ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи на тему:

«РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ ДОСТУПОМ ПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ»

Виконала студентка 4 курсу, групи БСД-43
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Яцкова Н.П.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Яцковій Наталії Петрівні
(прізвище, ім’я, по батькові)

1. Тема бакалаврської роботи: «Розробка рекомендацій щодо управління доступом привілейованих користувачів інформаційної системи організації»
керівник бакалаврської роботи Марченко Віталій Вікторович, ст. викладач
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24» лютого 2023 року № 26.

2. Строк подання студентом бакалаврської роботи 29.05.2023 р.

3. Вихідні дані до бакалаврської роботи
корпоративна інформаційна система;
програмне забезпечення управління привілейованим доступом;
наукова та технічна література, експлуатаційна документація, нормативні документи.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Політики контролю доступу як складова забезпечення інформаційної безпеки в інформаційній системі.
2. Дослідження ринку PAM рішень.
3. Керування привілейованими обліковими записами та їх захист за допомогою PAM рішення CyberArk Privileged Access Management.
4. Розробка рекомендацій щодо ефективного управління доступом привілейованих користувачів

5. Перелік графічного матеріалу

1. Тема бакалаврської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Політики контролю доступу.
4. Дослідження ринку PAM рішень.
5. Архітектура CYBERARK PRIVILEGED ACCESS MANAGEMENT.
6. Керування користувачами.
7. Робота з привілейованими обліковими записами.
8. Рекомендації щодо управління доступом.
9. Висновки за результатами роботи.

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Визначення актуальності проблеми управління доступом привілейованих користувачів як складова частина забезпечення кібербезпеки корпоративної інформаційної системи.	03.03.2023	
2.	Аналіз наукової та технічної літератури з питань теми бакалаврської роботи.	24.03.2023	
3.	Аналіз програмних продуктів, які дозволяють забезпечити управління доступом привілейованих користувачів.	07.04.2023	
4.	Впровадження та налаштування вибраного рішення	28.04.2023	
5.	Розроблення рекомендацій щодо ефективного управління доступом привілейованих користувачів.	12.05.2023	
6.	Оформлення результатів дослідження .	19.05.2023	
7.	Підготовка доповіді до захисту.	26.05.2023	

Студент _____ Яцкова Н.П.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА

на бакалаврську роботу

студентки Яцкової Наталії Петрівни

на тему: «Розробка рекомендацій щодо управління доступом привілейованих користувачів інформаційної системи організації»

Актуальність: З кожним роком зростає кількість кіберзагроз і витоків даних, пов'язаних з привілейованими обліковими записами.

Привілейовані користувачі, такі як адміністратори системи або керівники з високим рівнем доступу, мають значний потенціал для зловживання своїми привілеями. Несанкціонований доступ або недостатній контроль над цими обліковими записами може призвести до серйозних проблем, включаючи втрату конфіденційної інформації, порушення регуляторних вимог, пошкодження репутації компанії та фінансових втрат.

Через це актуальність теми розробки рекомендацій щодо управління доступом привілейованих користувачів інформаційної системи організації наголошується необхідністю захисту конфіденційної інформації та запобігання кіберзагрозам.

Позитивні сторони:

1. При проведенні аналізу було розкрито питання як політики розмежування доступу пов’язані з управлінням доступом привілейованих користувачів.
2. Проведено налаштування контролю та моніторингу привілейованих користувачів у інформаційній системі на основі рішення CyberArk Privileged Access Management.
3. Розроблення рекомендацій щодо ефективного управління доступом привілейованих користувачів.
4. Текст написано зрозуміло, чітко. Висновки послідовно описують суть викладених розділів. Список використаних інформаційних джерел дає зрозуміти, що до написання роботи підходили старанно.

Недоліки:

1. У роботі можна було б розкрити більше практичної складової з налаштування керування користувачами в системі.
2. Було б краще, якби налаштування проводилося б на більш розширеній інформаційній системі.

Висновок: Враховуючи недоліки, бакалаврська робота заслуговує оцінку **відмінно**, а студентка **Яцкова Н.П.** – присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую

Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Яцкова Н.П. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Розробка рекомендацій щодо управління доступом привілейованих користувачів інформаційної системи організації»
Бакалаврська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Яцкова Н.П. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Берестяна Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студентка Яцкова Н.П. обрала тему роботи, метою якої було розробити рекомендації щодо ефективного управління доступом привілейованих користувачів для забезпечення інформаційної безпеки в корпоративній інформаційній системі на основі PAM рішення. Перелік використаних джерел свідчить про вміння студенткою розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Яцкова Н.П. показала добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконувала сумлінно, акуратно та за планом.

Все це дозволяє оцінити виконану бакалаврську роботу студентки Яцкової Наталії Петрівни на оцінку «відмінно» та присвоїти їй кваліфікацію: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студентка Яцкова Н.П.
(прізвище та ініціали)
допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2023 року

РЕФЕРАТ

Текстова частина бакалаврської роботи: 70 сторінок, 26 рисунків, 13 джерел.

Об'єкт дослідження – управління доступом привілейованих користувачів як складова частина забезпечення кібербезпеки корпоративної інформаційної системи.

Предмет дослідження – програмне забезпечення для управління привілейованим доступом CyberArk Privileged Access Management в корпоративній інформаційній системі.

Мета роботи – розробити рекомендації щодо ефективного управління доступом привілейованих користувачів для забезпечення інформаційної безпеки в корпоративній інформаційній системі на основі рішення CyberArk Privileged Access Management.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.

В роботі розкрита основна інформація про політики контролю доступу та їх класи.

Було дане визначення привілейованим користувачам та їх роль в корпоративній системі.

Проаналізовано ринок PAM рішень.

Досліджено основні можливості програмного продукту CyberArk Privileged Access Management.

На основі досліджень, що були проведені в даній роботі, були створені рекомендації щодо безпечного керування привілейованими обліковими записами.

Галузь використання – кібербезпека корпоративних інформаційних систем.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КЕРУВАННЯ ПРИВІЛЕЙОВАНИМИ ОБЛІКОВИМИ ЗАПИСАМИ, ПРИВІЛЕЙОВАНИЙ ДОСТУП, ПОЛІТИКА КОНТРОЛЮ ДОСТУПУ, МОДЕЛЬ КОНТРОЛЮ ДОСТУПУ, ПРИВІЛЕЙОВАНИЙ КОРИСТУВАЧ

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

PAM (Privileged Account Management) - керування привілейованими обліковими записами

IT – інформаційні технології

КІС – корпоративна інформаційна система

DAC (Discretionary Access Control) – дискреційне керування доступом

MAC (Mandatory Access Control) – мандатне керування доступом

RBAC (Role-based access control) – керування доступом на основі ролей

HRU model (Harrison, Ruzzo, Ullman model) – модель Харрісона, Руззо, Ульмана

TAM (Typed Access Matrix) - типізована матриця доступу

БД – база даних

MFA (Multi-Factor Authentication) – багатофакторна аутентифікація

SSO (Single sign-on) – Технологія єдиного входу

SSH (Secure Shell) – мережевий протокол для віддаленого управління комп’ютером

AD (Active Directory) – служба директорій

VPN (Virtual Private Network) – віртуальна приватна мережа

PCI-DSS (Payment Card Industry Data Security Standard) – стандарт безпеки даних індустрії платіжних карт

API (Application Programming Interface) – прикладний програмний інтерфейс

ВСТУП

Актуальність дослідження. Керування привілейованими обліковими записами (Privileged Account Management, PAM) – це набір рішень, які полегшують реалізацію моніторингу і контролю облікових записів, а також проведені аудиторські дії.

Основне призначення таких методів і засобів – запобігання витоку конфіденційної інформації, запобігання збоїв у роботі інформаційної системи, що були викликані діями користувачів привілейованого облікового запису.

Облікові записи з більш широкими можливостями та доступом можуть стати джерелом витоку даних або ціллю атаки зловмисника. Крім того, не виключено, що його скомпрометує сам власник.

Основні принципи керування привілейованими користувачами включають керівництво компанії, працівники, які забезпечують роботу IT-інфраструктури, персонал, який здійснює контроль і аудит.

Щоб правильно організувати контроль привілейованих користувачів, необхідно вибрати рішення, яке може контролювати поведінку таких облікових записів. Рішення повинно не тільки відстежувати дії користувачів, а й надавати інформацію про те, хто працював під обліковим записом в конкретний час.

Елементи керування привілейованим доступом до облікового запису слід зберігати окремо від звичайних даних співробітників.

Через це дана тема бакалаврської роботи про впровадження систем привілейованих користувачів є актуальною.

Об'єкт дослідження. Управління доступом привілейованих користувачів як складова частина забезпечення кібербезпеки корпоративної інформаційної системи.

Предмет дослідження. Програмне забезпечення для управління привілейованим доступом CyberArk Privileged Access Management в корпоративній інформаційній системі.

Мета роботи. Розробити рекомендації щодо ефективного управління доступом привілейованих користувачів для забезпечення інформаційної безпеки в корпоративній інформаційній системі на основі рішення CyberArk Privileged Access Management.

Завдання бакалаврської роботи:

- Дослідження такої сутності як політика контролю доступу
- Проаналізувати місце та роль користувачів з привілейованими обліковими записами у корпоративній системі
- Проаналізувати ринок PAM рішень та обрати оптимальне рішення
- Визначити та проаналізувати основні можливості програмного продукту CyberArk Privileged Access Management

Методи дослідження. Опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.

Практичне значення одержаних результатів. Розробка рекомендацій щодо ефективного впровадження та експлуатації комплексу керування привілейованими обліковими записами в інформаційній системі організації.

1 ПОЛІТИКИ КОНТРОЛЮ ДОСТУПУ ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

1.1 Визначення політики контролю доступу. Концепції розробки, механізми захисту, основні класи

Важливою вимогою будь-якої системи управління інформацією є захист даних і ресурсів від несанкціонованого розголошення (секретність) і несанкціонованих або неналежних модифікацій (цілісність), водночас забезпечуючи їхню доступність для законних користувачів (відсутність відмов у наданні послуг). Таким чином, забезпечення захисту вимагає, щоб кожен доступ до системи та її ресурсів контролювався, і щоб всі і тільки авторизовані доступи могли мати місце. Цей процес називається контролем доступу. Розробка системи контролю доступу вимагає визначення правил, згідно з якими доступ повинен контролюватися, і їх реалізації у вигляді функцій, що виконуються комп'ютерною системою. Процес розробки зазвичай здійснюється за допомогою багатоетапного підходу, що базується на наступних концепціях [1]:

- Політика безпеки: визначає правила (високого рівня), згідно з якими має регулюватися контроль доступу.
- Модель безпеки: забезпечує формальне представлення політики безпеки контролю доступу та її роботи. Формалізація дозволяє довести властивості безпеки, які забезпечує система контролю доступу, що проектується.
- Механізм безпеки: визначає низькорівневі (програмні та апаратні) функції, які реалізують контроль, накладений політикою і формально зазначений у моделі.

Ці концепції відповідають концептуальному розділенню між різними рівнями абстракції проекту і забезпечують традиційні переваги багатоетапної розробки програмного забезпечення. Зокрема, поділ між політиками і механізмами забезпечує незалежність між вимогами до захисту, які необхідно виконувати, з

одного боку, і механізмами, які їх забезпечують, з іншого. Таким чином, стає можливим:

- обговорювати вимоги захисту незалежно від їх виконання та реалізації;
- порівнювати різні політики контролю доступу, а також різні механізми, що реалізують ту саму політику;
- розробляти механізми здатні забезпечити виконання декількох політик.

Останній аспект є особливо важливим: якщо механізм прив'язаний до конкретної політики, зміна політики вимагатиме зміни всієї системи контролю доступу; механізми, здатні застосовувати кілька політик, уникають цього недоліку. Етап формалізації між визначенням політики та її реалізацією у вигляді механізму дозволяє визначити формальну модель, що представляє політику та її роботу, що дає можливість визначити і довести властивості безпеки, які матимуть системи, що застосовують цю модель. Таким чином, якщо довести, що модель є "безпечною" і що механізм правильно реалізує модель, ми можемо стверджувати, що система є "безпечною" (в рамках розглянутого визначення безпеки). Реалізація коректного механізму далеко не тривіальна і ускладняється необхідністю впоратися з можливими слабкими місцями безпеки, зумовленими самою реалізацією, а також складністю відображення примітивів контролю доступу на комп'ютерну систему. Механізм контролю доступу повинен працювати як еталонний монітор, тобто довірений компонент, що перехоплює кожен запит до системи. Він також повинен володіти наступними властивостями:

- захищений від несанкціонованого доступу: не повинно бути можливості змінити його (або, принаймні, не повинно бути можливості, щоб зміни залишилися непоміченими);
- не можна обійти: він має бути посередником у всіх доступах до системи та її ресурсів;
- ядро безпеки: воно повинно бути обмежене певною частиною системи (розпорошення функцій безпеки по всій системі означає, що весь код повинен бути перевірений);

- невеликий: він повинен мати обмежений розмір, щоб піддаватися суворим методам перевірки.

Визначення політик контролю доступу є далеко не тривіальним процесом. Одна з головних труднощів полягає в інтерпретації, часто складної та іноді неоднозначної політики безпеки в реальному світі і в їх перекладі в чітко визначені і однозначні правила, які можуть бути застосовані комп'ютерною системою. Багато реальних ситуацій мають складні політики, де рішення про доступ залежать від застосування різних правил, що випливають, наприклад, із законів, практик та організаційних положень. Політика безпеки повинна охоплювати всі різні правила, що підлягають застосуванню, і, крім того, повинна також враховувати можливі додаткові загрози, пов'язані з використанням комп'ютерної системи. Політики контролю доступу можна згрупувати в три основні класи:

- Дискреційні (DAC) (засновані на авторизації) політики контролюють доступ на основі особи запитувача і правил доступу, які визначають, що запитувачі можуть (або не можуть) робити та що їм дозволено (або заборонено) робити.
- Мандатні (MAC) політики контролюють доступ на основі обов'язкових правил, визначених центром управління.
- Політики на основі ролей (RBAC) контролюють доступ в залежності від ролей, які користувачі мають в системі, а також від правил, що визначають, який доступ дозволено користувачам з певними ролями.

Дискреційні та рольові політики зазвичай поєднуються з (або включають) адміністративною політикою, яка визначає, хто може визначати дозволи/правила, що регулюють контроль доступу.

У цьому розділі буде проілюстровано різні політики та моделі контролю доступу, які запропоновані в літературі, а також проведене дослідження їх низькорівневої реалізації з точки зору механізмів безпеки.

