядається умовне корпоративне середовище середньої організації, структура та IT-інфраструктура якої відповідають типовим умовам сучасних підприємств, що використовують доменну інфраструктуру на базі Active Directory та комплексні засоби захисту кінцевих точок.

Організація складається з центрального офісу та кількох віддалених підрозділів. У центральному офісі розміщено основну частину серверної інфраструктури, включаючи:

- контролери домену Active Directory;
- файлові сервери з доступом до загальних ресурсів підрозділів;
- сервери бізнес-застосунків;
- поштовий сервер;
- засоби захисту інформації.

Віддалені підрозділи підключені до центрального офісу захищеними каналами зв'язку VPN, використовують єдиний домен та отримують доступ до критичних сервісів через внутрішню мережу та, частково, через захищені веб-інтерфейси.

Користувачі корпоративного середовища поділяються на кілька основних категорій:

- рядові співробітники підрозділів;
- керівники структурних підрозділів;
- технічний персонал;
- зовнішні користувачі, які отримують обмежений доступ до окремих сервісів.

Основними інформаційними ресурсами, доступ до яких необхідно регулювати, є:

- облікові записи користувачів та групи безпеки домену;
- файлові ресурси;
- бази даних, які містять конфіденційну інформацію;
- бізнес-застосунки, до яких доступ надається через клієнтські додатки або

Додано примітку [DY4]: (ERP/CRM, системи електронного документообігу);

Додано примітку [DY5]: (сервери керування антивірусним захистом, EDR/XDR-рішення, системи журналювання)

Додано примітку [DY6]: (офісні працівники, аналітики, менеджери з продажу тощо)

Додано примітку [DY7]: (системні адміністратори, адміністратори баз даних, розробники, фахівці з кібербезпеки

Додано примітку [DY8]: (загальні мережеві каталоги, персональні директорії, архіви документів);

веб-інтерфейси;

- адміністративні інтерфейси серверів, мережевого обладнання, засобів віртуалізації та систем захисту інформації.

На рівні інфраструктури для ідентифікації та автентифікації користувачів використовується домен Active Directory, у якому зберігаються облікові записи користувачів, комп'ютерів, груп та інші об'єкти каталогу. Для захисту кінцевих точок та серверів застосовується комплекс рішень ESET, керування яким здійснюється централізовано через сервер керування ESET PROTECT. Для управління та захисту привілейованого доступом планується використання MFA, ESET Secure Authentication, призначеної для контролю адміністративних облікових записів і критичних сесій доступу.

Таким чином, корпоративне середовище, що розглядається, характеризується:

- наявністю доменної інфраструктури, яка служить єдиним джерелом ідентичностей користувачів;
- використанням централізованих засобів захисту кінцевих точок;
- потребою у впорядкованому управлінні доступом до широкого спектра інформаційних ресурсів;
- наявністю різнорівневих категорій користувачів з різною відповідальністю та обсягами прав;
- необхідністю контролю й обмеження привілейованого доступу до критичних ресурсів.

Саме в таких умовах питання побудови цілісної технології управління ідентифікацією та доступом набуває практичного значення, оскільки від ефективності цих процесів залежить захищеність ключових активів організації.

2.2. Аналіз загроз і вразливостей, пов'язаних з управлінням обліковими записами та доступом

Управління обліковими записами та правами доступу користувачів у корпоративному середовищі на базі Active Directory (AD) є одним із найважливіших напрямів забезпечення кібербезпеки. Порушення в цій сфері безпосередньо впливають на конфіденційність, цілісність і доступність

інформаційних ресурсів, а також можуть призвести до повного компрометування доменної інфраструктури.

До основних загроз, пов'язаних з управлінням ідентичністю та доступом, належать:

1. Компрометація облікових даних користувачів

Найбільш розповсюдженим вектором атак є отримання зловмисником дійсних облікових даних користувача домену. Це може відбуватися внаслідок:

- фішингових атак та прийомів соціальної інженерії;
- використання шкідливого програмного забезпечення для перехоплення паролів;
- повторного використання паролів на зовнішніх ресурсах, бази яких були скомпрометовані;
- підбору слабких паролів, особливо за умови відсутності політик складності та блокування облікових записів.

Отримавши обліковий запис звичайного користувача, зловмисник може виконувати дії від його імені, отримувати доступ до файлових ресурсів, поштової скриньки, внутрішніх сервісів та використовувати цей доступ як плацдарм для подальшого руху всередині мережі.

2. Надмірні привілеї та накопичення прав доступу

У процесі роботи співробітника в організації він може багаторазово змінювати посади, підрозділи, брати участь у тимчасових проєктах. У разі відсутності формалізованих процедур періодичного перегляду доступів, користувачі з часом накопичують надмірну кількість прав, які вже не потрібні для виконання їхніх поточних функцій.

Таке накопичення привілеїв впливає на:

- збільшує потенційні наслідки компрометації облікових даних;
- ускладнює аналіз відповідності фактичних прав посадовим обов'язкам;
- створює зайві можливості для ненавмисних помилок або зловживань.

3. Використання спільних облікових записів і відсутність персоніфікації

У деяких випадках для доступу до певних ресурсів компанії застосовуються спільні

Додано примітку [DY9]: (технічні облікові записи, загальні поштові скриньки, акаунти для інтеграцій)

логіни й паролі, відомі кільком співробітникам. Це порушує принцип персоніфікації та призводить до того, що:

- неможливо однозначно визначити, хто саме здійснив ту чи іншу дію;
- складно безпечно змінити пароль при звільненні одного зі співробітників;
- підвищується ризик несанкціонованого доступу при витоку пароля.

Особливо небезпечним є використання спільних адміністративних облікових записів у групах на кшталт «Domain Admins», «Schema Admins» та інших адміністративних групах AD.

4. Недостатній контроль життєвого циклу облікових записів

У багатьох організаціях процеси створення, модифікації та видалення облікових записів у AD виконуються вручну, часто на підставі неформальних запитів. Це призводить до:

- затримок з відключенням доступу після звільнення або переведення співробітника;
- появи залишкових облікових записів, які ніхто фактично не використовує, але які залишаються активними;
- невідповідності між даними HR-системи та фактичними обліковими записи в AD.

Такі облікові записи є зручним об’єктом для зловмисників, оскільки їх легше використовувати непомітно.

5. Помилки конфігурації політик доступу та делегування повноважень

Active Directory надає широкі можливості для делегування адміністративних прав і налаштування політик доступу через групи безпеки та GPO. Неправильні або надмірні делегування створюють окремий клас вразливостей, коли користувачі або служби отримують більше прав, ніж необхідно.

Типові помилки включають:

- делегування прав на зміну паролів або членства в групах без достатнього обмеження кола об’єктів;
- надання технічним обліковим записам прав, що дозволяють змінювати критичні налаштування домену;

- некоректне налаштування ACL на об’єктах каталогу.

6. Ескалація привілеїв у середовищі Active Directory

Особливо небезпечною загрозою є ескалація привілеїв (privilege escalation) – ситуація, коли зловмисник, який спочатку отримав доступ до звичайного доменного облікового запису, поступово підвищує свої права до рівня привілейованих груп (наприклад, «Domain Admins»).

У середовищі AD ескалація привілеїв часто ґрунтується на:

- помилках делегування доступу до OU та об’єктів каталогу (коли користувач або сервіс має право змінювати атрибути акаунтів чи груп, що знаходяться в ланцюжку до привілейованих облікових записів);
- некоректно налаштованих ACL, які дозволяють змінювати членство в групах безпеки або властивості критичних об’єктів;

Додано примітку [DY10]: Access control list

- наявності сервісних облікових записів із надмірними правами, паролі від яких можливо підібрати наприклад, через атаки типу Kerberoasting чи витягнути з конфігураційних файлів;
- використанні вразливих механізмів автентифікації, наприклад Pass-the-Hash, Pass-the-Ticket, що дозволяють повторно використовувати вкрадені хеші паролів або квитки Kerberos без знання самого пароля;
- сценаріях так званих «прихованих адміністраторів», коли користувач формально не входить до привілейованих груп, але сукупність делегованих йому прав дозволяє опосередковано отримати контроль над критичними обліковими записами чи налаштуваннями.

У результаті навіть обмежена початкова компрометація звичайного користувача, наприклад технічного акаунту з невеликими правами, може бути використана як стартова точка для побудови ланцюжка атак, який зрештою приводить до повної компрометації домену. Це робить захист від ескалації привілеїв одним із пріоритетних завдань при розробці технології IAM.