1.2 Дискреційні політики

Дискреційні політики забезпечують контроль доступу на основі особистих даних запитувачів і чітких правил доступу, які встановлюють, хто може, а хто не може виконувати які дії над якими ресурсами. Вони називаються дискреційними, оскільки користувачам може бути надана можливість передавати свої привілеї іншим користувачам, де надання та відкликання привілеїв регулюється адміністративною політикою. Тут буде розповідатися про ранні дискреційні моделі, щоб передати основні ідеї специфікацій прав доступу та їх застосування. Щоб повернутися до дискреційних політик, потрібно розглянути обов'язковий контроль. Розпочати потрібно з обговорення "примітивних" дискреційних політик на основі моделі матриці доступу.

1.2.1 Модель матриці доступу

Модель матриці доступу забезпечує основу для опису дискреційного контролю доступу. Оригінальна модель називається матрицею доступу, оскільки стан авторизації, що існує в системі в даний момент часу, представлено у вигляді матриці. Таким чином, матриця дає абстрактне представлення систем захисту. Хоча ця модель може здатися примітивною, оскільки згодом були досліджені більш багаті політики, її використання є корисним для ілюстрації деяких аспектів, які слід враховувати при формалізації системи контролю доступу.

Першим кроком у розробці системи контролю доступу є ідентифікація об'єктів, що підлягають захисту суб'єктів, які виконують дії та запитують доступ до об'єктів, а також дій, які можуть бути виконані над об'єктами, і які необхідно контролювати. Суб'єкти, об'єкти і дії можуть відрізнятися в різних системах або контекстах застосування. Наприклад, у захисті операційних систем об'єктами зазвичай є файли, каталоги або програми; у системах баз даних об'єктами зазвичай є файли, каталоги або програми; у системах баз даних об'єктами можуть бути відношення, представлення, збережені процедури тощо. Цікаво відзначити, що суб'єкти можуть самі бути об'єктами (це стосується, наприклад, виконуваного коду та збережених процедур). Суб'єкт може створювати додаткові суб'єкти (наприклад, дочірні процеси) для виконання свого завдання. Суб'єкт-творець отримує привілеї

керування над створеними процесами (наприклад, можливість призупиняти або завершувати свої дочірні процеси).

У моделі матриці доступу стан системи визначається трійкою (S, O, A), де S - множина суб'єктів, які можуть реалізовувати привілеї; O - множина об'єктів, на яких можуть бути реалізовані привілеї (суб'єкти можуть розглядатися як об'єкти, у цьому випадку $S \subseteq O$); і A - матриця доступу, де рядки відповідають суб'єктам, стовпці - об'єктам, а запис A[s, o] повідомляє про привілеї s на o. Тип об'єктів та дії, що виконуються над ними залежать від системи. Просто надаючи фреймворк, в якому можна вказати повноваження модель може враховувати різні привілеї. Наприклад, на додаток до традиційних дій читання, запису та виконання, право власності (тобто, власність об'єктів суб'єктами) та контроль (для моделювання батьківсько-дочірніх відносин між процесами). На рис. 1 показано приклад матриці доступу [1].

	File 1	File 2	File 3	Program 1
Ann	own read write	read write		execute
Bob	read		read write	
Carl		read		execute read

Рис. 1.1. Приклад матриці доступу

Зміна стану системи здійснюється за допомогою команд, які можуть виконувати примітивні операції над станом авторизації залежно від деяких умов. Формалізація HRU визначила шість примітивних операцій, які описують зміни стану системи. Ці операції, вплив яких на стан авторизації проілюстровано на рис. 1.2, відповідають додаванню та видаленню суб'єкта, а також додаванню та видаленню привілеїв.

OPERATION (op)	CONDITIONS	NEW STATE ($Q \vdash_{op} Q'$)
enter r into $A[s,o]$	$s \in S$ $o \in O$	$S' = S$ $O' = O$ $A'[s,o] = A[s,o] \cup \{r\}$ $A'[s_i,o_j] = A[s_i,o_j] \quad \forall (s_i,o_j) \neq (s,o)$
delete r from $A[s,o]$	$s \in S$ $o \in O$	$S' = S$ $O' = O$ $A'[s,o] = A[s,o] \setminus \{r\}$ $A'[s_i,o_j] = A[s_i,o_j] \quad \forall (s_i,o_j) \neq (s,o)$
create subject s'	$s' \notin S$	$S' = S \cup \{s'\}$ $O' = O \cup \{s'\}$ $A'[s,o] = A[s,o] \quad \forall s \in S, o \in O$ $A'[s',o] = \emptyset \quad \forall o \in O'$ $A'[s,s'] = \emptyset \quad \forall s \in S'$
create object o'	$o' \notin O$	$S' = S$ $O' = O \cup \{o'\}$ $A'[s,o] = A[s,o] \quad \forall s \in S, o \in O$ $A'[s,o'] = \emptyset \quad \forall s \in S'$
destroy subject s'	$s' \in S$	$S' = S \setminus \{s'\}$ $O' = O \setminus \{s'\}$ $A'[s,o] = A[s,o] \quad \forall s \in S', o \in O'$
destroy object o'	$o' \in O$ $o' \notin S$	$S' = S$ $O' = O \setminus \{o'\}$ $A'[s,o] = A[s,o] \quad \forall s \in S', o \in O'$

Рис. 1.2. Примітивні операції моделі HRU

Кожна команда складається з умовної частини та тіла і має вигляд [1]

command $c(x_1, \ldots, x_k)$

if r_1 in $A[x_{s1}, x_{o1}]$ and

r_2 in $A[x_{s2}, x_{o2}]$ and

.

.

r_m in $A[x_{sm}, x_{om}]$ and

then op_1

op_2

.

.

op_n

end.

де n > 0, m ≥ 0. Тут r_1, ..., r_m - дії, op_1, ..., op_n - примітивні операції, а s_1, ..., s_m та o_1, ..., o_m - цілі числа від 1 до k. Якщо m=0, команда не має умовної частини.

Наприклад, наступна команда створює файл і надає суб'єкту, що його створив, привілеї на володіння цим файлом [1].

command CREATE(creator,file)

create object file

enter Own into A[creator,file] end.

Наступні команди дозволяють власнику надавати або відкликати привілеї для інших користувачів на виконання дій над їх файлами.

command CONFER_a(owner,friend,file)

if Own in A[owner,file]

then enter a into A[friend,file] end.

command REVOKE_a (owner,ex-friend,file)

if Own in A[owner,file]

then delete a from A[ex-friend,file] end.

Зауважте, що тут a - це не параметр, а абревіатура для визначення багатьох подібних команд, по одній для кожного значення, якого може набувати a (наприклад, $\mathrm{CONFER}_{\mathrm{read}}$, $\mathrm{REVOKE}_{\mathrm{write}}$). Оскільки команди не є параметричними діями w.r.t., для кожної дії, яку можна надати/відкликати, потрібно вказати окрему команду.

Нехай $Q \vdash_{op} Q'$ позначає виконання операції op над станом Q, що призводить до стану Q'. Виконання команди c($a_1, \ldots, a_k$) на стані системи Q =(S, O, A) викликає перехід зі стану Q у стан Q' такий, що $\exists$ Q_1,..., Q_n, для якого $Q \vdash_{op_1^*} Q_1 \vdash_{op_2^*} \ldots \vdash_{op_n^*} Q_n = Q'$, де $op_1^* \ldots op_n^*$ - примітивні операції $op_1 \ldots op_n$ у тілі (операторній частині) команди c, в яких кожному формальному параметру x_i підставляються фактичні параметри a_i, i:= 1, ..., k. Якщо умовна частина команди не перевіряється, то команда не має ніякого ефекту і Q = Q' [1].

Хоча модель HRU не містить вбудованих адміністративних політик, можливість визначення команд дозволяє їх формулювати. Адміністративні повноваження можна визначити, прикріпивши прапорці до привілеїв доступу. Наприклад, прапорець копіювання, позначений $*$, прикріплений до привілею, може

вказувати на те, що привілей може бути переданий іншим особам. Надання привілеїв можна виконати за допомогою команд, подібних до наведеної нижче (знову ж таки, тут $\mathrm{TRANSFER_a}$ - це абревіатура, що позначає стільки команд, скільки існує дій).

command $\mathrm{TRANSFER_a}$ (subj,friend,file)

if a^* in A[subj,file]

then enter a into A[friend,file] end.

Можливість визначення команд цього типу, безумовно, забезпечує гнучкість, оскільки можна врахувати різні адміністративні політики, визначивши відповідні команди. Наприклад, може підтримуватися альтернативний адміністративний прапорець (який називається transfer only і позначається +), який надає суб'єкту можливість передавати привілеї іншим, але при цьому суб'єкт втрачає привілей. Така гнучкість створює цікаву проблему, яка називається безпекою, і пов'язану з поширенням привілеїв серед суб'єктів системи. Інтуїтивно зрозуміло, що для системи з початковою конфігурацією Q проблема безпеки полягає у визначенні того, чи може даний суб'єкт s коли-небудь отримати заданий доступ a до об'єкта o, тобто чи існує послідовність запитів які виконані на Q можуть призвести до стану Q', у якому a з'являється у комірці A[s, o] яка не мала її у Q. (Потрібно зауважити, що, не всі витоки привілеїв є поганими, і суб'єкти можуть навмисно передавати свої привілеї "надійним" суб'єктам. Тому надійні суб'єкти ігноруються в аналізі). Виходить що проблема безпеки взагалі нерозв'язна (її можна звести до проблеми зупинки машини Тюрінга). Натомість вона залишається розв'язною для випадків, коли суб'єкти та об'єкти скінченні, та в монооперацийних системах, тобто системах, де тіло команд може мати не більше однієї операції (в той час як умовна частина все ще може бути як завгодно складною). Однак, монооперацийні системи мають обмеження, яке робить створення операції практично марними: одна команда create не може зробити більше, ніж додати порожнього рядка/стовпчика (вона не може нічого туди записати). Тому неможливо підтримувати відносини власності або контролю між суб'єктами. Прогрес в аналізі безпеки був досягнутий у пізнішому розширенні моделі HRU Сандху, який запропонував модель TAM (Typed Access

Matrix). TAM розширює HRU за рахунок сильнішої типізації: кожен суб'єкт і об'єкт має тип; тип асоціюється з суб'єктами/об'єктами при їх створенні і після цього не змінюється. Результати безпеки обчислюються за поліноміальний час для випадків, коли система є монотонною (привілеї не можуть бути видалені), команди обмежені трьома параметрами, і немає циклічних створень. В іншому випадку безпека залишається нерозв'язною.

1.3 Мандатні політики

Мандатні (обов'язкові) політики безпеки забезпечують контроль доступу на основі правил санкціонованих центрів управління. Найпоширенішою формою мандатних політик є багаторівнева політика безпеки, що базується на класифікації суб'єктів та об'єктів у системі. Об'єкти - це пасивні сутності, що зберігають інформацію. Суб'єкти це активні сутності, які запитують доступ до об'єктів. Варто зауважити, що існує різниця між суб'єктами обов'язкової політики та суб'єктами авторизації які розглядаються в дискреційних політиках. У той час як суб'єкти авторизації зазвичай відповідають користувачам (або їхнім групам), обов'язкові політики розрізняють між користувачами та суб'єктами. Користувачі - це люди, які мають доступ до системи, тоді як суб'єкти - це процеси (тобто програми, що виконуються), які діють від імені користувачів. Це розрізнення дозволяє політиці контролювати непрямий доступ (витоки або модифікації), спричинені виконанням процесів. В свою чергу, мандатні політики поділяються на: політики що базуються на секретності, модель Белла-ЛаПадули, модель Біби.

1.3.1 Мандатна політика, що базується на секретності

Політика обов'язкової секретності контролює прямі та непрямі потоки інформації з метою запобігання її витоку до несанкціонованих суб'єктів. Рівень безпеки класу доступу, пов'язаного з об'єктом, відображає чутливість інформації, що міститься в об'єкті, тобто потенційну шкоду, яка може бути завдана в результаті несанкціонованого розголошення інформації. Рівень безпеки класу доступу,

пов'язаного з користувачем, який також називається допуском, відображає надійність користувача не розголошувати конфіденційну інформацію користувачам, які не мають дозволу на її перегляд. Категорії визначають сферу компетенції користувачів та даних і використовуються для забезпечення більш детальної класифікації безпеки суб'єктів та об'єктів, ніж класифікації, що надаються лише за рівнями безпеки. Вони є основою для запровадження обмежень на основі принципу службової необхідності (тобто, обмеження доступу суб'єктів до інформації, яку їм дійсно потрібно знати для виконання своєї роботи).

Користувачі можуть підключатися до системи з будь-яким класом доступу, який домінує в їхньому допуску. Користувач, який підключається до системи з певним класом доступу, створює тему у цьому класі доступу. Наприклад, відповідно до решітки на рис. 3, користувач що має дозвіл (TS,{Nuclear}) може підключатися до системи як (S,{Nuclear}), (TS,∅), або (TS,∅) суб'єктом [1].

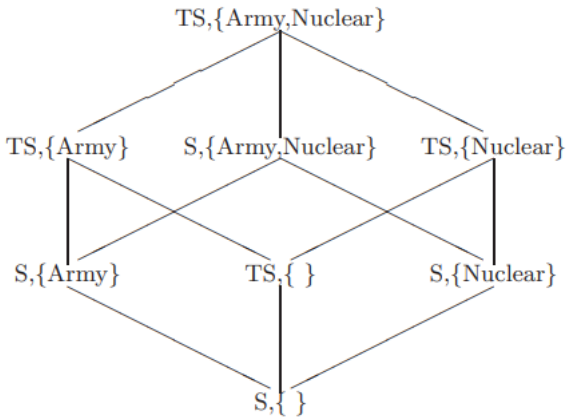


Рис. 1.3. Приклад захисної решітки

Запити суб'єкта на доступ до об'єкта контролюються відносно класу доступу суб'єкта та об'єкта і задовольняються тільки якщо виконується деяке відношення, що залежить від запитуваного доступу. Зокрема, два принципи, вперше сформульовані Беллом і ЛаПадулою, повинні бути виконані для того, щоб захистити конфіденційність інформації:

No-read-up. Суб'єкту дозволено доступ на читання до об'єкта лише у тому випадку, якщо клас доступу суб'єкта домінує над класом доступу об'єкта.

No-write-down. Суб'єкту дозволено доступ на запис до об'єкту тільки у тому випадку, якщо клас доступу суб'єкта клас домінує над класом доступу об'єкта.

Дотримання цих двох принципів запобігає перетіканню інформації від суб'єктів/об'єктів високого рівня до суб'єктів/об'єктів нижчого рівня, тим самим забезпечуючи виконання вимог захисту (тобто, жоден процес не зможе зробити конфіденційну інформацію доступною користувачам, які не мають до неї доступу). Це проілюстровано на рис. 1.4, де чотири класи доступу складаються лише з рівня безпеки (TS, S, C та U). Необхідно звернути увагу на важливість контролю операцій читання і запису, оскільки обидві операції можуть бути використані неналежним чином для витоку інформації.