7. Використання застарілих або небезпечних механізмів автентифікації

Застосування слабких криптографічних алгоритмів, застарілих протоколів, відсутність шифрування каналів зв’язку, відсутність багатофакторної

автентифікації для доступу до критичних сервісів – усе це знижує загальну стійкість інфраструктури до атак на облікові записи.

8. Недостатній моніторинг та аудит подій безпеки

За відсутності централізованого збору й аналізу журналів спроб входу, зміни прав, додавання до груп, створення або видалення облікових записів, інциденти, пов'язані з управлінням доступом, можуть залишатися непоміченими протягом тривалого часу. Це дозволяє зловмисникам діяти непомітно, виконувати ескалацію привілеїв і закріплюватися в інфраструктурі.

Отже, сукупність загроз, пов'язаних з управлінням обліковими записами й доступом у середовищі Active Directory, включно з можливістю ескалації привілеїв, вимагає побудови цілісної технології IAM, яка забезпечить:

- мінімізацію прав користувачів і сервісів;
- контроль і обмеження привілейованих облікових записів;
- коректне делегування адміністративних функцій;
- ефективний аудит і моніторинг усіх операцій, пов'язаних з доступом.

Саме ці вимоги будуть покладені в основу формування цільової технології управління ідентифікацією та доступом у подальших підрозділах.

2.3 Оцінка існуючого стану управління ідентифікацією та доступом в організації

На основі загальної характеристики корпоративного середовища та аналізу типових загроз можна виділити ключові особливості та недоліки поточного стану управління ідентифікацією та доступом в умовній організації.

По-перше, процеси управління обліковими записами не є повністю формалізованими. Хоча створення та видалення облікових записів у домені Active Directory здійснюється централізовано адміністраторами, порядок надання прав доступу багато в чому залежить від окремих рішень відповідальних осіб і не завжди жорстко прив'язаний до посадових інструкцій та затверджених ролей. Це призводить до відхилень між формальною структурою організації і фактичним розподілом доступів у домені.

По-друге, структура груп безпеки та організаційних одиниць (OU) в AD сформована переважно історично. У ній можна виділити:

- групи, створені для реалізації конкретних проєктів, які вже завершені, але продовжують існувати;
- користувачів, які залишаються членами груп, доступ до ресурсів яких їм більше не потрібен;
- OU, які не повністю відповідають актуальній організаційній структурі, що ускладнює делегування прав та застосування групових політик.

По-третє, життєвий цикл облікових записів недостатньо автоматизований. Повідомлення про прийом, переведення або звільнення співробітників надходять адміністраторам у вигляді e-mail або усних доручень, після чого вручну створюються або деактивуються облікові записи. Такий підхід має низку наслідків:

- можливі затримки з деактивацією акаунта після звільнення;
- збереження активних акаунтів співробітників, які тривалий час не працюють в організації;
- невідповідність між роллю користувача та фактично призначеними правами при зміні посади.

Це безпосередньо підвищує ризик як навмисних, так і ненавмисних зловживань, а також ускладнює розслідування інцидентів, пов’язаних із привілейованим доступом.

По-четверте, наявні засоби журналювання та моніторингу не завжди забезпечують цілісний огляд подій IAM. Хоча на рівні операційних систем ведуться журнали входу/виходу, зміни облікових записів, події безпеки, їх збір і аналіз можуть бути фрагментованими. Відсутність централізованої кореляції подій (наприклад, у SIEM) означає, що:

- множинні невдалі спроби автентифікації, які передують успішному входу, можуть залишитися непоміченими;
- зміни членства в критичних групах безпеки не завжди виділяються як події підвищеного ризику;
- аномальна активність користувачів не аналізується системно.

По-п’яте, контроль за розподілом прав доступу до файлових ресурсів і бізнес-застосунків є частково ручним. Права на спільні папки, бази даних і прикладні системи задаються як через групи AD, так і локально на рівні самих застосунків. Це ускладнює отримання єдиної картини доступів та веде до ситуацій, коли:

- один і той самий користувач має різні рівні доступу до однотипних ресурсів у різних підрозділах;
- при зміні посади необхідно вручну змінювати налаштування в кількох системах, що збільшує ризик помилок;
- «тимчасові» доступи, надані для виконання разового завдання, залишаються активними після його завершення.

По-шосте, політики автентифікації не повністю відповідають сучасним вимогам, зокрема:

- багатофакторна автентифікація застосовується лише для окремих критичних систем або не застосовується взагалі;
- парольна політика дозволяє використання відносно коротких паролів або недостатньо жорстко регламентує їхню складність;
- не завжди впроваджені механізми виявлення й блокування типових атак на паролі.

У сукупності ці фактори свідчать про те, що існуючий стан управління ідентифікацією та доступом в організації є функціонально працездатним, але недостатньо надійним з точки зору кібербезпеки. Він забезпечує базовий рівень контролю доступу, однак:

- не гарантує мінімізацію прав користувачів і сервісів;
- допускає можливість ескалації привілеїв через помилки конфігурації або накопичені привілеї;
- не забезпечує належного рівня прозорості й аудиту дій, пов’язаних з управлінням доступом.

Це обґрунтовує необхідність розробки цілісної технології IAM, яка:

- спиратиметься на доменну інфраструктуру Active Directory як центральний репозиторій ідентичностей;

- використовуватиме можливості комплексу засобів захисту ESET PROTECT Elite для посилення контролю доступу й моніторингу кінцевих точок;

У наступних підрозділах буде проведено детальний аналіз можливостей зазначених засобів та сформовано вимоги до цільової технології управління ідентифікацією та доступом користувачів у даному корпоративному середовищі.

2.4. Аналіз можливостей Active Directory та комплексу ESET PROTECT Elite у контексті IAM

Після виявлення основних загроз і недоліків чинної моделі управління ідентичністю та доступом доцільно розглянути, яким чином існуючі технології та засоби можуть бути використані для їх мінімізації. У даному підрозділі розглядаються можливості доменної інфраструктури Active Directory та комплексу засобів захисту ESET PROTECT Elite.

2.4.1. Можливості Active Directory в управлінні ідентичністю та доступом

У більшості корпоративних середовищ Active Directory виступає базовою платформою для управління обліковими записами користувачів, комп'ютерів, груп та інших об'єктів. До основних можливостей AD, важливих для IAM, належать:

- **Централізований каталог ідентичностей**
  Усі облікові записи користувачів і групи безпеки зберігаються в єдиному каталозі. Це дозволяє:
  - забезпечувати уніфіковану автентифікацію користувачів у домені;
  - використовувати групи безпеки для управління доступом до файлових ресурсів, застосунків і сервісів;
  - інтегрувати каталог із іншими системами.
- **Організаційні одиниці (OU) та делегування повноважень**
  Структуру домену можна будувати відповідно до організаційної структури підприємства (підрозділи, філії, функціональні напрямки). На рівні OU реалізується делегування адміністративних прав, що дозволяє передавати частину повноважень локальним адміністраторам, не надаючи їм повного

доступу до всього домену. При коректному налаштуванні це є інструментом розподілу обов'язків і зниження ризиків.

- **Групи безпеки та рольовий доступ**
  Active Directory підтримує створення груп, які можуть відображати функціональні ролі (наприклад, «Бухгалтерія_Читання», «HR_Повний_доступ»). Призначення користувачів у такі групи дозволяє реалізувати рольову модель RBAC: права призначаються групам, а не окремим користувачам.
- **Політика паролів та блокування облікових записів**
  AD надає механізми:
  - визначення мінімальної довжини та складності пароля;
  - налаштування строку дії пароля;
  - обмеження кількості невдалих спроб входу.
    Використання цих можливостей дозволяє зменшити ризики компрометації облікових даних через прості паролі та brute-force.
- **Групові політики**
  Групові політики дають змогу централізовано виконувати налаштування безпеки на робочих станціях і серверах, зокрема:
  - обмеження локальних адміністраторських прав;
  - налаштування журналювання подій;
  - вимоги до блокування робочих станцій, використання шифрування, параметрів мережевого доступу.
- **Журналювання та аудит**
  Увімкнення розширеного аудиту в AD дозволяє фіксувати:
  - події входу/виходу;
  - зміну членства в групах;
  - створення, видалення, зміну облікових записів;
  - зміну критичних атрибутів об'єктів.
    Ця інформація може використовуватися як безпосередньо, так і через

інтеграцію з SIEM для виявлення спроб ескалації привілеїв та інших аномалій.

Таким чином, Active Directory забезпечує базовий набір функцій IAM: централізовану ідентифікацію, автентифікацію, рольовий доступ, делегування повноважень та аудит. Однак для повноцінного захисту від сучасних загроз, особливо щодо привілейованих облікових записів та кінцевих точок, необхідна інтеграція з додатковими засобами.