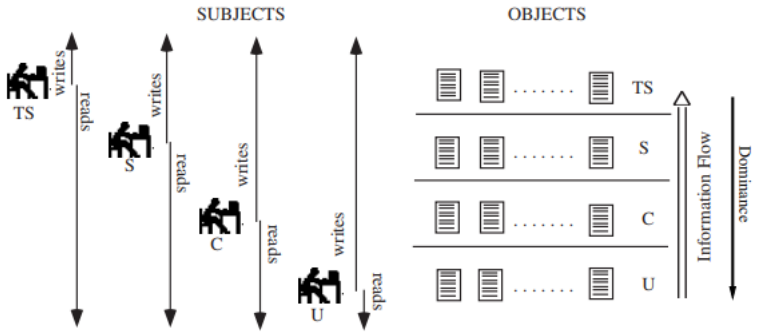


Рис. 1.4. Інформаційний потік для забезпечення секретності

Хоча користувачі можуть підключатися до системи на будь-якому рівні, нижчому за їхній допуск, суворе застосування принципів "не читати" і "не записувати" може виявитися занадто жорстким. Реальні ситуації часто вимагають винятків з обов'язкових обмежень. Наприклад, може виникнути потреба в зниженні статусу даних (наприклад, дані, що підпадають під ембарго, які можуть бути зняті через деякий час). Крім того, інформація, оприлюднена може бути менш чутливою, ніж інформація, яку процес зчитував. Наприклад, процедура може отримати доступ до особистої інформації про працівників організації та повернути пільги, які мають бути надані кожному працівникові. Хоча особиста інформація може вважатися секретною, вигоди можуть вважатися конфіденційними. Щоб реагувати на такі ситуації, багаторівневі системи повинні передбачати винятки, послаблення або відмову від обмежень у контрольований спосіб для процесів, яким довіряють, і

забезпечити санітарну обробку інформації (це означає, що чутливість вихідної інформації втрачається).

Варто зауважити, що політики DAC та MAC не є взаємовиключними, а можуть застосовуватися спільно. У цьому випадку для надання доступу до інформації необхідні: наявність необхідного для цього дозволу, та дотримання обов'язкової політики. Інтуїтивно зрозуміло, що дискреційна політика діє в межах обов'язкової політики: вона може обмежити лише набір доступів, які були б дозволені лише за допомогою MAC.

1.3.2 Модель Белла-ЛаПадули

Тут буде проілюстровано деякі концепції формалізації моделі, щоб дати уявлення про різні аспекти, які необхідно враховувати при визначенні моделі безпеки. Спочатку потрібно зазначити, що були запропоновані різні версії моделі (через формалізацію нових властивостей, або пов'язаних з конкретними середовищами застосування), проте основні принципи залишаються незмінними. Крім того, тут буде розглянуто лише аспекти формалізації, необхідні для ілюстрації концепцій, які хочемо донести: задля простоти формулювання моделі спрощено, а деякі аспекти опускаються.

У моделі Белла та ЛаПадули система складається з множини суб'єктів S, об'єктів O та дій A, які включають read та write. Модель також передбачає наявність решітки L класів доступу та функції $\lambda : S \cup O \rightarrow L$, яка, будучи застосованою до суб'єкта (об'єкта, відповідно) у певному стані, повертає класифікацію суб'єкта (об'єкта) у цьому стані. Стан $v \in V$ визначається як трійка (b, M, λ), де $b \in \wp(S \times O \times A)$ - множина поточних доступів (s, o, a), M - матриця доступу, що виражає дискреційні дозволи (як у моделі HRU), а λ - зв'язок класів доступу з суб'єктами та об'єктами. Система складається з початкового стану v_0, множини запитів R та функції переходу стану $T : V \times R \rightarrow V$, яка перетворює стан системи в інший стан в результаті виконання запиту. Інтуїтивно зрозуміло, що запити охоплюють отримання та звільнення доступу, надання та відкликання повноважень, а також зміну рівнів. Далі модель визначає набір аксіом, що описують властивості, яким

повинна задовольняти система і які виражають обмеження, що накладаються обов'язковою політикою. Перша версія моделі Белла і ЛаПадули визначала такі критерії [1]:

- simple property (проста властивість). Стан v задовольняє просту властивість безпеки, якщо для кожного s ∈ S, o ∈ O: (s, o, read) ∈ b ⇒ λ(s) ≥ λ(o).
- *-property. Стан v задовольняє властивості *-безпеки, якщо для кожного s ∈ S, o ∈ O: (s, o, write) ∈ b ⇒ λ(o) ≥ λ(s).

Дві аксіоми, наведені вище, відповідають принципам заборони зчитування і заборони запису, які були розглянуті у Частині 1.3.1. Стан називається безпечним якщо він задовольняє як просту властивість безпеки, так і *-властивість. Система (v_0, R, T) є безпечною тоді, коли кожен стан, який досягається з v_0 шляхом виконання однієї або більше скінченних послідовностей запитів з R, є безпечним.

У першому формулюванні своєї моделі Белл і ЛаПадула наводять базову Теорему Безпеки (BST), яка стверджує, що система є безпечною, якщо її початковий стан v_0 є безпечним, і перехід з одного стану в інший T зберігає безпеку, тобто переводить безпечний стан в інший безпечний стан.

Проблема зміни рівня безпеки суб'єктів та об'єктів була зафіксована формально у Белла і ЛаПадули не як аксіома, а як неформальне керівництво з проектування, яке називається принципом спокою. Принцип спокою стверджує, що класифікація активних об'єктів не повинна змінюватися під час нормальної експлуатації. У наступному перегляді моделі було введено відмінність між рівнем, призначеним об'єкту (допуском), і його поточним рівнем (який може бути будь-яким, де домінує його допуск), що також передбачало зміну формулювання аксіом, що дозволило зробити контроль більш гнучким.

Ще однією властивістю, включеною в модель Белла і ЛаПадули, є властивість дискретності, яка обмежує множину поточних доступів b підмножиною матриці доступу M. Інтуїтивно зрозуміло, що це забезпечує дискреційний контроль.

1.3.3 Модель Біби

Мандатна політика, яка була висвітлена вище, захищає лише конфіденційність інформації; контроль за її цілісністю не здійснюється. Суб'єкти з низьким рівнем доступу все одно можуть здійснювати неналежні непрямі модифікації об'єктів, які вони не можуть записати. Відштовхуючись від принципів моделі Белла і ЛаПадули, Біба запропонував подвійну політику захисту цілісності, яка контролює потік інформації і не дозволяє суб'єктам опосередковано модифікувати інформацію, яку вони не можуть писати. Як і у випадку з секретністю, кожному суб'єкту та об'єкту в системі присвоюється класифікація цілісності. Класифікації та відносини домінування між ними визначаються, як і раніше. Прикладом рівнів цілісності можуть бути: Критична (C), Важлива (I) та Невідома (U). Семантика класифікацій цілісності полягає в наступному. Рівень цілісності, пов'язаний з користувачем, відображає надійність користувача при додаванні, зміні або видаленні інформації. Рівень цілісності, пов'язаний з об'єктом, відображає як ступінь довіри до інформації, що зберігається в об'єкті, так і потенційну шкоду, яка може виникнути в результаті несанкціонованої модифікації інформації. Знову ж таки, категорії визначають сферу компетенції користувачів і даних. Контроль доступу здійснюється відповідно до наступних двох принципів:

- No-read-down. Суб'єкту дозволено доступ на читання до об'єкту тільки у тому випадку, якщо клас доступу об'єкту домінує над класом доступу суб'єкта.
- No-write-up. Суб'єкту дозволено доступ на запис до об'єкту тільки у тому випадку, якщо клас доступу суб'єкта домінує над класом доступу об'єкта.

Дотримання цих принципів забезпечує цілісність, запобігаючи перетіканню інформації, що зберігається в об'єктах нижчого рівня (а отже, менш надійних), до об'єктів вищого рівня або непорівнянних з ними. Це проілюстровано на рис. 1.4, де в якості прикладу взято класи, що складаються лише з рівнів цілісності (C, I та U).

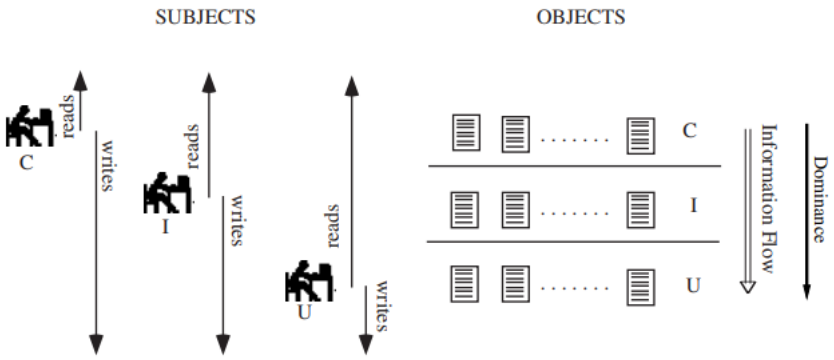


Рис. 1.5. Інформаційний потік для цілісності

Два принципи, наведені вище, є дублюванням двох принципів, сформульованих в моделі Белла і ЛаПадула. Пропозиція Біби також досліджувала альтернативні критерії для забезпечення цілісності, що дозволяє більш динамічний контроль. Вони включали в себе наступні дві політики [1].

Нижня оцінка для суб’єктів. Обмежує операції запису за принципом принципом no-write-up. На операції читання не накладається жодних обмежень. Однак, суб'єкт s, який читає об'єкт o, знижує свою класифікацію до найбільшої нижньої межі класифікації обох об'єктів, тобто $\lambda'(s) = glb(\lambda(s), \lambda(o))$.

Нижня межа для об'єктів. Обмежує операції читання за принципом принципом no-read-down. На операції запису не накладається жодних обмежень. Однак, якщо суб'єкт s записує об'єкт o, то класифікація об'єкта знижується до найбільшої нижньої межі класифікації обох об'єктів, тобто $\lambda'(o) = glb(\lambda(s), \lambda(o))$.

Інтуїтивно зрозуміло, що ці дві політики намагаються застосувати більш динамічну поведінку для дотримання обмежень. Однак обидва підходи мають певні недоліки. У підході "нижньої оцінки для суб'єктів" здатність суб'єкта виконати процедуру може залежати від того, в якому порядку запитуються операції: суб'єкту може бути відмовлено у виконанні процедури через операції читання виконані раніше. Останню політику насправді не можна вважати захистом цілісності: враховуючи що суб'єктам дозволено записувати вище свого рівня; при порушенні цілісності можуть виникнути компроміси; знижуючи рівень об'єкту, політика просто сигналізує про цей факт.

Як видно з рис. 1.4 і 1.5, політики секретності дозволяють потік інформації тільки від нижчого до вищого класу (секретності), в той час як політики цілісності дозволяють потік інформації лише з вищого класу до нижчого (цілісність). Якщо потрібно контролювати і секретність, і цілісність, об'єктам і суб'єктам слід призначити два класи доступу: один - для секретності, інший - для цілісності.

Основним обмеженням політики, запропонованої Бібою, є те, що вона охоплює лише порушення цілісності, спричинені неналежними інформаційними потоками. Однак, цілісність є набагато ширшим поняттям, і слід брати до уваги додаткові аспекти.

1.4 Політики контролю доступу на основі ролей

Контроль доступу на основі ролей (RBAC) є альтернативою традиційним дискреційним (DAC) та мандатним контролю доступу (MAC), яка привертає все більшу увагу, особливо для комерційних застосунків. Основна мотивація RBAC - це необхідність визначати та впроваджувати специфічні для підприємства політики безпеки таким чином, щоб вони природно відповідали структурі організації. Насправді у великій кількості видів бізнес-діяльності особистість користувача має значення лише з точки зору підзвітності. Для цілей контролю доступу набагато важливіше знати, якими є організаційні обов'язки користувача, а не хто є користувачем. Звичайний дискреційний контроль доступу, в якому індивідуальна власність користувача на дані відіграє таку важливу роль, не дуже добре підходять. Так само, як і повний обов'язковий контроль доступу, в якому користувачі мають допуск до інформації, а об'єкти мають класифікацію безпеки. Контроль доступу на основі ролей намагається заповнити цю прогалину, поєднуючи гнучкість явних дозволів з додатково накладеними організаційними обмеженнями.

1.4.1 Політики на основі ролей

Рольові політики регулюють доступ користувачів до інформації на основі організаційної діяльності та відповідальності, яку користувачі мають у системі.

Незважаючи на те, що були зроблені різні пропозиції, основні концепції є спільними для всіх підходів. По суті, рольова політика вимагає визначення ролей у системі, де роль можна визначити як набір дій та обов'язків, пов'язаних з конкретною робочою діяльністю. Роль може мати широку сферу застосування, відображаючи назву посади користувача (наприклад, секретар), або вона може бути більш конкретною, відображаючи, наприклад, завдання, яке користувач повинен виконувати (наприклад, обробка замовлень). Тоді, замість того, щоб вказувати всі права доступу, вказуються права доступу до об'єктів для ролей. Потім користувачам надаються повноваження на прийняття ролей (див. рис. 1.6) [1].

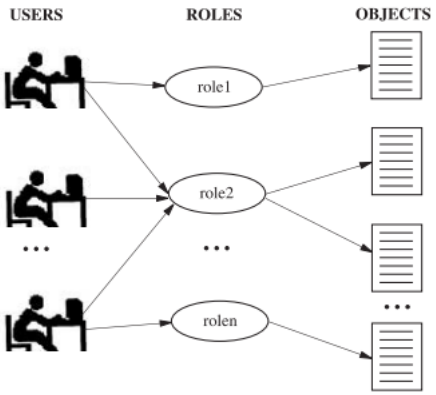


Рис. 1.6. Контроль доступу на основі ролей

Користувачеві, який грає роль, дозволено виконувати всі дії, які дозволено для цієї ролі. Загалом, користувач може виконувати різні ролі в різних випадках. Також одну й ту саму роль можуть виконувати кілька користувачів, навіть одночасно. Деякі пропозиції щодо контролю доступу на основі ролей дозволяють користувачеві виконувати декілька ролей одночасно. Інші пропозиції обмежують користувача лише однією роллю за раз, або визнають, що деякі ролі можуть виконуватися спільно, тоді як інші повинні бути прийняті у виключенні одна одної. Важливо відзначити різницю між групами і ролями: групи визначають набори користувачів тоді як ролі визначають набори привілеїв. Між ними існує семантична різниця: ролі можуть бути "активовані" і "деактивовані" користувачами на власний розсуд, тоді як членство в групі застосовується завжди, тобто користувачі не можуть вмикати і вимикати членство в групах (і відповідні повноваження) за

власним бажанням. Однак, оскільки можна визначити ролі, які відповідають організаційним фігурам (наприклад, секретар, завідувач кафедри, викладач), один і той самий "концепт" можна розглядати і як групу, і як роль.