2.4.2. Можливості комплексу ESET PROTECT Elite в контексті IAM

Комплекс ESET PROTECT Elite, зокрема сервер керування ESET PROTECT, агенти на станціях, модулі EDR/Inspect, багатофакторна аутентифікація, традиційно розглядається як рішення класу захисту кінцевих точок. Однак у контексті IAM він виконує важливі допоміжні функції:

- **Інтеграція з Active Directory**
  Сервер керування ESET PROTECT може імпортувати структуру домену, групи та облікові записи, що дозволяє:
  - будувати структуру керованих комп’ютерів відповідно до OU чи груп AD;
  - застосовувати політики безпеки на основі приналежності комп’ютерів та користувачів до певних підрозділів;
  - забезпечити прив’язку подій безпеки до конкретних користувачів домену.
- **Рольове керування доступом до консолі ESET PROTECT**
  Адміністратори системи можуть мати різні ролі (наприклад, адміністратор усієї інфраструктури, адміністратор окремої філії, оператор моніторингу). Це дозволяє обмежити привілеї навіть у межах самої системи захисту, уникати надлишкових прав і реалізувати принцип поділу обов’язків.
- **Політики безпеки на кінцевих точках**
  Через консоль ESET PROTECT можна централізовано:
  - задавати політику використання пристроїв, що впливає на ризики витоку даних;

- контролювати використання конкретних застосунків;
- налаштовувати брандмауер і мережеві правила;
- застосовувати засоби контролю доступу до веб-ресурсів.

Таким чином, навіть при наявності облікових даних користувача зловмисник може бути обмежений у можливості виконувати небезпечні дії на кінцевій точці.

- **Виявлення аномальної активності та спроб ескалації привілеїв**
  Модулі розширеного виявлення дозволяють фіксувати:
  - запуск інструментів, характерних для атак на AD (наприклад, утиліт для збору хешів, сканування домену, Pass-the-Hash/Pass-the-Ticket);
  - спроби виконання підозрілих сценаріїв із підвищеними правами;
  - аномальну поведінку процесів, пов’язану з доступом до системних файлів, реєстру, мережевих служб.

Такі події можуть слугувати індикаторами того, що зловмисник намагається використати скомпрометований обліковий запис для ескалації привілеїв.

- **Журналювання та інтеграція з SOC/SIEM**
  Події, що збираються ESET PROTECT / EDR, можуть передаватися до SIEM або SOC-платформи для кореляції з подіями AD. Це дозволяє створювати комплексні сценарії виявлення, де враховуються і події автентифікації, і поведінка процесів на кінцевих точках.

Отже, ESET PROTECT Elite виступає важливим елементом загальної технології IAM/PAM, забезпечуючи контроль і моніторинг на рівні кінцевих точок, а також рольове керування в межах консолі безпеки.

2.4.3. Можливості ESET Secure Authentication для захисту облікових записів та доступу

ESET Secure Authentication є засобом реалізації багатофакторної автентифікації, який інтегрується з доменною інфраструктурою Active Directory та різними сервісами доступу, наприклад VPN, RDP, SSH, веб-додатки тощо. У контексті даної роботи ESA використовується як ключовий компонент технології IAM для посилення захисту облікових записів та доступу до критичних інформаційних ресурсів.

Основні можливості ESA, релевантні для задач IAM:

– Інтеграція з Active Directory.
ESA інтегрується в домен, що дозволяє зберегти централізований каталог ідентичностей і не створювати окремі акаунти в системі MFA.
– Захист доступу до критичних сервісів за допомогою MFA.
ESA підтримує:

- захист входу користувачів до VPN-шлюзів;
- захист RDP-доступу до серверів;
- захист входу до веб-додатків через підтримувані інтеграції.

Таким чином, навіть при компрометації пароля зловмисник не зможе отримати доступ без другого фактора.
– Різні типи факторів автентифікації.
Система підтримує одноразові паролі (OTP) у мобільному застосунку, push-повідомлення, SMS-коди, апаратні токени тощо. Це дозволяє обрати варіант MFA, який найбільше відповідає вимогам безпеки та зручності в конкретній організації.
– Гнучке призначення MFA за групами користувачів.
Завдяки інтеграції з AD, політики MFA можуть застосовуватися до конкретних груп: наприклад, для адміністраторів домену та співробітників HR MFA є обов’язковою, а для інших користувачів – впроваджується поетапно.
– Централізоване управління та аудит.
Адміністратор має змогу відслідковувати події автентифікації, переглядати спроби входу з MFA та керувати прив’язкою токенів до користувачів. Це підвищує прозорість процесів автентифікації та спрощує розслідування інцидентів.
– Сумісність із існуючою інфраструктурою.
ESA розгортається в наявному домені та не потребує радикальної зміни архітектури. Для організації, яка вже використовує ESET PROTECT, це спрощує інтеграцію та адміністрування.

Таким чином, ESET Secure Authentication виступає важливим компонентом технології IAM, забезпечуючи додатковий рівень захисту для облікових записів та доступу до критичних ресурсів за рахунок багатофакторної автентифікації. У подальших розділах ESA розглядається як основний засіб посиленого контролю доступу до адміністративних та чутливих сервісів.

2.4.3. Можливості ESET Secure Authentication для захисту облікових записів та доступу

ESET Secure Authentication є засобом реалізації багатофакторної автентифікації, який інтегрується з доменною інфраструктурою Active Directory та різними сервісами доступу (VPN, RDP, веб-додатки тощо). У контексті даної роботи ESA використовується як ключовий компонент технології IAM для посилення захисту облікових записів та доступу до критичних інформаційних ресурсів.

Основні можливості ESA, релевантні для задач IAM:

– Інтеграція з Active Directory.

ESA підключається до домену як RADIUS- або AD-інтегрований сервер, використовуючи наявні облікові записи. Це дозволяє зберегти централізований каталог ідентичностей і не створювати окремі акаунти в системі MFA.

– Захист доступу до критичних сервісів за допомогою MFA.

ESA підтримує:

- захист входу у Windows;
- захист підключення по RDP;
- будь що за протоколом RADIUS(VPN,SSH, Linux login тощо);
- Захист підтримуваних веб застосунків та інтеграція за допомогою SAML;
- Захист AD FS;
- Identity Provider Connector;
- Компонент ESA Authentication Server містить API на основі REST, який можна використовувати для додавання 2FA в користувацькі програми.

– Різні типи факторів автентифікації.

Система підтримує одноразові паролі у мобільному застосунку, одноразові паролі поштою або за допомогою SMS, push-повідомлення в мобільному застосунку,

апаратні токени. Це дозволяє обрати варіант багатофакторної аутентифікації, який найбільше відповідає вимогам безпеки та зручності в конкретній організації.

– Гнучке призначення багатофакторної аутентифікації користувачам.

Завдяки інтеграції з AD, багатофакторну аутентифікацію можуть застосовувати до конкретних груп: наприклад, для адміністраторів домену та співробітників HR багатофакторна аутентифікація є обов'язковою, а для інших користувачів – впроваджується поетапно.

– Централізоване управління та аудит.

Адміністратор має змогу відслідковувати події автентифікації, переглядати спроби входу з багатофакторною аутентифікацією та керувати прив'язкою токенів до користувачів. Це підвищує прозорість процесів автентифікації та спрощує розслідування інцидентів.

– Сумісність із існуючою інфраструктурою.

ESA розгортається поверх вже наявного домену та не потребує радикальної зміни архітектури. Для організації, яка вже використовує ESET PROTECT, це спрощує інтеграцію та адміністрування.

Таким чином, ESET Secure Authentication виступає важливим компонентом технології IAM, забезпечуючи додатковий рівень захисту для облікових записів та доступу до критичних ресурсів за рахунок багатофакторної автентифікації. У подальших розділах ESA розглядається як основний засіб посиленого контролю доступу до адміністративних та чутливих сервісів.

2.5. Формування вимог до технології управління ідентифікацією та доступом користувачів

На основі:

- аналізу загроз і вразливостей, пов'язаних з управлінням обліковими записами та доступом у середовищі Active Directory (підрозділ 2.2);
- оцінки поточного стану процесів IAM в організації (підрозділ 2.3);
- аналізу можливостей Active Directory, комплексу ESET PROTECT Elite(підрозділ 2.4);

можна сформулювати вимоги до цільової технології управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів.

Функціональні вимоги:

1. **Централізоване управління ідентичністю**
    - використання Active Directory як єдиного репозиторію облікових записів користувачів і груп;
    - уніфіковані правила створення, зміни та видалення облікових записів;
    - чітка відповідність між функціональними ролями та членством у групах безпеки.
2. **Реалізація рольової моделі доступу (RBAC)**
    - визначення ролей для основних категорій користувачів (рядові співробітники, керівники, технічний персонал, зовнішні користувачі);
    - встановлення відповідності «роль → набір прав доступу» до файлових ресурсів, систем і сервісів;
    - мінімізація індивідуальних (ручних) призначень прав на користувачів.
3. **Керування життєвим циклом облікових записів**
    - формалізовані процедури створення акаунтів при прийомі на роботу, зміни прав при зміні посади та їх деактивації при звільненні;
    - періодичний перегляд прав доступу керівниками підрозділів.
4. **Багатофакторна аутентифікація**
    - застосування багатофакторної автентифікації для доступу до критичних систем (адміністративні консолі, віддалений доступ, доступ до конфіденційних даних);
    - диференціація вимог до автентифікації за категоріями користувачів і типами операцій;
5. **Моніторинг та аудит IAM**
    - централізований збір журналів автентифікації, змін прав, членства в групах, дій привілейованих користувачів;
    - інтеграція подій AD, ESET PROTECT із системами моніторингу/аналізу (SIEM або аналог);

- можливість формування звітів щодо активності користувачів і відповідності прав посадовим функціям.

6. **Виявлення та запобігання ескалації привілеїв**
    - регулярний аналіз конфігурації AD (ACL, делегування, членство в групах) для виявлення ланцюжків ескалації;
    - виявлення на кінцевих точках інструментів і дій, характерних для атак на AD;
    - окремі категорії користувачів, для яких MFA є обов'язковою
    - обов'язкова багатофакторна аутентифікація для доступу до критичних ресурсів.

Нефункціональні вимоги:

1. **Відповідність нормативним вимогам та стандартам**
    - узгодженість політик доступу та процесів IAM з вимогами ISO/IEC 27001, 27002, 27005, 27035 та іншими релевантними стандартами;
    - дотримання законодавчих вимог щодо обробки персональних даних і захисту інформації.
2. **Масштабованість і гнучкість**
    - здатність технології підтримувати збільшення кількості користувачів, систем і філій без істотної перебудови архітектури;
    - можливість розширення (інтеграція з новими сервісами, хмарними платформами).
3. **Надійність і стійкість до відмов**
    - резервування ключових компонентів (контролерів домену, серверів безпеки);
    - забезпечення безперервності роботи критичних процесів автентифікації та авторизації.
4. **Зручність адміністрування та експлуатації**
    - наявність зрозумілих інтерфейсів керування та звітності для адміністраторів;

- можливість часткової автоматизації типових операцій (надання доступу, зміна прав, блокування акаунтів).

5. **Інтегрованість і сумісність**
   - підтримка стандартних протоколів і механізмів інтеграції (LDAP, Kerberos, SAML, OAuth2/OIDC);
   - можливість взаємодії між AD, ESET PROTECT та open-source компонентами в межах єдиної технології IAM.

Сформульовані вимоги слугуватимуть основою для розробки цільової технології управління ідентифікацією та доступом, що буде описана в розділі 3. У наступному розділі буде розроблено архітектуру рішення, модель ролей і політик доступу, показано інтеграцію Active Directory та комплексу ESET PROTECT Elite у єдину технологію IAM, а також розглянуто питання оцінювання її ефективності.

ВИСНОВКИ ДО РОЗДІЛУ 2

У другому розділі виконано аналіз управління ідентичністю та доступом в умовному корпоративному середовищі на базі Active Directory та наявних засобів захисту. Виявлено основні загрози та вразливості, пов’язані з обліковими записами користувачів і привілейованими акаунтами: компрометація облікових даних, накопичення надмірних прав, використання спільних облікових записів, недостатньо формалізований життєвий цикл акаунтів, помилки делегування повноважень та небезпечні сценарії ескалації привілеїв у домені.

Було показано, що існуючі процеси управління доступом є функціонально працездатними, але недостатньо зрілими з точки зору кібербезпеки: структура OU та груп AD сформована історично, регламенти надання й відкликання доступів частково ручні, контроль привілейованих акаунтів обмежений, а моніторинг подій IAM фрагментарний. Це створює умови для потенційного несанкціонованого доступу, прихованої ескалації привілеїв та ускладнює розслідування інцидентів.

На основі аналізу можливостей Active Directory та комплексу ESET PROTECT Elite було сформульовано вимоги до цільової технології IAM. До ключових вимог віднесено: централізоване управління ідентичністю, впровадження рольової моделі доступу, формалізацію життєвого циклу акаунтів, виділення та контроль

привілейованих облікових записів, застосування багатофакторної автентифікації для критичних операцій, централізований аудит і моніторинг подій, а також здатність виявляти та запобігати ескалації привілеїв.

У результаті другого розділу обґрунтовано необхідність розробки цілісної технології IAM, яка використовуватиме наявну доменну інфраструктуру, засоби захисту кінцевих точок та двохфакторну аутентифікацію для зниження виявлених ризиків.

3 РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

3.1. Проєктування цільової архітектури IAM для корпоративного середовища

На основі вимог, сформованих у розділі 2, у даному підрозділі розробляється цільова архітектура технології управління ідентифікацією та доступом користувачів. Архітектура має спиратися на наявну доменну інфраструктуру Active Directory та комплекс засобів захисту ESET PROTECT Elite.

3.1.1. Архітектурні принципи побудови технології IAM.

Цільова архітектура IAM розробляється з урахуванням таких базових принципів:

- Централізація управління ідентичністю – усі облікові записи користувачів, груп і сервісів зберігаються в єдиному каталозі Active Directory. Інші системи використовують AD як джерело істини щодо ідентичностей.
- Рольова модель доступу – права доступу до корпоративних ресурсів визначаються не на рівні окремих користувачів, а через ролі, відображені в групах безпеки AD. Надання або відкликання доступу здійснюється через зміну ролей.
- Принцип найменших привілеїв та поділу обов’язків – кожен користувач та сервіс отримує лише мінімально необхідний набір прав. Критичні операції, пов’язані з управлінням доменом, повинні виконуватися обмеженим колом адміністраторів із застосуванням MFA і, по можливості, за участю кількох осіб.
- Just-in-Time та Just-Enough-Access для привілейованих дій – підвищені права надаються лише на час виконання конкретного завдання і в обсязі, мінімально необхідному для його виконання.
- Модульність та інтегрованість – архітектура має складатися з окремих модулів, які взаємодіють через стандартні протоколи та інтерфейси.
- Прозорість та аудит – усі критичні операції, пов’язані з управлінням обліковими записами, правами, привілейованими сесіями та автентифікацією, мають журналюватися та бути доступними для аналізу.

- Підтримка концепції Zero Trust – доступ до ресурсів не повинен базуватись лише на розташуванні в «довіреній» мережі. При ухваленні рішень про доступ враховується ідентичність, контекст (тип пристрою, місцезнаходження, час), рівень ризику та політики безпеки.

3.1.2. Логічна структура цільової архітектури

Логічно технологію IAM можна представити у вигляді кількох взаємопов'язаних рівнів:

- Рівень управління ідентичністю
  - служба каталогів Active Directory;
  - організаційні одиниці, що відображають структуру організації;
  - облікові записи користувачів, комп'ютерів, сервісів;
  - групи безпеки, що реалізують ролі доступу.
- Рівень управління доступом
  - Багатофакторна автентифікації ESET Secure Authentication для критичних сценаріїв доступу.
  - механізми автентифікації та авторизації в AD;
  - політики доступу до файлових ресурсів, баз даних, внутрішніх застосунків через групи AD.
- Рівень захисту кінцевих точок і моніторингу;
  - агенти та продукти захисту ESET на робочих станціях і серверах;
  - політики безпеки на кінцевих точках;
  - централізована консоль ESET PROTECT із рольовою моделлю для адміністраторів безпеки.
- Рівень журналювання та аналітики
  - централізований збір логів AD (події входу, зміни членства в групах, зміни облікових записів);
  - логування подій ESET Secure Authentication, ESET PROTECT та ESET Inspect;
  - SIEM, яка дозволяє будувати сценарії виявлення ескалації привілеїв та інших аномалій.

Додано примітку [DY11]: На схемі (для ілюстрації в дипломі) це можна подати як багатошарову архітектуру, де:
в центрі – Active Directory як ядро ідентичностей;
з одного боку – esa, який «нависає» над привілейованими обліковими записами;
з іншого боку – ESET PROTECT, який «спостерігає» за діяльністю на кінцевих точках;
зверху – шар Access Management / SSO для прикладних систем;
знизу – шар моніторингу та SIEM, що збирає події від усіх компонентів.

3.1.3. Потоки взаємодії та основні сценарії

У межах запропонованої архітектури можна виділити кілька ключових сценаріїв взаємодії.