Рольовий підхід має кілька переваг. Деякі з них ми розглянемо нижче.

Керування повноваженнями. Політики на основі ролей отримують вигоду від логічної незалежності у визначенні повноважень користувачів, розбиваючи цю задачу на дві частини: призначення ролей користувачам і призначення повноважень доступу до об'єктів ролям. Це значно спрощує управління політикою безпеки: коли новий користувач приєднується до організації, адміністратору потрібно лише призначити йому ролі, що відповідають його посаді; при зміні посади користувача, адміністратор просто змінює ролі, пов'язані з цим користувачем; коли в систему додається новий додаток або завдання, адміністратору потрібно лише вирішити, яким ролям дозволено її виконувати.

Ієрархічні ролі. У багатьох додатках існує природна ієрархія ролей, заснована на знайомих принципах узагальнення та спеціалізації. На рис. 1.7 показано приклад ієрархії ролей: кожна роль представлена у вигляді вузла, а між спеціалізованою роллю та її узагальненням є дуга. Ієрархія ролей може бути використана для авторизації. Наприклад, повноваження, надані ролям, можуть бути поширені на їхні спеціалізації (наприклад, роль секретаря може мати всі права доступу, надані адміністративному персоналу). Належність повноважень також може бути застосована до призначень ролей, дозволяючи користувачам активувати всі узагальнення призначених їм ролей (наприклад, користувачеві, якому дозволено активувати роль секретар, також буде дозволено активувати роль адміністратор). Наслідування повноважень має перевагу у подальшому спрощенні керування повноваженнями. Але потрібно зауважити, що не завжди імплікація може бути потрібною, оскільки розповсюдження всіх повноважень суперечить принципу найменших привілеїв. Ієрархія також була використана в для визначення адміністративних привілеїв: окрім ієрархії організаційних ролей, визначається додаткова ієрархія адміністративних ролей; кожна адміністративна роль може бути наділена повноваженнями над частиною ролі ієрархії.

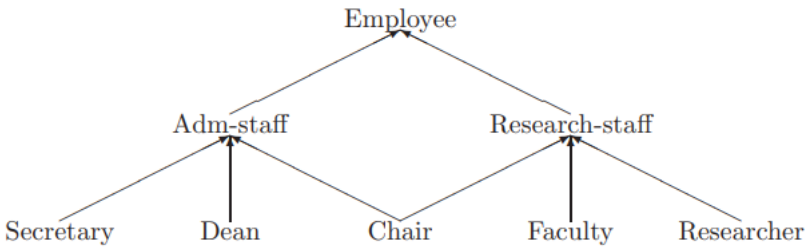


Рис. 1.7. Приклад ієрархії ролей

Ролі з найменшими привілеями. Ці ролі дозволяють користувачеві входити в систему з найменшими привілеями, необхідними для виконання конкретного завдання. Користувачам, які мають потужні ролі, не потрібно використовувати їх, доки ці привілеї не знадобляться. Це мінімізує небезпеку шкоди через ненавмисні помилки, троянських програм або зловмисників, які маскуються під законних користувачів.

Розподіл обов'язків. Розподіл обов'язків - це принцип, згідно з яким жоден користувач не повинен мати достатньо привілеїв, щоб зловживати системою на власний розсуд. Наприклад, особа, яка призначає зарплату, не повинна бути тією ж особою, яка може їх підготувати. Розподіл обов'язків можна забезпечити або статично (шляхом визначення конфліктуючих ролей, тобто ролей, які не можуть виконуватися той самий користувач) або динамічно (за допомогою контролю під час доступу). Прикладом динамічного розподілу обов'язків є правило двох осіб. Першим користувачем, який виконує операцію з двома особами, може бути будь-який авторизований користувач, тоді як другим користувачем може бути будь-який авторизований користувач, відмінний від першого.

Обмеження. Ролі забезпечують основу для специфікації та забезпечення виконання подальших вимог захисту, які можуть знадобитися в реальній політиці. Наприклад, можна вказати обмеження кардинальності, які обмежують кількість користувачів, яким дозволено активувати роль, або кількість ролей, яким дозволено використовувати певні привілеї. Обмеження також можуть бути динамічними, тобто накладатися на активацію ролей, а не на їх призначення. Наприклад, хоча декілька користувачів можуть мати право активувати роль голова, додаткове

обмеження може вимагати обмеження, щоб її міг активувати лише один користувач за один раз.

Рольова політика є перспективним напрямком і корисною парадигмою для багатьох комерційних та державних організацій. Однак, все ще існує певна робота, щоб охопити всі різні вимоги, які можуть виникнути в реальних ситуаціях. Наприклад, простий ієрархічний зв'язок, як це передбачається в простих ієрархічних відносинах, може бути недостатнім для моделювання різних видів відносин, які можуть виникнути. Наприклад, секретарю може знадобитися дозвіл на написання певних документів від імені свого керівника, але жодна з цих ролей не є спеціалізацією іншої. У такому випадку слід підтримувати різні способи поширення привілеїв. Так само слід збагатити адміністративну політику. Наприклад, традиційна концепція власності може більше не застосовуватися: користувач не обов'язково є власником об'єктів, які він створив, виконуючи певну роль. Також не слід забувати про ідентичність користувачів. Якщо це правда, що в більшості організацій роль (а не особистість) визначає привілеї, які можна виконувати, то також вірно і те, що в деяких випадках особу запитувача потрібно враховувати навіть тоді, коли прийнята політика базується на ролях. Наприклад, лікарю може бути дозволено вказувати лікування та доступ до файлів, але він може бути обмежений лікуванням та файлами для своїх пацієнтів, де відносини між лікарем і пацієнтом визначаються на основі їхньої ідентичності.

1.5 Привілейовані користувачі

Привілейовані користувачі в інформаційних системах – це адміністратори баз даних, спеціалісти з інформаційної та кібербезпеки, інженери систем та мереж. Для виконання робочих завдань їм потрібні необмежений доступ до пристроїв, баз даних, додатків, серверів й мереж. З таким рівнем привілейованого доступу користувачі мають величезні можливості. Вони можуть виконувати зміни в мережах, серверах, додатках, БД й, навіть, корпоративних пристроях (наприклад в ноутбуках, зовнішніх та внутрішніх накопичувачах даних). Керувати обліковими

записами та привілеями інших користувачів. Переглядати особисту інформацію робітників й клієнтів, різноманітні конфіденційні дані, куди входять юридичні дані, інтелектуальна власність, програмний код, які всі знаходяться в БД, що ними підтримуються. Можуть змінювати або видаляти дані. Реагувати на можливі попередження системи безпеки, переглядаючи, змінюючи чи видаляючи журнали аудиту.

Але зазвичай такі дії виконуються непомітно й за рамками їх робочих активів. А що може статися, якщо вони випадково чи навмисно принесуть загрозу доступності, конфіденційності чи цілісності даним організації своїми діями? Не маючи моніторингу, користувачі з привілеями можуть принести значну шкоду навіть без їх викриття.

Небезпеки привілейованих облікових записів користувачів. Величезна кількість IT-активів, що включають в себе хмарні технології, віртуалізацію, та технології Big Data, створюють потреби в ролях користувачів з більшими привілеями для їхнього контролю та управління. В кінці кінців, необмежені привілеї користувачів зазвичай призначаються певним ролям, щоб спростити процес управління іншими користувачами й дати гарантію, що вони можуть виконувати свою роботу. При цьому ця робота не буде змушувати спрацьовувати системи безпеки чи блокувати доступ до певних ресурсів.

Існують небезпеки, які пов’язані з обліковими записами користувачів з привілеями.

Спільне використання облікових даних. Деякі організації призначають для цілої ролі привілейовані права користувача, а не конкретній людині. Це знижує можливість відслідковування зловмисника у випадку випадкової чи навмисної зміни активів чи даних.

Порушення стандартів відповідності. Привілейований користувач може випадково чи спеціально порушувати стандарти цілісності, конфіденційності, доступності:

- Проблеми доступності. Користувачі з привілеями можуть зробити неправильні налаштування, що може призвести до заблокування доступу до веб-

сайту чи будь-якого іншого ресурсу. Вони можу змінювати паролі, тим самим блокуючи авторизованих користувачів.

- Проблеми цілісності. Користувачі з привілеями мають можливості змінювати або видаляти дані, навіть журнали аудиту, чиє завдання виявляти випадкові чи спеціальні зміни в даних.
- Проблеми конфіденційності. Користувачі з привілеями можуть отримувати доступ до ідентифікаційної особистої інформації або інших конфіденційних даних, навіть при умові, що цей доступ для їх роботи не потрібний.

Висновки до першого розділу

Політики контролю доступу в корпоративній інформаційній системі є одним з ефективних методів забезпечення інформаційної безпеки. За допомогою них обмежується доступ до конфіденційної інформації відповідно до прав користувачів на ті чи інші дані. Це зменшує ризик витоку цієї критичної інформації чи її несанкціоноване використання.

Якщо політики контролю доступу будуть правильно налаштовані, це знизить рівень можливих загроз, пов’язаних з привілейованими користувачами, та підніме рівень захисту інформації з обмеженим доступом в корпоративній системі. Ці політики в усіх сферах, наприклад державна, банківська, комерційна сфери.

2 ДОСЛІДЖЕННЯ РИНКУ PAM РІШЕНЬ

Управління привілейованим доступом (PAM), або управління привілейованими обліковими записами, - це певний клас рішень для забезпечення безпеки, який дозволяє організаціям контролювати і відстежувати діяльність привілейованих користувачів, включаючи їхній доступ до ключових бізнес-систем і те, що вони можуть робити після входу в систему. Більшість організацій впорядковують свої системи за рівнями відповідно до серйозності наслідків у разі злому або неправомірного використання системи. Привілейовані облікові записи, такі як облікові записи адміністратора домену та мережевого обладнання, надають адміністративні рівні доступу до систем високого рівня на основі вищих рівнів дозволів. Постачальники систем управління привілейованим доступом пропонують рішення, які допомагають адміністраторам контролювати доступ до критично важливих бізнес-ресурсів і гарантують, що ці високорівневі системи залишаються в безпеці. Цей додатковий рівень безпеки захищає критичні бізнес-системи, а також сприяє кращому управлінню та дотриманню вимог щодо захисту даних.

Звіт Verizon про розслідування витоків даних за 2020 рік показав, що понад 80% хакерських атак пов'язані з грубим використанням втрачених або викрадених облікових даних, а нещодавнє дослідження Centrify показало, що 74% витоків даних пов'язані з доступом до привілейованих облікових записів. Вкрай важливо, щоб організації забезпечували безпеку облікових даних для входу в систему, особливо для систем високого рівня ризику. Постачальники рішень PAM забезпечують таку безпеку, зберігаючи облікові дані для входу до привілейованих адміністративних облікових записів у захищеному сховищі, що знижує ризик їх викрадення. Щоб отримати доступ до цих облікових даних, користувачі повинні пройти процес автентифікації, який фіксує, що вони отримали доступ до облікового запису. Цей процес дозволяє організаціям чітко бачити, хто і звідки отримує доступ до облікового запису, що, в свою чергу, допомагає їм відстежувати будь-яку підозрілу або потенційно зловмисну активність, як внутрішню, так і зовнішню [2].

У даному розділі буде розглянуто десять рішень для управління привілейованим доступом, призначених для захисту критично важливих систем організації. Буде розглянуто такі функції, як керування паролями та багатофакторна автентифікація, безпека на основі ролей, сповіщення в режимі реального часу та надійні звіти. Буде також надана довідкова інформація про постачальників рішень для управління привілейованим доступом і ключові особливості самих рішень, а також про те, для якого типу клієнтів вони найкраще підходять.

2.1 JumpCloud Open Directory Platform™

Платформа Open Directory Platform™ від JumpCloud безпечно підключає привілейованих користувачів до критично важливих систем, додатків, файлів і мереж. JumpCloud забезпечує повну видимість і контроль над привілейованими обліковими записами. Вона забезпечує надійну автентифікацію, що дозволяє адміністраторам вимагати багатофакторну автентифікацію (MFA) перед наданням доступу, а також інтегрована з нашими можливостями єдиного підпису (SSO), за допомогою яких адміністратори можуть встановлювати деталізовані політики, що визначають, до яких ресурсів привілейовані облікові записи та окремі користувачі можуть отримати доступ за допомогою своїх ідентифікаційних даних [3].

Платформа відкритих каталогів JumpCloud також має надійне управління паролями та ключами SSH, що дозволяє адміністраторам встановлювати гранульований контроль складності паролів для привілейованих облікових записів, а також отримувати сповіщення про наближення терміну дії паролів та спроби злому цих облікових записів грубою силою.

Функції управління пристроями JumpCloud дозволяють адміністраторам повідомляти привілейованих користувачів про необхідність зміни пароля через певні проміжки часу, що автоматично оновлює паролі та доступ на всіх їхніх пристроях під управлінням MacOS, Windows та Linux, зменшуючи ризик від

статичних паролів, фішингу облікових даних та інших методів, що використовуються для атак на привілейованих користувачів.

JumpCloud використовують понад 180 000 організацій по всьому світу. Рішення має високу масштабованість та гнучкість і може слугувати основним каталогом організації або інтегруватися з існуючими каталогами, такими як Google Workload та Azure AD. Платформа має повний набір функцій управління ідентичностями, доступом та пристроями, що дозволяє організаціям контролювати та керувати привілейованими та стандартними ідентичностями з єдиної консолі. JumpCloud підходить підприємствам будь-якого розміру, які шукають ефективне та просте у використанні рішення для управління привілейованим доступом.

2.2 Heimdal™ Privileged Access Management

Heimdal™ - постачальник послуг з кібербезпеки з широким спектром рішень. Всі продукти безпеки Heimdal™ можуть бути розгорнуті за допомогою однієї платформи і агента. Heimdal™ Privileged Access Management - це рішення для управління привілейованим доступом, призначене для спрощення процесу захисту доступу користувачів до привілейованих облікових записів, а також для проактивного усунення загроз, пов'язаних з ідентифікацією [4].

За допомогою Heimdal™ Privileged Access Management адміністратори можуть увійти в інтуїтивно зрозумілу, сумісну з настільними та мобільними пристроями інформаційну панель, щоб призначати дозволи відповідно до ролей в Active Directory, видаляти права локального адміністратора, скасовувати права адміністратора в режимі реального часу, встановлювати періоди ескалації, реєструвати сеанси, схвалювати або відхиляти запити на ескалацію привілеїв - або створювати робочі процеси для автоматизації цього процесу. Інформаційна панель також пропонує функцію детального звітування, що дозволяє адміністраторам створювати звіти про використання привілейованих облікових записів, включаючи середню тривалість ескалації, для яких користувачів або файлів було підвищено привілеї, а також які дії були виконані під час сеансу.

Ці дані можуть бути використані для підтримки судового аналізу інцидентів, а також для підтвердження відповідності стандартам, таким як NIST AC-5 і NIST AC-1,6. Рішення PAM від Heimdal™ також проактивно усуває загрози для привілейованих облікових записів, автоматично завершуючи привілейовані сеанси при виявленні загрози на пристрої користувача, запобігаючи поширенню шкідливого програмного забезпечення і припиняючи доступ зловмисників до конфіденційних корпоративних даних, що зберігаються в системах високого рівня.

Heimdal™ Privileged Access Management розгортається в хмарі, що забезпечує високий рівень масштабованості і дозволяє адміністраторам входити в систему в будь-який час і з будь-якого місця. Рішення легко інтегрується з іншими рішеннями Heimdal™, що робить його особливо придатним для існуючих клієнтів. Heimdal™ PAM можуть використовувати організації будь-якого розміру, які шукають простий спосіб керувати та автоматизувати процеси ескалації привілеїв, а також контролювати дії привілейованих користувачів під час доступу до систем високого рівня.

2.3 ARCON | Privileged Access Management

Рішення ARCON для управління ризиками призначені для захисту даних і конфіденційності шляхом прогнозування ризикованих ситуацій, захисту організацій від цих ризиків і запобігання їх переростанню в інциденти. ARCON | Privileged Access Management (PAM) дозволяє командам корпоративної безпеки захищати та керувати всім життєвим циклом привілейованих облікових записів. Воно захищає привілейовані облікові дані від зловмисних інсайдерських атак і кіберзлочинів третіх сторін [5].

ARCON | PAM має захищене сховище паролів, яке автоматизує часту зміну паролів. Сховище генерує та зберігає надійні, динамічні паролі, доступ до яких мають лише авторизовані користувачі. Для доступу до сховища користувачі повинні пройти багатофакторну автентифікацію (MFA). ARCON пропонує власне програмне забезпечення на основі одноразового пароля (OTP) для перевірки

ідентичності користувачів, і цей інструмент інтегрується з рішеннями автентифікації сторонніх виробників, якщо організація хоче побудувати рівні автентифікації навколо сховища. Безпека MFA дозволяє ARCON | PAM запускати єдиний вхід (SSO) для доступу до всіх критично важливих систем без необхідності користувачам ділитися своїми обліковими даними. Це робить процес входу більш ефективним, одночасно захищаючи критичні дані від загрози зламу паролів. Нарешті, весь привілейований доступ надається "точно і вчасно", що зменшує поверхню загрози, надаючи перевагу доступу за потребою, а не постійним привілеям.

Розширений моніторинг сеансів дає адміністраторам повне уявлення про те, хто і чому використовує середовище привілейованого доступу, що дозволяє швидше зменшити ризики. ARCON | PAM також надає повний аудиторський слід привілейованих дій, а також звіти та аналітику результатів за допомогою механізму звітності рішення. Це дозволяє менеджерам і аудиторам оцінювати стан відповідності в організації в міру необхідності.

ARCON | PAM також має високу масштабованість. З цих причин, незважаючи на використання технології корпоративного рівня, ARCON | PAM можна використовувати для організацій будь-якого розміру.

2.4 BeyondTrust Privileged Remote Access

BeyondTrust - провідний постачальник рішень для управління привілейованим доступом. Вони пропонують широкий спектр рішень, які забезпечують високий рівень прозорості та безпеки для кінцевих точок, серверів, хмарних середовищ, DevOps та мережевих пристроїв. Privileged Remote Access - це рішення BeyondTrust для управління та аудиту внутрішнього та стороннього віддаленого привілейованого доступу без необхідності використання VPN. Воно призначене для підвищення продуктивності співробітників, незалежно від їхнього місцезнаходження, а також для запобігання доступу зловмисників до критично важливих бізнес-систем [6].

Privileged Remote Access зберігає паролі в захищеному хмарному сховищі на пристрої. Крім того, це рішення інтегрується з BeyondTrust Password Safe, яке постачається як програмне забезпечення. Обидва варіанти увімкнуть можливості BeyondTrust щодо ін'єкції облікових даних, які дозволяють BeyondTrust безпечно вводити облікові дані зі сховища безпосередньо в сеанс. Це означає, що користувачі не розкривають свої облікові дані в будь-який момент під час входу в систему. Рішення також має потужні можливості моніторингу, з можливостями відстеження та аудиту, доступними в єдиному інтерфейсі. Адміністратори можуть налаштувати параметри авторизації та сповіщень, щоб отримувати сповіщення, коли користувач отримує доступ до привілейованого віддаленого доступу. Ці сповіщення також зручні для віддалених працівників, щоб адміністратори мали змогу затверджувати запити на доступ і контролювати використання на своїх мобільних пристроях з будь-якого місця. Комплексні контрольні журнали та криміналістика сеансів дозволяють IT-командам переглядати та контролювати використання привілейованих облікових записів, а також створювати звіти для підтвердження відповідності.

Privileged Remote Access включає в себе настільні консолі для Windows, Mac і Linux. Він також дозволяє привілейованим користувачам отримувати доступ до критично важливих систем через веб-консоль або мобільний додаток для привілейованого доступу в будь-який час і в будь-якому місці. Це робить його потужним рішенням PAM для будь-якої організації з віддаленими працівниками, яким потрібен доступ до привілейованих систем.

2.5 Bravura Privilege

Bravura Security пропонує зручні рішення для управління ідентифікацією, правами та обліковими даними, які легко розгортаються та є простими у використанні. Їхні рішення дозволяють організаціям посилити внутрішній контроль і мережеву безпеку, а також знизити операційні витрати завдяки розгортанню та управлінню хмарними технологіями. Bravura Privilege, їхнє

рішення PAM, захищає привілейованих користувачів, додатки та сервіси. Маючи високу масштабованість, воно підтримує понад мільйон змін паролів щодня по всьому світу [7].

Bravura Privilege генерує паролі випадковим чином і зберігає їх у зашифрованому сховищі, яке вимагає від користувачів підтвердити свою особу, перш ніж вони зможуть отримати доступ до них. Рішення забезпечує попередньо авторизований одноразовий доступ, щоб користувачі отримували доступ до критично важливих облікових записів в потрібний момент і не могли залишатися в системі, коли їм це не потрібно. Розширення для входу запускаються автоматично через розширення для браузера, а всі запити на доступ і сеанси реєструються за допомогою відеозапису та клавіатурного журналу. Це дозволяє адміністраторам повністю контролювати діяльність привілейованих облікових записів. Bravura Privilege використовує спеціальний агент для додатків на основі відбитків пальців і автоматично повертає одноразові ключі, щоб усунути спільні та статичні облікові дані, знижуючи ризик злому через крадіжку облікових даних. Рішення також реєструє всі випадки доступу користувачів, створюючи сильну підзвітність і дозволяючи адміністраторам бачити, хто і до яких систем має доступ.

Bravura Privilege спрощує завдання координації зміни паролів і доступу до спільних облікових записів на різних платформах. Воно може інтегруватися з усіма клієнтами, серверами, гіпервізорами, гостьовими операційними системами, базами даних і додатками, а також може бути розгорнуте локально або в хмарі. Це універсальне рішення забезпечує надійне управління доступом для будь-якого підприємства, яке прагне захистити велику кількість привілейованих облікових записів.

2.6 Broadcom Symantec Privileged Access Management

Symantec є провідним виробником рішень для запобігання втраті корпоративних даних (DLP), захисту кінцевих точок та веб-безпеки. Symantec Privileged Account Management (PAM) - це рішення для управління

привілейованими обліковими записами, покликане допомогти організаціям легше контролювати та керувати доступом до корпоративних облікових записів високого рівня, щоб знизити ризик порушень, пов'язаних з обліковими даними, та забезпечити відповідність галузевим стандартам, таким як PCI-DSS [8].

Symantec PAM зберігає всі привілейовані облікові дані, включаючи паролі root і адміністратора, а також ключі SSH, у захищеному сховищі. Перш ніж отримати доступ до сховища, користувачі повинні підтвердити свою особу за допомогою двофакторної автентифікації, а облікові дані автоматично повертаються відповідно до налаштованих адміністратором політик, щоб забезпечити відповідність стандартам захисту даних і запобігти порушенням, пов'язаним з використанням постійних облікових даних. Symantec PAM безперервно відстежує активність привілейованих користувачів, застосовуючи методи машинного навчання для порівняння поточних дій з історичними, щоб виявити підозрілу або аномальну поведінку. Адміністратори можуть налаштувати автоматичне виправлення такої поведінки, щоб допомогти обмежити латеральне поширення атак по всій мережі. Нарешті, платформа збирає дані аудиту з кожного привілейованого сеансу, пов'язуючи всі дії з конкретним користувачем і зберігаючи ці дані в зашифрованому сховищі, де вони можуть бути використані для аудиту та дотримання нормативних вимог або як докази ризикованої поведінки. З цією ж метою адміністратори можуть записувати всі привілейовані сеанси на відео.

Symantec Privileged Access Management чудово підходить середнім і великим організаціям, які бажають впровадити рішення PAM для запобігання порушень, пов'язаних з обліковими даними, і атак на сторонні облікові записи, що призводять до їх компрометації. Платформа також добре підходить компаніям, які вже використовують інші технології безпеки Symantec, оскільки вони отримають вигоду від простоти інтеграції та уніфікованого огляду своїх інструментів безпеки.

2.7 CyberArk Privileged Access Management

CyberArk займає одну з найбільших часток ринку PAM, пропонуючи рішення корпоративного рівня на основі політик, які дозволяють IT-командам захищати, керувати та реєструвати діяльність привілейованих облікових записів. Їхнє рішення Core Privilege Access Security (PAS) забезпечує багаторівневий захист доступу до привілейованих облікових записів і поставляється з більш ніж 500 готовими інтеграціями. Централізоване управління та звітність дають адміністраторам чітке уявлення про те, хто і з якою метою отримує доступ до критично важливих систем [9].

Core PAS безперервно сканує мережу для виявлення привілейованого доступу. IT-команди можуть підтверджувати спроби доступу, додаючи їх до черги, або автоматично направляти облікові записи та облікові дані відповідно до політик компанії. Облікові дані для доступу до критично важливих активів ізольовано зберігаються в захищеному сховищі, що допомагає запобігти витоку облікових даних. З центральної консолі управління IT-команди можуть записувати та перевіряти привілейовані сеанси в зашифрованому сховищі. Записи включають відтворення відео, тому адміністратори можуть переглядати конкретні дії та натискання клавіш і відстежувати їх на предмет підозрілої активності. Якщо виявлено підозрілу поведінку, Core PAS автоматично призупиняє або завершує привілейований сеанс залежно від рівня ризику. Автоматичне перенаправлення облікових даних після призупинення або завершення сеансу гарантує, що зловмисники або скомпрометовані внутрішні облікові записи не зможуть знову отримати доступ до системи.

CyberArk також пропонує розширену версію Core Privileged Access Security, яка включає централізовано керований гранульований контроль доступу для захисту серверів з найменшими привілеями та моніторинг мережі на предмет загроз для контролерів доменів. Обидва ці модулі повністю інтегруються зі стандартним рішенням. Рішення CyberArk поставляється з локальними, хмарними та SaaS варіантами розгортання, що робить його придатним для всіх організацій, незалежно від того, на якій стадії переходу вони знаходяться на хмарні технології.

Core Privileged Access Security підходить для будь-якого підприємства, яке шукає надійне та гнучке рішення для управління привілейованим доступом.

2.8 Delinea Secret Server

Delinea є фахівцем з надання рішень для управління доступом на рівні підприємства. Secret Server - це інструмент управління привілейованим доступом від Delinea, розроблений, щоб допомогти організаціям контролювати, управляти та захищати доступ до найбільш важливих корпоративних баз даних, додатків, гіпервізорів, інструментів безпеки та мережевих пристроїв. Secret Server пропонує ряд потужних функцій безпеки, а також надійні інструменти моніторингу та аудиту сеансів, щоб допомогти компаніям захистити дані компанії від атак зловмисників і забезпечити відповідність нормативним вимогам щодо захисту даних [10].

Secret Server зберігає всі привілейовані облікові дані в зашифрованому централізованому сховищі, доступ до якого користувачі можуть отримати лише за допомогою двофакторної автентифікації. Після перевірки користувачі можуть переглядати лише ті паролі, які їм потрібні для виконання своєї роботи, відповідно до налаштованих адміністратором засобів контролю доступу. З централізованого порталу управління адміністратори можуть надавати та скасовувати привілеї для доступу "точно і вчасно", а також налаштовувати політики складності паролів і зміни облікових даних. Це виключає використання слабких і статичних паролів, знижуючи ризик їх крадіжки. Адміністратори також можуть налаштувати власний робочий процес для делегування запитів на доступ, в тому числі для третіх осіб. Потужні можливості запису сеансів дозволяють організаціям контролювати привілейовану діяльність як для забезпечення дотримання нормативних вимог, так і для виявлення джерела будь-якої шахрайської або підозрілої активності.

Secret Server доступний для розгортання локально або в хмарі в двох пакетах: професійний пакет пропонує зашифроване сховище паролів з інтеграцією AD, аудитом і звітністю, а також інтеграцією CRM, SAML і HS; пакет Platinum пропонує все вищезазначене, а також робочі процеси затвердження, захист Unix,

розширені сценарії та аварійне відновлення. Загалом, Secret Server від Delinea - це надійне рішення для підприємств, які прагнуть захистити і централізовано керувати доступом до своїх критично важливих систем, облікових записів і додатків, як для запобігання атакам з метою заволодіння обліковими записами, так і для забезпечення відповідності федеральним і галузевим стандартам захисту даних.

2.9 Foxpass Privileged Access Management

Foxpass Privileged Access Management автоматизує доступ до серверів і мережі, захищаючи критичні бізнес-системи та зменшуючи навантаження на ресурси IT-команди. Він розроблений для безперешкодної інтеграції з будь-якими системами, які вже є в організації, включаючи хмарні поштові системи та існуючі SSO-рішення, щоб клієнти могли налаштувати свій захист всього за кілька хвилин [11].

Foxpass Privileged Access Management пропонує самообслуговування SSH-ключів і паролів з MFA і зміною паролів. Адміністратори можуть встановлювати вимоги до паролів за допомогою простого у використанні інтерфейсу. Рішення також пропонує повний API, який дозволяє адміністраторам автоматизувати контроль доступу до серверів, змінювати інформацію про користувачів та керувати членством у групах. API реєструє запити на автентифікацію, щоб адміністратори мали чітке уявлення про те, хто отримує доступ до критично важливих систем, і ці журнали також можна використовувати як доказ відповідності вимогам. Хмарні LDAP і RADIUS дозволяють Foxpass PAM забезпечувати єдиний вхід для всього стека додатків організації, зменшуючи потребу в паролях. Адміністратори також можуть увімкнути MFA на цьому рівні для додаткової безпеки, а також реєстрацію запитів LDAP і RADIUS для автоматичного виявлення загроз і реагування на них.