1) Звичайний вхід користувача в домен та доступ до ресурсів

- Користувач проходить автентифікацію в домені Active Directory (Kerberos).
- За потреби, проходиться перевірка другого фактору.
- На основі його членства в групах безпеки AD система визначає, до яких ресурсів він має доступ.
- Політики GPO застосовуються до робочої станції користувача: налаштування безпеки, брандмауер, обмеження локальних прав.
- Агенти та продукти захисту ESET забезпечують контроль стану кінцевої точки.
- Події автентифікації та доступу фіксуються в журналах AD та можуть передаватися до SIEM.

2) Доступ до веб-застосунків та хмарних сервісів

- Користувач аутентифікується через AD FS SSO з перевіркою другого фактору за допомогою ESET Secure Authentication.

4) Моніторинг та виявлення підозрілої активності

- Події AD, ESET PROTECT, багатофакторної аутентифікації надходять до централізованої системи збору логів.
- На основі кореляційних правил виявляються сценарії, характерні для ескалації привілеїв:
  - численні невдалі спроби входу з подальшим успішним входом;
  - раптове додавання користувача до груп високого рівня;
  - нетипові адміністративні сесії в неробочий час;
- При виявленні таких подій ініціюються розслідування і, за потреби, автоматичні реакції.

Додано примітку [DY12]: (входи, зміна прав, додавання до груп)

Додано примітку [DY13]: (підозрілі процеси, експлойти, змінена поведінка)

Додано примітку [DY14]: (блокування облікового запису, завершення сесії, ізоляція станції)

3.1.4. Роль окремих компонентів у цільовій архітектурі

У межах запропонованої архітектури кожен компонент виконує чітко визначену функцію в загальній технології управління ідентифікацією та доступом.

Active Directory - є ядром ідентичностей організації. У каталозі AD зберігаються облікові записи користувачів, комп'ютерів і сервісів, а також групи безпеки, що реалізують рольову модель доступу. Active Directory забезпечує:

- централізовану автентифікацію користувачів і сервісів (Kerberos/NTLM);
- побудову OU-структури відповідно до організаційної структури;
- делегування адміністративних повноважень;
- застосування групових політик безпеки (GPO) до робочих станцій і серверів;
- єдине «джерело істини» для інших компонентів технології IAM.

ESET PROTECT Elite - відповідає за контроль і захист кінцевих точок, доповнюючи механізми IAM на рівні пристроїв. У контексті запропонованої технології ESET PROTECT забезпечує:

- централізоване розгортання та керування агентами захисту на робочих станціях і серверах;
- застосування політик безпеки з урахуванням ролей і груп Active Directory (наприклад, посилені обмеження для комп'ютерів користувачів HR чи адміністраторів);
- виявлення шкідливих програм, експлойтів і підозрілої активності, що може бути пов'язана зі спробами ескалації привілеїв або зловживанням обліковими записами;
- надання додаткових телеметричних даних для аналізу інцидентів, пов'язаних з управлінням доступом.

ESET Secure Authentication - є ключовим компонентом рівня посиленої автентифікації в розробленій технології. ESA інтегрується з Active Directory та використовується для захисту доступу до критичних облікових записів, ресурсів і сервісів. Основні функції ESA в архітектурі:

- реалізація багатофакторної автентифікації для окремих категорій користувачів (насамперед адміністраторів, співробітників, які працюють з конфіденційними даними, та користувачів, що отримують віддалений доступ до ресурсів);

- захист доступу до сервісів VPN, RDP, веб-застосунків та інших критичних точок входу в інфраструктуру навіть у разі компрометації пароля;
- прив’язка політик MFA до груп і ролей у Active Directory, що дозволяє, зокрема, зробити MFA обов’язковою для членів адміністративних та високоризикових ролей;
- централізоване керування токенами та засобами другого фактора, аудит подій автентифікації й MFA, що підвищує прозорість доступу до критичних ресурсів.

Для уніфікації доступу до веб-застосунків і окремих хмарних сервісів у архітектурі може використовуватися роль федеративних служб Active Directory (AD FS). AD FS виступає як служба єдиного входу (SSO), яка:

- забезпечує автентифікацію користувачів на основі їхніх доменних облікових записів;
- видає токени доступу для веб-застосунків, що підтримують протоколи SAML, OAuth, OpenID Connect;
- дозволяє передавати до застосунків атрибути користувача та його ролі, отримані з Active Directory;
- інтегрується з ESET Secure Authentication, використовуючи як додатковий крок під час входу до окремих застосунків або при доступі ззовні.

Окрему роль відіграють засоби централізованого журналювання та аналітики подій (лог-менеджери, SIEM-системи), вони:

- збирають події з Active Directory (входи, зміни членства в групах, зміни облікових записів), ESET PROTECT (події безпеки на кінцевих точках), ESET Secure Authentication (успішні та невдалі спроби MFA), а також з інших критичних компонентів;
- дозволяють будувати кореляційні правила й виявляти підозрілі сценарії (спроби ескалації привілеїв, аномальні входи, багаторазові відмови MFA тощо);
- забезпечують підґрунтя для оперативного реагування на інциденти та проведення розслідувань.

Узгоджена робота Active Directory, ESET PROTECT Elite, ESET Secure Authentication [21], AD FS та систем журналювання формує цілісну технологію управління ідентифікацією та доступом користувачів, яка поєднує централізоване керування ідентичністю, рольовий контроль доступу, багатофакторну автентифікацію критичних облікових записів, єдиний вхід до низки сервісів і постійний моніторинг використання доступів.

3.2. Моделювання ролей та політик доступу в системі управління ідентифікацією та доступом

Ефективне управління ідентифікацією та доступом у корпоративному середовищі неможливе без чітко визначеної рольової моделі. Саме ролі визначають, які дії користувач може виконувати з інформаційними ресурсами, а також які додаткові вимоги до безпеки (наприклад, обов'язкове застосування багатофакторної автентифікації) до нього висуваються.

У цьому підрозділі формується рольова модель для умовної організації, що використовує доменну інфраструктуру Active Directory, засоби захисту кінцевих точок ESET PROTECT Elite та систему багатофакторної автентифікації ESET Secure Authentication (ESA). Окремі сценарії можуть доповнюватися використанням служб федерації Active Directory Federation Services (AD FS) [14] для єдиного входу (SSO) у веб-застосунки.

3.2.1. Принципи побудови рольової моделі

Під роллю у контексті IAM розуміють логічну сутність, що поєднує в собі набір повноважень і прав доступу, необхідних користувачу для виконання його посадових обов'язків. Рольова модель (Role-Based Access Control, RBAC) дозволяє прив'язувати доступ не до окремих осіб, а до ролей, що істотно спрощує управління правами та зменшує ризики їх неконтрольованого накопичення.

При розробленні рольової моделі для умовної організації приймаються такі базові принципи:

- Принцип найменших привілеїв

Кожен користувач повинен мати лише ті права, які необхідні йому для виконання службових задач. Ролі формуються так, щоб уникати надмірних привілеїв, а доступ до конфіденційних даних та критичних систем обмежується окремими ролями з підвищеними вимогами до безпеки.

- Відповідність організаційній структурі.

  Ролі повинні відображати реальну організаційну структуру: підрозділи (відділ продажів, HR, IT), посади (співробітник, керівник, адміністратор), а також участь в окремих проєктах. Це дозволяє легко співвідносити ролі з посадовими інструкціями та регламентами.

- Розділення обов'язків.

  Для критичних операцій (наприклад, управління фінансовими транзакціями, адміністрування домену, доступ до персональних даних) функції поділяються між різними ролями, щоб одна особа не могла одноосібно здійснити повний цикл потенційно небезпечних дій.

- Централізоване управління через Active Directory.

  Усі ролі відображаються у вигляді груп безпеки в Active Directory. Облікові записи користувачів прив'язуються до ролей шляхом додавання до відповідних груп. Ролі не «зашиваються» в окремі системи, а базуються на єдиному каталозі AD [13].

- Посилення захисту за рахунок MFA.

  Для окремих ролей, пов'язаних з підвищеним ризиком (адміністратори, HR, користувачі з доступом до конфіденційних даних), доступ до критичних ресурсів захищається за допомогою багатофакторної автентифікації через ESET Secure Authentication [21]. Таким чином, роль визначає не лише права доступу, а й рівень вимог до автентифікації.

- Масштабованість та модульність.

  Ролі мають бути побудовані так, щоб їх можна було комбінувати: базова роль користувача + функціональна роль доступу до конкретної системи +, за потреби, тимчасова проєктна роль. Це полегшує адаптацію моделі до змін у структурі та впровадження нових сервісів.