Рішення PAM від Foxpass забезпечує безпеку корпоративного рівня, але має високу масштабованість і доступне як локально, так і в хмарі. Воно також легко інтегрується з існуючими сторонніми продуктами, такими як Google Workspace, Microsoft 365 та Okta. Клієнти хвалять Foxpass за їхню технічну підтримку 24/7,

особливо за дзвінки в режимі реального часу. Тому Foxpass Privileged Access Management є надійним рішенням для організацій будь-якого розміру, які шукають зручну систему управління привілейованим доступом, яку легко інтегрувати та розгортати.

2.10 One Identity Safeguard

One Identity - це постачальник рішень безпеки, орієнтованих на ідентифікацію, призначених для зменшення поверхні атаки внутрішніх і зовнішніх загроз для організацій. Всі PAM-продукти One Identity доступні у вигляді модулів або інтегрованих пакетів, тому клієнти можуть додавати нові можливості до вже існуючих заходів. Рішення Safeguard дозволяє організаціям захищати, контролювати та перевіряти привілейовані облікові записи протягом усього сеансу роботи. Воно має потужні можливості автоматичного виявлення та забезпечення, які полегшують адміністраторам моніторинг та реагування на підозрілу або несанкціоновану поведінку [12].

Завдяки рішенню Safeguard від One Identity користувачі можуть отримати доступ до своїх привілейованих і непривілейованих ресурсів з одного облікового запису, що усуває ризик помилки при наданні доступу. Це також зменшує навантаження на службу підтримки, автоматизуючи процес надання привілейованих облікових даних відповідно до ролі користувача. Привілейовані облікові записи зберігаються в захищеному сховищі для посилення безпеки, з централізованою автентифікацією та SSO для додаткового захисту та підвищення ефективності. Safeguard використовує машинне навчання для аналізу активності користувача як під час доступу, так і протягом сеансу. Він також записує натискання клавіш, рухи миші та переглянуті вікна, щоб виявити несанкціоноване використання критично важливих бізнес-систем і підвищити підзвітність. Адміністратори можуть віддалено переглядати ці записи і шукати в них, як у базі даних, конкретні події в сеансах. Вони також можуть бути використані для цілей управління та дотримання нормативних вимог.

Safeguard дозволяє адміністраторам налаштовувати рівень автентифікації, необхідний для кожного користувача, від вимоги повних облікових даних до обмеження доступу за допомогою гранульованого делегування для доступу "точно і вчасно" або найменш привілейованого доступу. Це забезпечує безпеку без шкоди для продуктивності співробітників. Потужні інструменти запису та аналізу роблять Safeguard потужним PAM-рішенням для великих підприємств, які потребують більшого контролю над привілейованими діями.

Висновки до другого розділу

Під час вибору PAM-системи необхідно проводити порівняння різних рішень, щоб обрати найкраще рішення для системи конкретної організації. В залежності від мети та необхідного функціоналу, рішення PAM будуть мати свої переваги та недоліки.

Під час зрівняння необхідно враховувати: функціональність, швидкість реагування, захист від кібератак та ціну. Одні системи можуть мати ширший функціонал, але можуть потребувати більше ресурсів, які не завжди є. Інші системи є дешевшими, але у них може бути недостатній функціонал.

3 КЕРУВАННЯ ПРИВІЛЕЙОВАНИМИ ОБЛІКОВИМИ ЗАПИСАМИ ТА ЇХ ЗАХИСТ ЗА ДОПОМОГОЮ PAM РІШЕННЯ CYBERARK PRIVILEGED ACCESS MANAGEMENT

3.1 Архітектура PAM рішення

PAM забезпечує безпечне середовище у межах підприємства, де всі адміністративні паролі надійно архівуються, передаються та є загальнодоступними для авторизованих користувачів, таких як IT-персонал, чергові адміністратори та локальні адміністратори у віддалених місцях.

Кілька рівнів безпеки, що лежить в основі рішення PAM, включаючи брандмауери, VPN, автентифікацію, контроль доступу, шифрування тощо, забезпечують найбезпечніше рішення для зберігання та обміну паролями в корпоративному середовищі.

Рішення PAM — це рішення plug-and-play, яке вимагає мінімальних зусиль з налаштування та може бути повністю працездатним за частку часу. Доступ до нього та керування ним можна отримати через клієнт Windows, веб-інтерфейс або різні API.

На рис. 3.1 показано різні компоненти рішення PAM і їх взаємодію [13].

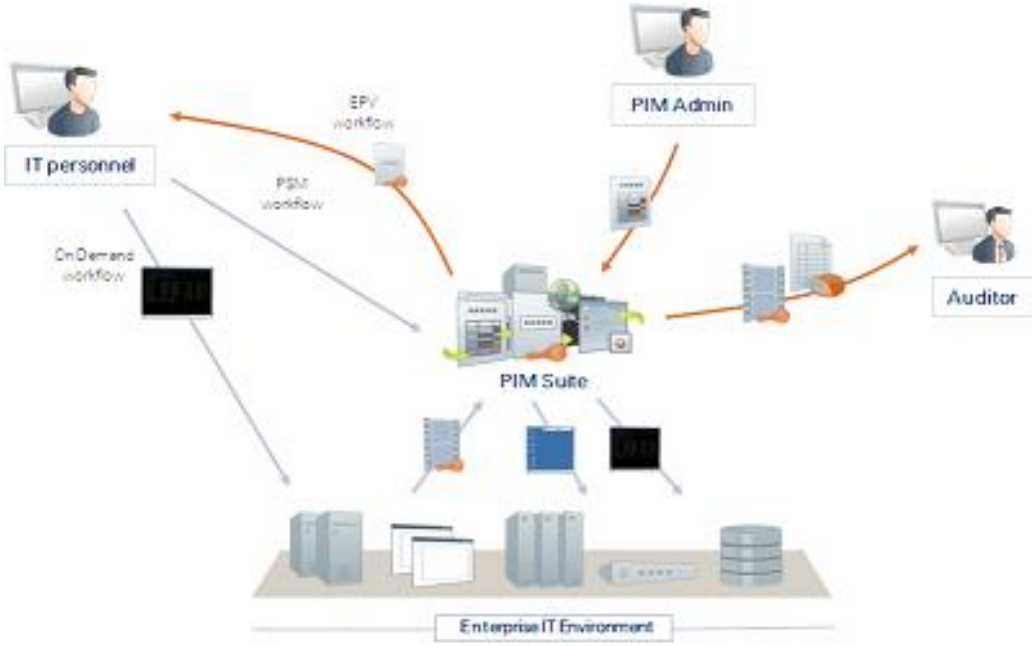


Рис. 3.1. Архітектура PAM

Архітектура рішення PAM складається з двох основних елементів. Одним з них є механізм зберігання даних (також відомий як «сервер»), який зберігає дані та відповідає за захист даних у стані спокою та надання автентифікованого та контрольованого доступу.

Другим елементом є інтерфейс (інтерфейс Windows, веб-інтерфейс і SDK), який взаємодіє з системою зберігання даних, з одного боку, і забезпечує доступ користувачам і додаткам, з іншого. Механізм зберігання та інтерфейс взаємодіють за допомогою безпечного протоколу CyberArk — протоколу Vault.

3.2 Проєктування та впровадження

3.2.1 Перевірка середовища й мережі

Для того, щоб встановити де і яку кількість компонентів CyberArk треба розгорнути, потрібно мати уявлення про такі аспекти:

- Топологія мережі організації, включаючи сегменти приватної мережі, які можуть містити кінцеві точки, такі як DMZ.
- Географічне розташування всіх ділянок з об’єктами дослідження та оцінка кількості об’єктів на кожній ділянці.
- У яких центрах обробки даних доступний HSM?
- Загальна кількість користувачів CyberArk та їх місцезнаходження. Це включає в себе оцінку відсотка загальної кількості користувачів, які отримують доступ до рішень CyberArk (і кінцевих точок) з кожного географічного регіону або центру обробки даних/офісу.
- Кількість одночасних сеансів RDP або SSH, які адміністратор може вимагати в певній «зоні» в будь-який момент часу.
- Будь-які додаткові норми, які можуть застосовуватися в певних регіонах, як-от GDPR (Загальний регламент про захист даних) або CCPA (Каліфорнійський закон щодо захисту персональних даних).

- Прогнозований ріст протягом наступних кількох років, включаючи загальну частоту придбань.

3.2.2 Список контролю доступу для управління користувачами

Варто, щоб групи користувачів як для прав доступу до програми CyberArk , так і для прав безпечного доступу визначали та керували ними на основі ролі користувача. Ролі, які можна використати для класифікації груп користувачів, а також практичні поради до них.

Ролі програми – ці ролі надають доступ до програми CyberArk, але не надають прямого доступу до сейфів. Вони поділяються на:

- Адміністраторів сховищ (Vault Administrators). Адміністратори сховища повинні мати власні облікові записи CyberArk і не повинні походити із зовнішніх каталогів (таких як AD і LDAP), щоб зменшити ризик атак на основі каталогів. Ці облікові записи повинні управлятися за допомогою CyberArk PAM Solution і можуть бути примусово підключені до PVWA або PrivateArk Client через сеанс PSM.
- Кінцеві користувачі & Аудитори. Кінцевими користувачами та аудиторами слід керувати за допомогою зовнішніх каталогів (таких як AD та LDAP). Це дозволяє здійснювати масштабне управління користувачами через зовнішні каталоги та сторонні інструменти IAG/IAM, зберігаючи при цьому додаткову безпеку для високопривілейованих користувачів, таких як адміністратори сховища.

Безпечні ролі – ці ролі є специфічними для сейфів - вони не визначають, який рівень адміністративних прав має користувач на рівні програми.

Призначення безпечних дозволів також слід здійснювати за допомогою зовнішнього каталогу, наприклад, AD або LDAP, де дозволи призначаються групам, а не окремим користувачам. Це полегшує керування, оскільки права на безпеку можна призначати, додаючи користувачів до груп AD/LDAP, після того, як відповідні групи будуть призначені відповідним сейфам на основі необхідної ролі.

Хоча CyberArk пропонує деякі базові безпечні ролі, детальна суть дозволів на безпеку дозволяє організації адаптувати свої безпечні ролі відповідно до вимог організації. Однак, завжди варто використовувати підхід найменших привілеїв, надаючи користувачам якомога менше дозволів, необхідних для виконання їхньої роботи.

Загалом, необхідно розробляти безпечні дозволи подібно до того, як описано в рис 3.2 [13]. Обліковий запис Майстра сховища має бути єдиним обліковим записом з повними правами на створені користувачем сховища, щоб надавати деякі з цих прав іншим користувачам або групам. Облікові записи адміністратора сховища, які використовуються для адміністрування самого рішення, повинні мати дуже мало дозволів на більшість сейфів. Такий розподіл дозволів на сейфи та програми забезпечує більшу безпеку, оскільки жоден обліковий запис (окрім вбудованого головного облікового запису) не має повних дозволів як на сейфи, так і на саму програму "CyberArk".

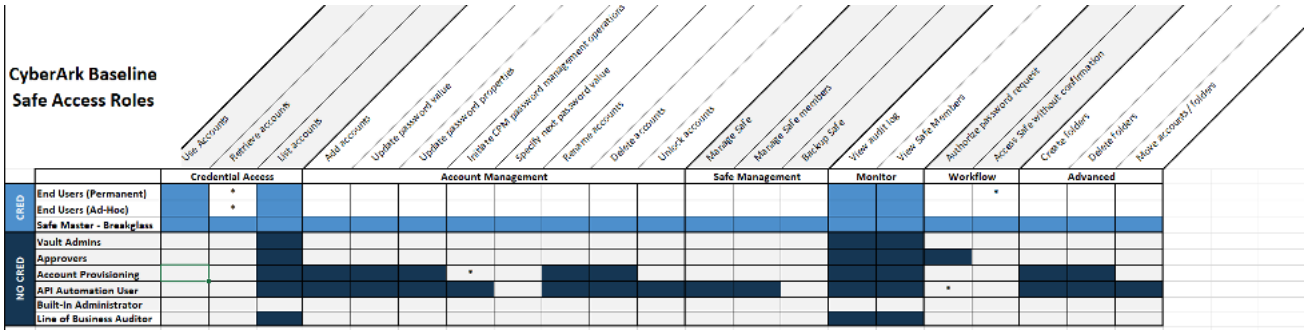


Рис. 3.2. Матриця Безпечних ролей

3.2.3 Управління користувачами

Для надання безпечного доступу слід використовувати користувачів і групи з підключеної служби каталогів. Кожна група має бути налаштована як "учасник Сейфу" з відповідними правами доступу. Коли користувачі додаються до визначених груп у каталозі, вони автоматично отримують доступ до налаштованих Сейфів. Аналогічно, користувачі, які видаляються з визначених груп, автоматично видаляються з Цифрового Сховища CyberArk. Для цього процес додавання користувачів до групи AD або видалення користувачів з групи для безпечного

доступу виконується в автоматизованому режимі в рамках загального процесу управління ідентифікацією та життєвим циклом.

Рішення CyberArk PAM пропонує комплексне управління внутрішніми користувачами. Якщо в організації немає служби каталогів, можна створити локальних користувачів і групи в CyberArk Digital Vault. Це можна зробити вручну або автоматично за допомогою одного з багатьох API, які пропонує CyberArk (наприклад, REST API або інтерфейс командного рядка). При локальному управлінні користувачами CyberArk може підтримувати локальну автентифікацію, а також будь-яку зовнішню службу автентифікації, що налаштовується (наприклад, LDAP, RADIUS і SAML).

При інтеграції рішень CyberArk із зовнішнім каталогом необхідно враховувати, які адміністратори каталогу можуть додавати користувачів до груп користувачів, що мають доступ до CyberArk Digital Vault. Якщо до групи користувачів CyberArk буде додано неавторизованого користувача, він може отримати доступ до привілейованих облікових записів, захищених у CyberArk Digital Vault. Організації повинні співпрацювати з адміністраторами каталогів, щоб встановити надійний процес затвердження, перш ніж додавати нового користувача до групи користувачів CyberArk. Крім того, для SSL-з'єднання між CyberArk Digital Vault і каталогом потрібен кореневий сертифікат для центру сертифікації, який видав сертифікат на серверах каталогу.

3.3 Можливості адміністратора

3.3.1 Керування користувачами

Прозоре керування користувачами за допомогою LDAP. Рішення PAM можна налаштувати для зв’язку з LDAP-сумісними серверами каталогів для отримання інформації про ідентифікацію користувача та безпеки. Це забезпечує автоматичне налаштування користувачів і груп, забезпечуючи прозоре керування користувачами.