З урахуванням цих принципів далі формуються класи ролей та їх відображення у структурі Active Directory.

3.2.2. Класифікація ролей користувачів в умовній організації

Для зручності побудови та подальшого супроводу рольової моделі виділимо кілька основних класів ролей.

Базові ролі співробітників - це ролі, що відображають належність користувача до певного підрозділу та рівня відповідальності:

- «Співробітник відділу продажів»;
- «Керівник відділу продажів»;
- «Співробітник HR»;
- «Співробітник фінансового відділу» тощо.

Такі ролі відповідають за:

– доступ до типових офісних ресурсів (спільні папки підрозділів, внутрішні портали);

– базовий доступ до профільних систем (CRM, документообіг, облік персоналу тощо).

Функціональні ролі доступу до прикладних систем відображають конкретні функції в прикладних системах:

- «Користувач CRM», «Менеджер CRM»;
- «Користувач BI-звітів», «Адміністратор BI-системи»;
- «Користувач HR-модуля документообігу» тощо.

Вони дозволяють розмежувати права всередині систем: наприклад, відокремити роль звичайного користувача, який вводить дані, від ролі менеджера, який аналізує та затверджує інформацію.

Клас адміністративних та технічних ролей охоплює:

- адміністраторів домену й серверів;
- адміністраторів прикладних систем;
- адміністраторів засобів захист.

Для них характерні підвищені привілеї та, відповідно, підвищені вимоги до контролю. Для адміністративних ролей застосовується обов'язковий MFA при доступі до критичних ресурсів.

Ролі, що створюються для конкретних проєктів або задач на визначений період:

- «Учасник проєкту X»;
- «Аудитор доступу»;
- «Тимчасовий консультант» тощо.

Такі ролі дають змогу надати потрібний доступ на певний час, не змінюючи постійні базові ролі користувачів.

Для кожного класу ролей далі визначається, до яких ресурсів надається доступ, які права встановлюються, а також чи потрібна MFA.

3.2.3. Відображення ролей у структурі Active Directory

Реалізація рольової моделі у технічному плані здійснюється через використання груп безпеки в Active Directory. При цьому доцільно розділити:

- рольові групи - відповідають ролям користувачів;
- ресурсні групи - відповідають правам доступу до конкретних ресурсів (папок, баз даних, прикладних систем).

Для впорядкування використовується окрема OU-структура, наприклад:

- OU=RBAC_Groups
    - OU=BusinessRoles – рольові групи бізнес-користувачів;
    - OU=ITRoles – рольові групи адміністраторів та IT-персоналу;
    - OU=ResourceGroups – групи доступу до ресурсів.

Приклад іменування груп:

- рольові групи:
    - GRP_ROLE_SALES_USER, GRP_ROLE_SALES_MANAGER;
    - GRP_ROLE_HR_EMPLOYEE;
    - GRP_ROLE_WIN_SERVER_ADMIN;
- ресурсні групи:

- GRP_SHARE_SALES_RO, GRP_SHARE_SALES_RW, GRP_SHARE_SALES_FULL;
- GRP_SHARE_HR_FULL;
- GRP_APP_CRM_USER, GRP_APP_CRM_MANAGER;
- GRP_APP_DOCFLOW_HR тощо.

Принцип побудови:

1. Користувач додається до **рольових груп** залежно від його посади, підрозділу та функцій.
2. Рольові групи додаються до **ресурсних груп**, які безпосередньо мають права на ресурси.
3. Ресурсні групи отримують дозволи на файлових серверах, у прикладних системах тощо.

Таким чином, при зміні посади або переході в інший підрозділ достатньо змінити членство користувача в рольових групах – права доступу будуть автоматично скориговані через зв’язки рольових і ресурсних груп.

3.2.4. Приклади побудови ролей та прав доступу

Приклад 1. Роль «Співробітник відділу продажів»

- Рольова група: GRP_ROLE_SALES_USER.
- Ресурсні групи:
  - GRP_SHARE_SALES_RO – читання спільних матеріалів;
  - GRP_APP_CRM_USER – доступ до CRM як звичайного користувача.
- Відображення:
  - GRP_ROLE_SALES_USER ∈ GRP_SHARE_SALES_RO;
  - GRP_ROLE_SALES_USER ∈ GRP_APP_CRM_USER.

Для цієї ролі рекомендовано використовувати багатофакторну аутентифікацію.

Приклад 2. Роль «Керівник відділу продажів»

- Рольова група: GRP_ROLE_SALES_MANAGER.
- Ресурсні групи:
  - GRP_SHARE_SALES_FULL – повний доступ до папки відділу;
  - GRP_APP_CRM_MANAGER – розширені права в CRM;

- GRP_APP_BI_SALES_REPORTS – доступ до аналітичних звітів.

- Відображення:
  - GRP_ROLE_SALES_MANAGER ∈ GRP_SHARE_SALES_FULL;
  - GRP_ROLE_SALES_MANAGER ∈ GRP_APP_CRM_MANAGER;
  - GRP_ROLE_SALES_MANAGER ∈ GRP_APP_BI_SALES_REPORTS.

Для цієї ролі багатофакторна аутентифікація є обов'язковою для доступу до CRM та BI-систем ззовні.

Приклад 3. Роль «Співробітник HR»

- Рольова група: GRP_ROLE_HR_EMPLOYEE.
- Ресурсні групи:
  - GRP_SHARE_HR_FULL – повний доступ до папки HR;
  - GRP_APP_DOCFLOW_HR – доступ до HR-модуля документообігу.

Багатофакторна аутентифікація для GRP_ROLE_HR_EMPLOYEE налаштовується як обов'язкова при доступі до HR-систем.

Приклад 4. Роль «Адміністратор серверів Windows»

- Рольова група: GRP_ROLE_WIN_SERVER_ADMIN.
- Ресурсні групи:
  - GRP_RDP_WIN_SERVERS – дозволяє RDP-доступ до серверів;
  - GRP_LOCAL_ADMINS_SERVERS – локальні адмін-права на серверах.

Для цієї ролі багатофакторна аутентифікація є обов'язковою умовою доступу до VPN, RDP та адміністративних веб-консолей.

риклад 5. Тимчасова роль «Учасник проєкту X»

- Рольова група: GRP_ROLE_PROJECT_X.
- Ресурсна група: GRP_SHARE_PROJECT_X – доступ до папки \\FS01\Projects\X.

Час життя цієї ролі обмежений рамками проєкту; після завершення роботи користувачі вилучаються з GRP_ROLE_PROJECT_X, і доступ автоматично відкликається.

3.2.5. Приклади політик доступу та взаємодії з багатофакторною аутентифікацією

Для того, щоб рольова модель працювала як цілісний механізм IAM, ролі та групи доповнюються формалізованими політиками доступу.

Політика 1. Доступ до HR-даних

- Доступ до \\FS01\HR та HR-модуля мають тільки члени GRP_ROLE_HR_EMPLOYEE.
- Доступ ззовні мережі можливий лише за наявності успішної MFA через ESA.
- Обробка персональних даних дозволена тільки з корпоративних комп'ютерів HR, для яких через ESET PROTECT:
    - заборонено запис на USB-носії;
    - за потреби увімкнено шифрування дисків.

Політика 2. Адміністрування домену та серверів

- Адміністративні операції виконуються лише акаунтами з груп GRP_ROLE_ADMINS_CANDIDATE та GRP_ROLE_WIN_SERVER_ADMIN.
- Для цих акаунтів обов'язкова MFA при доступі до VPN, RDP та адміністративних веб-консолей.
- Прямий інтерактивний вхід привілейованими акаунтами на звичайні робочі станції забороняється через GPO.

Політика 3. Запобігання ескалації привілеїв

- Звичайні користувачі не мають локальних адмін-прав на своїх станціях.
- Винятки оформлюються як тимчасова роль (наприклад, GRP_TEMP_LOCAL_ADMINS), для якої MFA є обов'язковою умовою.
- ESET PROTECT контролює запуск інструментів, пов'язаних з ескалацією привілеїв, та генерує події безпеки.

Політика 4. Журналювання й аудит IAM/MFA-подій

- Увімкнено аудит у AD [12] (створення/видалення акаунтів, зміни членства в групах, спроби входу).
- ESA журналює всі MFA-події (успішні/невдалі) з можливістю експорту до централізованої системи журналювання.

- ESET PROTECT передає події, пов’язані з підозрілою активністю на кінцевих точках.
- У системі журналювання/аналітики події корелюються, що дозволяє виявляти підозрілі сценарії: наприклад, комбінацію додавання до привілейованої групи, невдалих спроб MFA та запуску спеціалізованих інструментів на станції користувача.

ВИСНОВКИ ДО РОЗДІЛУ 3

У третьому розділі кваліфікаційної роботи було розроблено та обґрунтовано технологію управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів на базі доменної інфраструктури Active Directory [12], комплексу засобів захисту кінцевих точок ESET PROTECT Elite та системи багатофакторної автентифікації ESET Secure Authentication [20] з можливим використанням служб федерації Active Directory Federation Services (AD FS) для забезпечення єдиного входу (SSO).

На основі вимог, сформульованих у другому розділі, спроєктовано цільову архітектуру технології IAM, яка реалізує принципи централізації управління ідентичністю, рольової моделі доступу, принципу найменших привілеїв, розділення обов’язків і посиленого контролю доступу до критичних ресурсів за рахунок багатофакторної автентифікації. Архітектура включає логічні рівні: управління ідентичністю, управління доступом (рольові групи та ресурсні групи, політики доступу), рівень посиленої автентифікації, рівень захисту кінцевих точок (ESET PROTECT Elite) та рівень журналювання й аналітики подій.

Було розроблено рольову модель доступу, яка охоплює базові ролі співробітників, функціональні ролі доступу до прикладних систем типу CRM, документообіг, BI), адміністративні ролі та тимчасові проєктні ролі. Показано, як ці ролі відображаються у вигляді груп безпеки Active Directory [13], які у свою чергу пов’язуються з ресурсними групами для файлових ресурсів, прикладних систем і сервісів віддаленого доступу. Для окремих високоризикових ролей (адміністратори, співробітники HR, користувачі з доступом до конфіденційних

даних) передбачено обов’язкове застосування багатофакторної автентифікації через ESET Secure Authentication [20].

На лабораторному стенді реалізовано інтеграцію між Active Directory, сервером ESET PROTECT [18] та системою ESET Secure Authentication. Описано послідовність налаштування: створення OU та груп у домені, побудова зв’язків між рольовими та ресурсними групами, призначення прав доступу до файлових ресурсів і прикладних систем, розгортання агентів ESET на робочих станціях і серверах, підключення ESA до каталогу AD, призначення MFA-політик для вибраних ролей, а також, за потреби, інтеграція з AD FS для реалізації SSO з MFA для веб-застосунків. Розроблено демонстраційні сценарії, що ілюструють як штатні процеси (прийом, зміна посади, звільнення, надання тимчасового доступу до проєктів), так і ситуації з доступом до критичних ресурсів (адміністрування серверів, обробка HR-даних), захищених багатофакторною автентифікацією.

Запропоновано методику оцінювання ефективності технології IAM, яка базується на системі кількісних та якісних показників: частка доступів, реалізованих через ролі та групи AD; рівень формалізації життєвого циклу облікових записів; кількість і характер привілейованих облікових записів; стійкість до ескалації привілеїв; рівень використання MFA для критичних ролей і сервісів; повнота журналювання IAM/MFA-подій та можливість їх кореляції з подіями безпеки на кінцевих точках. Сформовано критерії успішності впровадження (мінімізація надмірних привілеїв, обов’язковий MFA для визначених ролей, централізація управління доступом і журналювання).

Отже, у третьому розділі виконано проєктування, реалізацію на лабораторному стенді та методичне обґрунтування технології управління ідентифікацією та доступом користувачів, яка спирається на вже поширені в організаціях технології (Active Directory, ESET PROTECT Elite, ESET Secure Authentication, AD FS) та дозволяє суттєво знизити ризики, виявлені у попередніх розділах, забезпечивши контрольований, рольовий і посилено захищений доступ до корпоративних інформаційних ресурсів.

ВИСНОВКИ

У кваліфікаційній роботі розглянуто проблему побудови дієвих політик інформаційної безпеки для організацій із on-premise інфраструктурою та гібридною моделлю роботи, де традиційна «периметрова» логіка захисту вже не забезпечує потрібної стійкості. Досягнуто мети роботи — розроблено технологію створення політик безпеки для інформаційної системи організації на основі моделі нульової довіри та визначено практичні підходи до її впровадження.

У першому розділі узагальнено сучасний ландшафт кіберзагроз і показано, що найбільш критичними для типових організацій є атаки на ідентичності, зростання частки ransomware, експлуатація вразливостей у публічно доступних компонентах і периметрі, а також посилення ролі третіх сторін і supply chain-атак. Окремо підкреслено український контекст, де інтенсивність кібератак і специфіка противника вимагають системного підходу до політик та опори на стандарти й рекомендації профільних органів реагування.

У другому розділі на прикладі узагальненої Windows-орієнтованої on-premise ІС із Active Directory, DMZ і віддаленим доступом визначено типові слабкі місця (парольна автентифікація без MFA, слабка сегментація, частковий BYOD, обмежене логування/моніторинг). На цій основі сформовано вимоги до захисту в парадигмі Zero Trust та спроєктовано цільову архітектуру: логічна сегментація на зони, “deny-by-default/allowlist” для міжсегментних взаємодій, обов’язкова MFA для VPN/RDP і привілейованих сценаріїв, керований захист кінцевих точок (EPP/EDR), мережевий рівень видимості, централізоване журналювання/кореляція (SIEM), ізоляція резервного контуру та дисципліна оновлень і керування вразливостями.

У третьому розділі розроблено технологію формування політик як узгодженого набору вимог, правил і процедур для ключових напрямів: керування доступом і життєвим циклом облікових записів (RBAC, JML), автентифікація та віддалений доступ (MFA, контроль пристроїв і маршрутів), захист робочих станцій/серверів (базовий безпечний стан, зменшення площини атаки), а також

моніторинг і реагування (джерела подій, пріоритетні сценарії детекції, ескалація). Наведений приклад практичної реалізації політик на базі ESET PROTECT/Endpoint/Server Security, ESET Secure Authentication, ESET Full Disk Encryption, AD/GPO та Suricata (IDS) демонструє, як перейти від “декларативних” документів до реально застосованих і контрольованих налаштувань у середовищі.

Практичне значення отриманих результатів полягає в тому, що запропонована технологія може бути використана як шаблон для організацій середнього масштабу, які прагнуть підвищити керованість безпеки без повної перебудови IT-ландшафту: вона задає цільовий стан, пріоритизацію контролів і зрозумілий маршрут поетапного впровадження Zero Trust. Подальший розвиток роботи доцільно спрямувати на деталізацію SIEM-контенту (use-case’и, кореляції, метрики ефективності), автоматизацію перевірок відповідності (continuous posture), а також розширення моделі на хмарні сервіси та Zero Trust Network Access (ZTNA) для змішаних середовищ.

ПЕРЕЛІК ПОСИЛАНЬ

1. NIST SP 800-207: Zero Trust Architecture National Institute of Standards and Technology. — Washington: U.S. Department of Commerce, 2022. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

2. NIST SP 800-123: Guide to General Server Security National Institute of Standards and Technology. — Washington: U.S. Department of Commerce, 2008. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

3. NIST SP 800-92: Guide to Computer Security Log Management, Analysis, and Retention National Institute of Standards and Technology. — Washington: U.S. Department of Commerce, 2006. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

4. NIST SP 800-94: Guide to Intrusion Detection and Prevention (IDP) Systems National Institute of Standards and Technology. — Washington: U.S. Department of Commerce, 2007. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

5. NIST SP 800-52 Rev. 2: Guidelines for TLS Implementations National Institute of Standards and Technology. — Washington: U.S. Department of Commerce, 2019. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

6. NIST SP 800-63-3: Digital Identity Guidelines (Authentication and Lifecycle Management) National Institute of Standards and Technology. Washington: U.S. Department of Commerce, 2017. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

7. ISO/IEC 27001:2022 Information Security Management Systems — Requirements. Geneva : ISO, 2022. URL: https://www.iso.org/standard/27001

8. ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection — Code of Practice for Information Security Controls. Geneva : ISO, 2022. URL: https://www.iso.org/standard/75652.html

9. ANSI INCITS 359-2004 Role Based Access Control (RBAC). — New York: American Standards Institute, 2004. URL:

https://www.techstreet.com/standards/incits-359-2004
10. CIS Benchmarks — Microsoft Windows Server 2022 Level 1 & 2. Center for Internet Security. URL:
https://www.cisecurity.org/benchmarks/
11. CIS Benchmarks — Active Directory. Center for Internet Security. URL:
https://www.cisecurity.org/benchmarks/
12. Active Directory Domain Services Overview & Design. Microsoft Corporation, 2023. URL:
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/ad-ds-design-and-deployment
13. Group Policy Overview and Best Practices. Microsoft Docs. Redmond : Microsoft Corporation, 2023. URL:
https://learn.microsoft.com/en-us/windows-server/administration/group-policy/group-policy-overview
14. Securing Privileged Access in Active Directory. Microsoft Corporation, 2023. URL:
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-privileged-access
15. Local Administrator Password Solution (LAPS) Overview. Microsoft Corporation, 2023. URL:
https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview
16. Windows Server Security Best Practices. Microsoft Corporation, 2023. — URL:
https://learn.microsoft.com/en-us/windows-server/security/security-and-assurance
17. Active Directory Federation Services (AD FS) Technical Reference. Microsoft Corporation, 2023. URL:
https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/overview/ad-fs-overview
18. ESET PROTECT Enterprise / Elite Administrator Guide. ESET. — Bratislava : ESET, 2024. URL:
https://help.eset.com/protect_enterprise/latest/en-US/index.html