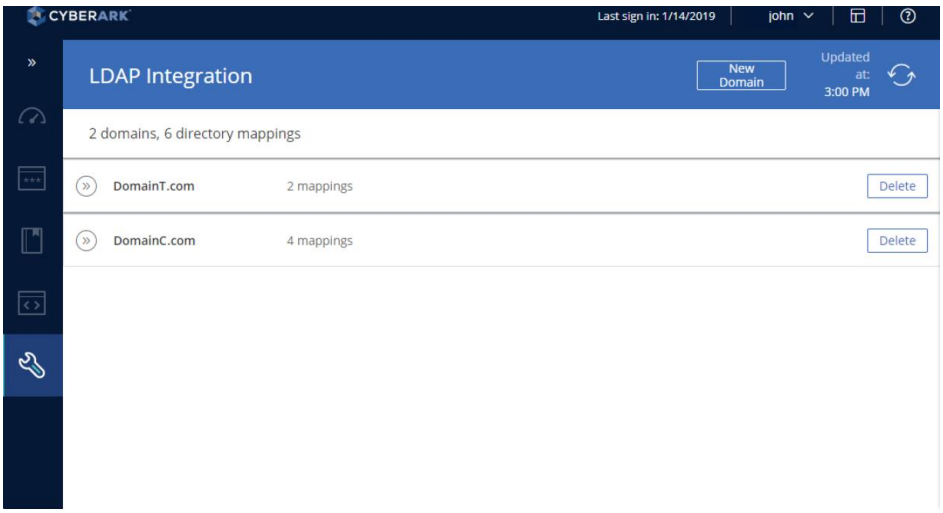


Рис. 3.3. Інтеграція LDAP

Проходження автентифікації в диспетчері привілейованого доступу. Щоб працювати з PAM, користувачі повинні пройти автентифікацію в Vault за допомогою попередньо визначеного методу автентифікації. PAM підтримує два рівні автентифікації: первинний і вторинний. Первинна автентифікація встановлює початкове безпечне з'єднання між інтерфейсом CyberArk і сервером CyberArk Vault, щоб надати доступ користувачам. Вторинна автентифікація зміцнює безпечне з'єднання, додаючи додаткову процедуру ідентифікації користувача.

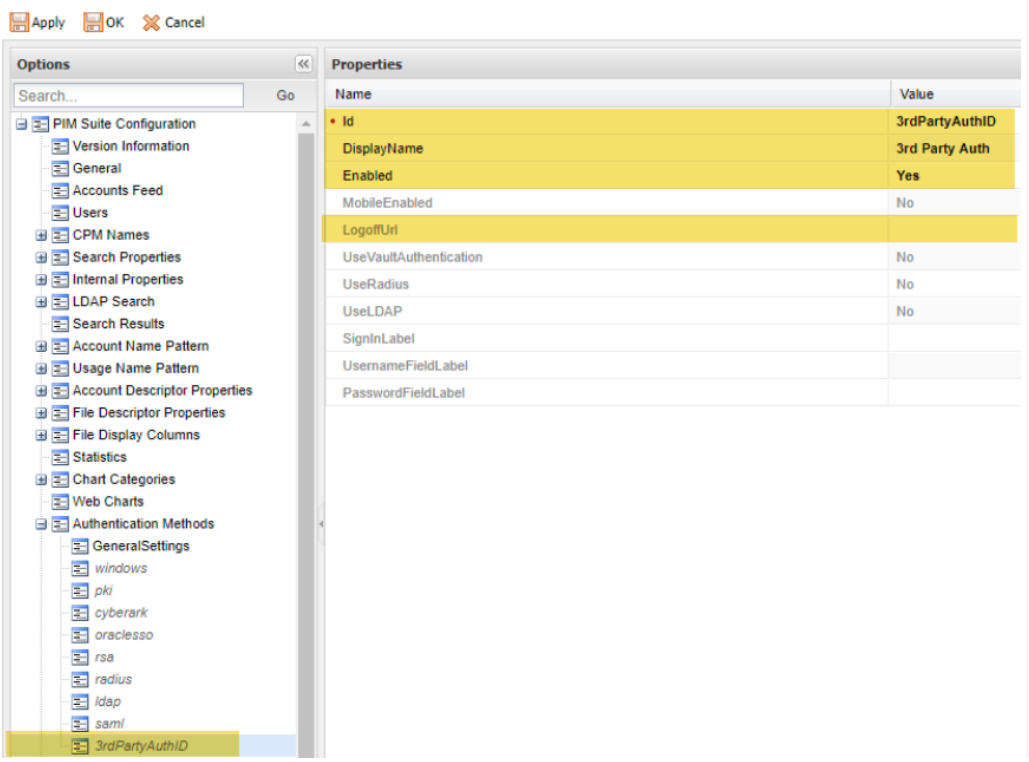


Рис. 3.4. Параметри методу автентифікації

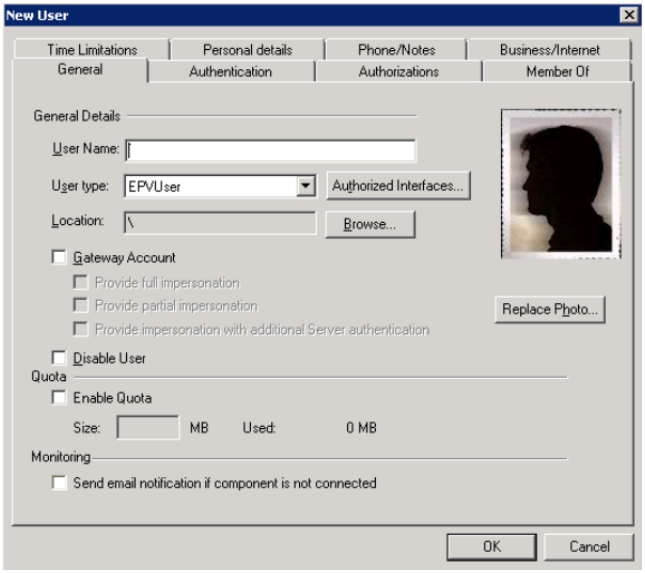
Налаштування автентифікації PKI для клієнта PrivateArk. Користувачі також можуть увійти в клієнт PrivateArk через PKI організації за допомогою свого особистого сертифіката, який автентифікує їх у Сейфі.

Рис. 3.5. Тест автентифікації

Керування місцезнаходженням. Розташування представляє собою організаційну ієрархію. Можна організовувати сейфи, користувачів і групи за розташуванням. Крім того, якщо впорядкувати усі сейфи відповідно до розташування, можна використовувати фільтр сейфів, щоб переглядати лише сейфи в певному місці, а не всі ваші сейфи одночасно. Також можна встановити максимальний обсяг дискової квоти, який можуть використовувати користувачі в місці, що забезпечує контроль над розміром сейфа.

Керування окремими користувачами. Адміністратор Сховища відповідає за керування користувачами в Сховищі. Користувачів можна створювати, видаляти, оновлювати тощо. Ці завдання виконуються у вікні Користувачі та групи. Користувачі поділяються на ієрархічні рівні, які відображають ієрархію в офісному середовищі. Кожен відділ може мати менеджера користувачів, який створює нових користувачів і оновлює властивості існуючих користувачів. Менеджери користувачів можуть керувати користувачами, які перебувають на тому самому ієрархічному рівні, і користувачами нижчих рівнів. Таким чином, менеджери користувачів мають можливість контролювати дозволи користувачів в інших відділах, які ієрархічно знаходяться нижче, так само, як це робив би їхній власний

менеджер. На Рис. 3.6 – 3.11 будуть показані вкладки, в які потрібно водити дані при створенні нового користувача.



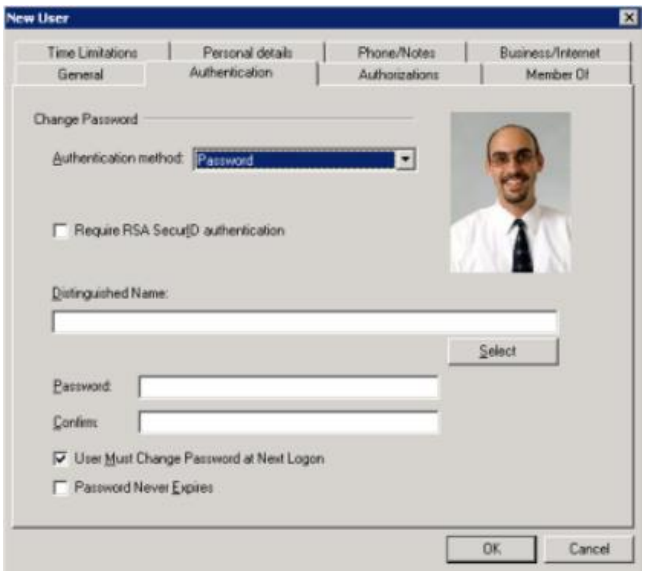
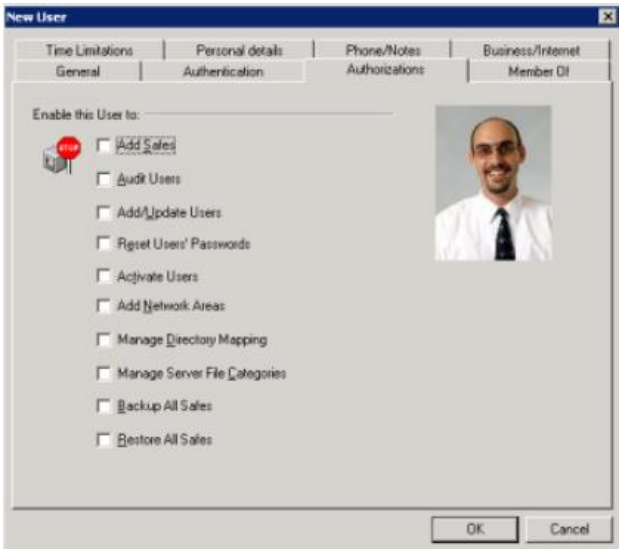


Рис. 3.6 – 3.7. Вкладки Загальна інформація та Автентифікація



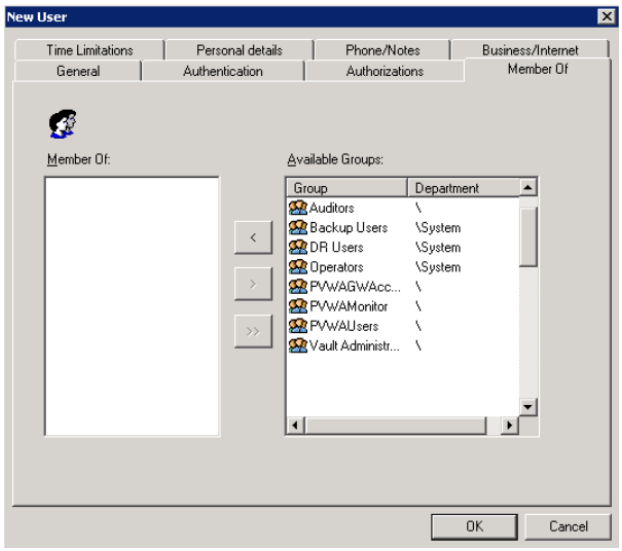


Рис. 3.8 – 3.9. Вкладки Авторизація та Член групи

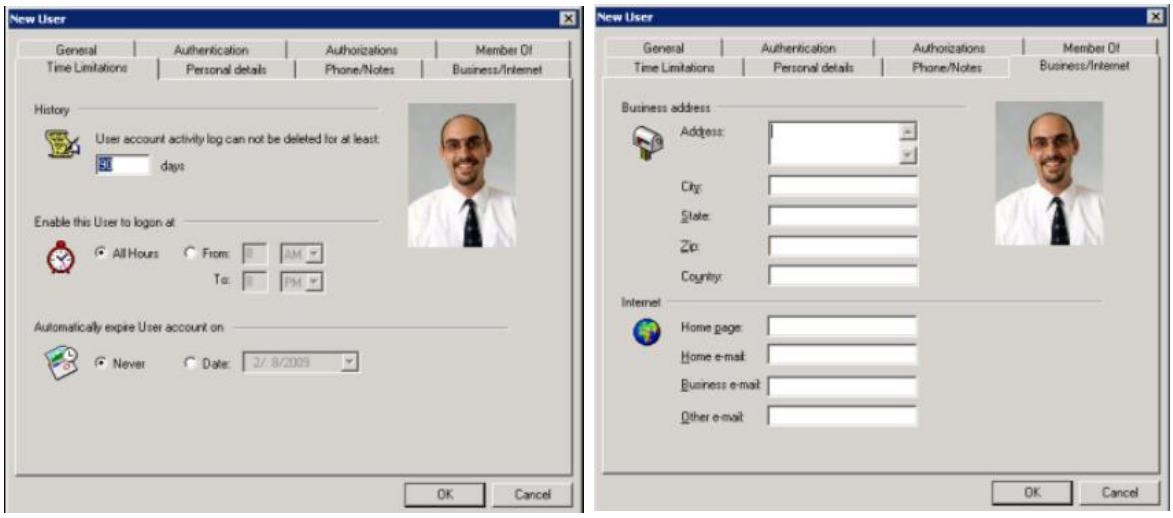


Рис. 3.10 – 3.11. Вкладки Часові обмеження та Бізнес/Інтернет

Керування групами. Група – це сукупність користувачів, які мають однакові повноваження. Визначивши групу, можна спільно надати всім користувачам у групі однакові повноваження. Так само, коли оновлюється повноваження групи, це впливає на повноваження кожного члена групи. Користувачі, які є членами кількох Груп, які володіють одним і тим самим Сейфом, матимуть повноваження першої групи, яку було додано як Власника до Сейфа, або комбінацію повноважень усіх груп, до яких вони належать, залежно від того, як Сховище налаштовано. Проте, якщо користувач є незалежним Власником того самого Сейфа, його власні повноваження матимуть перевагу над дозволами Групи.

Попередньо визначені користувачі та групи. CyberArk Vault автоматично створює кількох користувачів і груп під час встановлення та оновлення. Ці користувачі створені для виконання адміністративних завдань і усувають необхідність постійного доступу конкретних користувачів для виконання адміністративних завдань. Попередньо визначені групи автоматично додаються до кожного сейфа в сховищі, а відповідний попередньо визначений користувач додається як учасник. Користувачі, додані до цих груп, одразу стають власниками всіх Сейфів відповідно до повноважень Групи в Сейфах. Ці групи можна видалити з Сейфів відповідно до конфігурації Сховища.