19. ESET Full Disk Encryption Deployment and Configuration. ESET. — Bratislava : ESET, 2024. URL: https://help.eset.com/eset_full_disk_encryption/latest/en-US/

20. ESET Secure Authentication Administrator Guide. ESET. — Bratislava : ESET, 2024. — URL: https://help.eset.com/esa/3.1/en-US/index.html

21. ESET Secure Authentication — Active Directory Integration. ESET. — Bratislava: ESET, 2024. URL: https://help.eset.com/esa/latest/en-US/admin_integration_active_directory.html

22. 2024 Data Breach Investigations Report (DBIR). Basking Ridge: Verizon Communications, 2024. URL: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

23. Microsoft Digital Defense Report 2024. Microsoft Security. Microsoft Corporation, 2024. URL: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

24. IBM X-Force Threat Intelligence Index 2025. IBM Security. URL: https://www.ibm.com/reports/threat-intelligence

25. State of Cyber Awareness in Ukraine. Center for Information Protection (CIP). Kyiv : National Security and Defense Council of Ukraine, 2024. URL: https://www.rnbo.gov.ua/en/

26. OWASP Authentication Cheat Sheet. OWASP Foundation. URL: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

27. MITRE ATT&CK Framework — Identity and Access Management Tactics. The MITRE Corporation. URL: https://attack.mitre.org/tactics/enterprise/

28. Zero Trust Model White Paper. Forrester Research, 2020. URL: https://www.forrester.com/report/

29. Enterprise Identity and Access Management Market Trends. Gartner, 2023. URL: https://www.gartner.com/en/documents/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

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

Кваліфікаційна робота
на тему:

«Технологія управління ідентифікацією та доступом користувачів до корпоративних інформаційних ресурсів»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми «Інформаційна та кібернетична безпека»

Виконав: студент групи БСДМ-61: Южаков Данило
Керівник роботи: д-р техн. наук, професор САВЧЕНКО Віталій

КИЇВ - 2025

Об'єкт дослідження – процес формування та впровадження політик інформаційної безпеки в організації середнього масштабу з гібридною моделлю роботи та on-premise доменною інфраструктурою

Предмет дослідження – технологія управління ідентифікацією та доступом на базі Active Directory та комплексу засобів захисту ESET PROTECT Elite з впровадженням багатофакторної автентифікації та рольової моделі доступу.

2

Мета роботи – розробити порядок застосування технології IAM та надати рекомендації щодо її реалізації в корпоративному середовищі на основі принципів Zero Trust, мінімальних привілеїв та безперервного моніторингу.

Наукові завдання:

Проаналізувати сучасні загрози та вразливості IAM-систем у корпоративному середовищі.
Дослідити можливості Active Directory та продуктів ESET для побудови захищеної інфраструктури IAM.
Розробити рольову модель доступу (RBAC) з чітким розподілом привілеїв.
Запроектувати впровадження багатофакторної автентифікації для критичних систем.
Сформувати політики доступу на основі принципів Zero Trust.
Розробити метрики оцінювання ефективності IAM-системи.

Апробація результатів. Результати кваліфікаційної роботи апробовані на Всеукраїнській науково-практичній конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

Основні вразливості та загрози IAM-систем

3

Критичні вразливості в управлінні доступом:

- Компрометація облікових даних через фішинг та соціальну інженерію;
- Надмірні привілеї та накопичення прав доступу при зміні посад;
- Використання спільних облікових записів без персоніфікації;
- Недостатній контроль життєвого циклу облікових записів.

- Помилки конфігурації Active Directory та делегування повноважень
- Ескалація привілеїв (Kerberoasting, Pass-the-Hash, Pass-the-Ticket)
- Застарілі механізми автентифікації(як NTLMv1)
- відсутність MFA
- Відсутність моніторингу та аудиту подій безпеки
- Використання застарілих та вразливих операційних систем та програмного забезпечення.
- Недоліки у налаштуваннях мережевого обладнання, в тому числі відсутність належно налаштованих списків контролю доступу.

Архітектура IAM-рішення на базі Active Directory та ESET

4

Архітектура IAM-рішення на базі Active Directory та ESET

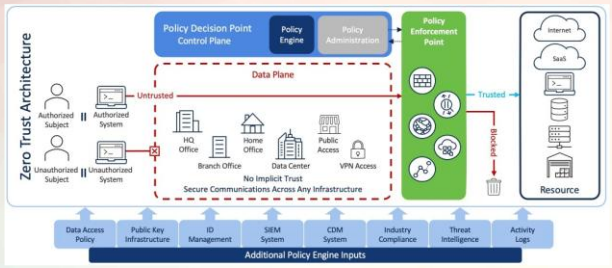
Запропонована архітектура базується на інтеграції кількох ключових компонентів:

Active Directory виступає центральним «джерелом істини» для управління ідентичностями, групами безпеки та реалізації рольової моделі RBAC.

ESET PROTECT Elite забезпечує централізоване управління безпекою кінцевих точок, моніторинг загроз та застосування політик безпеки.

Рольова модель доступу (RBAC)

5



Ресурсні групи (призначаються об'єктам):
• GRP_SHARE_SALES_RO/RW/FULL – доступ до папок продажів
• GRP_APP_CRM_USER/MANAGER – доступ до CRM-системи
• GRP_SHARE_HR_FULL – повний доступ до HR-даних
• GRP_RDP_WIN_SERVERS – RDP-доступ до серверів

Модель дозволяє гнучко управляти правами доступу та мінімізує ручні призначення.

Розроблена рольова модель реалізована в Active Directory з поділом на рольові та ресурсні групи.

Рольові групи:
• GRP_ROLE_SALES_USER – співробітник відділу продажів
•GRP_ROLE_SALES_MANAGER – керівник відділу продажів
• GRP_ROLE_HR_EMPLOYEE – співробітник HR (обов'язкова MFA)
•GRP_ROLE_WIN_SERVER_ADMIN – адміністратор серверів (обов'язкова MFA)

Ключові політики доступу та впровадження Zero Trust

6

Політика 1. Доступ до HR-даних
Доступ до HR-ресурсів тільки для групи GRP_ROLE_HR_EMPLOYEE. Обов'язкова MFA для зовнішнього доступу. Заборона USB-носіїв. Шифрування дисків на робочих станціях.

Політика 3. Запобігання ескалації
Відсутність локальних адмін-прав у звичайних користувачів. Контроль інструментів збору хешів через ESET PROTECT. Обов'язкова MFA для тимчасового підвищення привілеїв.

Політика 2. Адміністрування домену
Адміністративні операції тільки для спеціальних груп. Обов'язкова MFA для VPN, RDP, WinLogon, UAC та веб-консолей.

Політика 4. Журналювання та аудит
Централізований збір подій створення/зміни акаунтів в AD. Фіксація всіх MFA-подій в ESET Secure Authentication. Передача подій безпеки з кінцевих точок у SIEM для кореляції.

ВИСНОВКИ

7

У ході виконання кваліфікаційної роботи було розроблено комплексну технологію управління ідентифікацією та доступом на базі Active Directory та ESET PROTECT Elite. Створено рольову модель доступу (RBAC) з чітким розподілом привілеїв між базовими, функціональними та адміністративними ролями.

Впроваджено систему багатофакторної автентифікації для критичних систем та адміністраторів за допомогою ESET Secure Authentication. Розроблено політики доступу на основі принципів Zero Trust, що включають перевірку кожного запиту, найменші привілеї та безперервний моніторинг. Сформовано метрики оцінювання ефективності IAM-системи.

Запропоноване рішення дозволяє суттєво знизити ризики компрометації облікових даних та ескалації привілеїв, забезпечуючи контрольований та посилено захищений доступ до корпоративних ресурсів в умовах гібридної роботи.


ДУІКТ
ЗГУРТОВАНІ CYBERSECURITY
СТКБ
ЗГУРТОВАНІ CYBERSECURITY
Дякую за увагу!
Доповідь закінчено