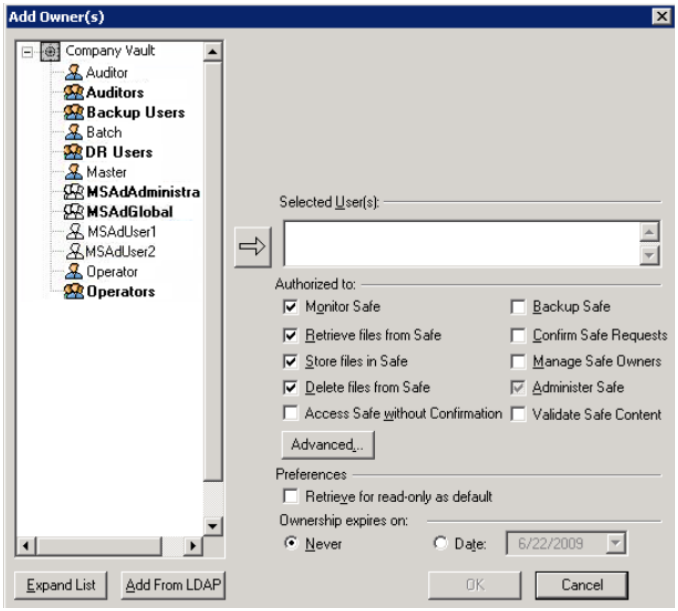


Рис. 3.12. Визначені групи

3.3.2 Привілейовані облікові записи

Управління доступом. Контроль доступу визначає, які авторизовані користувачі можуть отримати доступ до інформації та звідки вони можуть отримати доступ до інформації. Рішення Privileged Access Manager керує контролем доступу, зберігаючи привілейовані особи в сейфах і надаючи доступ лише авторизованим користувачам. Детальні дозволи визначають інформацію, яку користувачі можуть бачити в кожному сейфі, і як вони можуть використовувати цю інформацію.

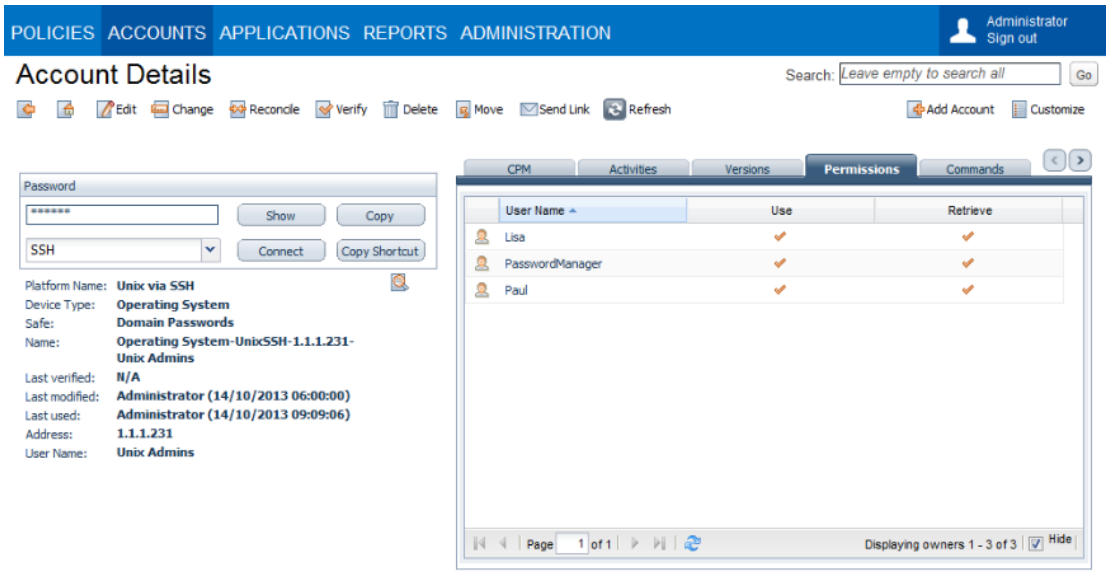


Рис. 3.13. Учасник в Сейфі

Інтерфейс управління платформами v10. Платформа визначає спільні характеристики для кількох облікових записів. Він визначає технічні налаштування для цих облікових записів, наприклад:

- Властивості облікового запису
- Політика та часові рамки керування обліковими даними
- Правила, які необхідно застосовувати під час генерації нового випадкового пароля
- Керування сеансами
- Пов’язані облікові записи
- Сповіщення поштою
- Робочі процеси

Параметри залежать від типу платформи. Кожен обліковий запис, визначений у системі, має бути пов’язаний із відповідною платформою.

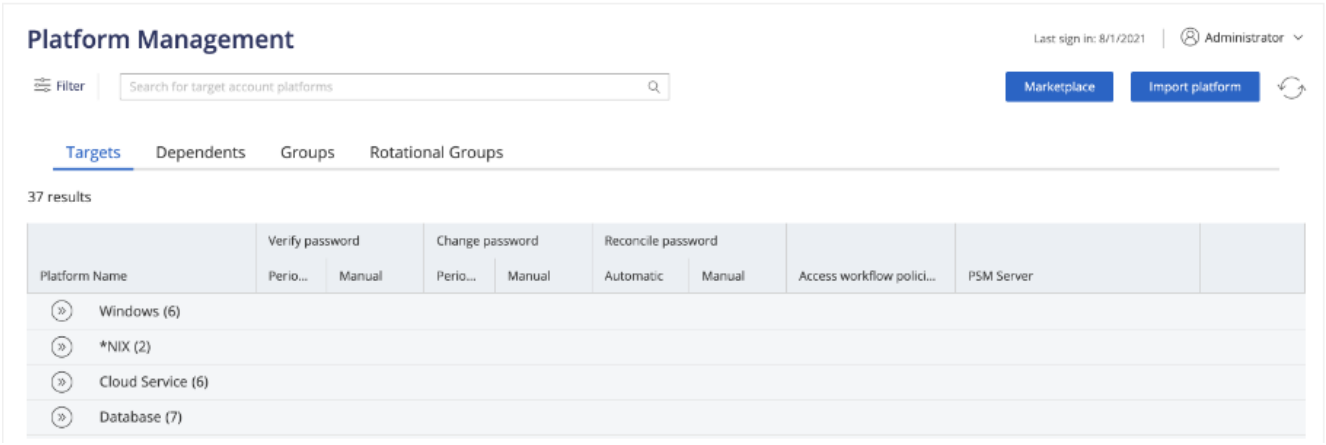


Рис. 3.14. Приклад Платформи

Політика безпеки. Головна політика пропонує централізований огляд політики безпеки та відповідності привілейованим обліковим записам в організації, одночасно дозволяючи налаштувати правила відповідності, визначені як базові для підприємства. Він налаштований із коробки та може бути використаний одразу після впровадження, забезпечуючи інтуїтивно зрозумілу, спрощену взаємодію з користувачем та розширене розуміння кінцевих результатів для адміністраторів, IT-персоналу, менеджерів та аудиторів. Рішення Privileged Access Manager

відокремлює правила політики вищого рівня та відповідності, такі як робочі процеси привілейованого доступу, керування обліковими записами та моніторинг сеансів, від технічних налаштувань, які визначають, як політика буде виконуватися на кожній платформі.

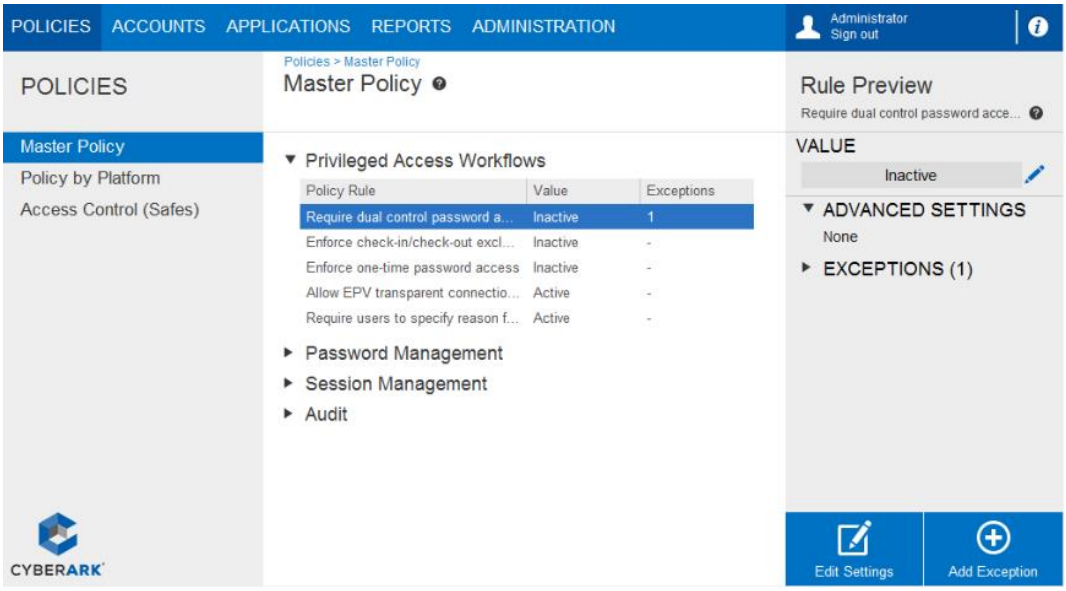


Рис. 3.15. Майстер створення політик

Налаштування доступу Just in Time до машин Windows. Бувають випадки, коли керування паролями локального адміністратора неможливо на початковому етапі розгортання. Доступ Just in Time можна використовувати як проміжний крок до повного впровадження Vaulting локальних адміністраторів. З його допомогою можна надати адміністраторам Windows на вимогу спеціальний привілейований доступ до цілей Windows протягом обмеженого періоду часу. Протягом цього часу користувачі домену можуть запитувати доступ до системи як локальний адміністратор.

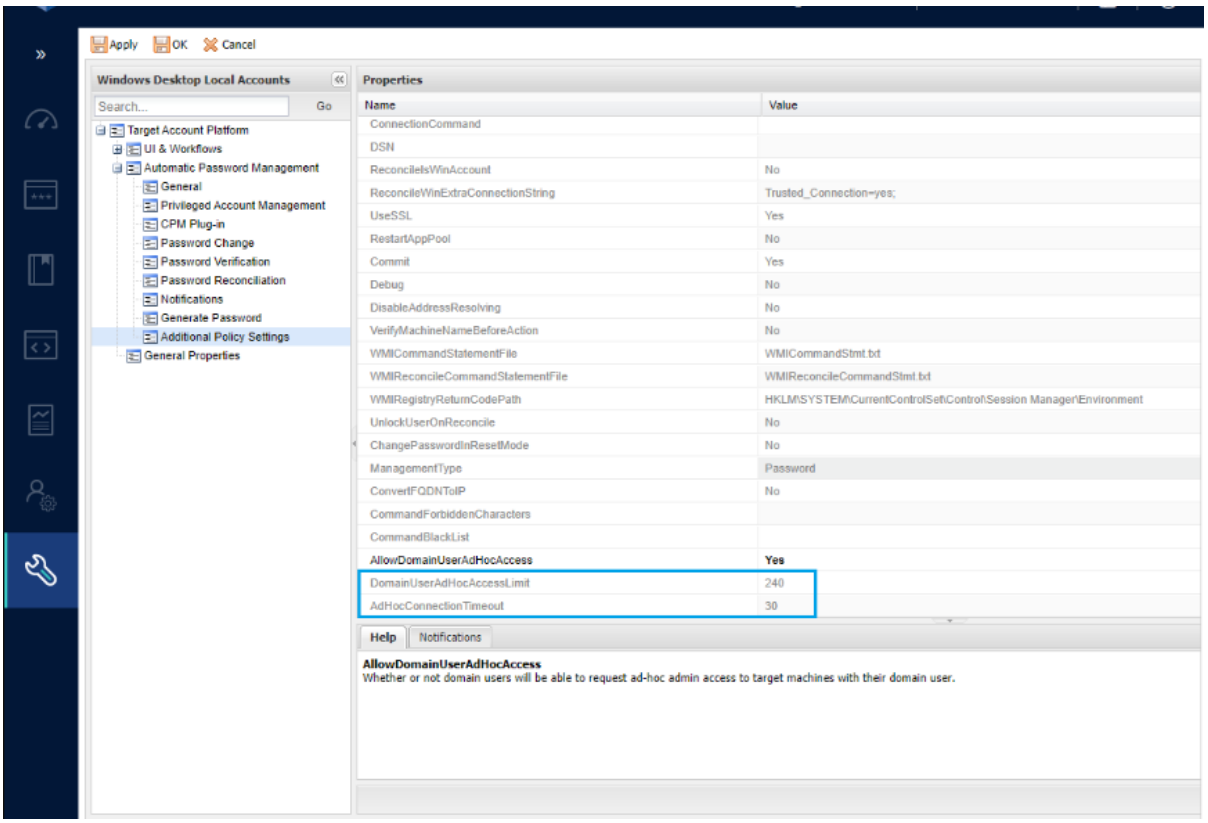


Рис. 3.16. Налаштування періоду доступу

Налаштування офлайн-доступу до цільових машин. PAM система прагне надавати безпечний безперервний доступ до облікових записів, коли необхідно в певний момент часу отримати до них доступ. Доступ до облікових записів, коли PAM офлайн, здійснюється за допомогою програми CyberArk Mobile. За допомогою CyberArk Mobile користувачі можуть отримати облікові дані для облікових записів і отримати прямий доступ до цільових систем і пристроїв. Для цього потрібно спочатку інтегрувати CyberArk Remote Access, для чого буде потрібна допомога служби підтримки CyberArk, а потім увімкнути можливість офлайн-доступу.

Рис. 3.17. Віддалені доступи

Висновки до третього розділу

PAM-система CyberArk Privileged Access Management є потужною системою з управління привілейованими користувачами та їх доступом до конфіденційної інформації, що зменшує кількість, пов'язаних з витоками даних, загроз. Система дає централізовано контролювати доступ до критичної інформації та слідкувати за діями користувачів. CyberArk PAM дає можливість автоматично керувати доступами до даних та систем, також захищає несанкціонованого використання прав доступу. Такі переваги роблять це PAM рішення необхідною частиною щодо забезпечення інформаційної безпеки в будь-якій організації.

4 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЕФЕКТИВНОГО УПРАВЛІННЯ ДОСТУПОМ ПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ

Управління привілейованим доступом протягом великого часу було складно вирішуваним завданням, через що було важко досягти належного рівня безпеки. PAM дає організаціям надійний спосіб захистити, контролювати та моніторити доступ до критично важливої інформації та ресурсів. Однак, якщо управління привілейованим доступом погано налагоджено, воно може стати серйозною проблемою і значно підвищити ризики організації.

Щоб забезпечити ефективне розгортання PAM, було розроблено, на мою думку, найкращі практики.

4.1 Використання тимчасової ескалації привілеїв

Дотримання принципу найменших привілеїв є найкращою практикою в будь-якій стратегії управління ідентифікацією та доступом (IAM). Навіть при використанні PAM привілеї слід надавати лише до необхідного рівня, а потім тимчасово підвищувати привілеї за потреби.

Створити і підтримувати конвеєр процесів, щоб визначити, коли тимчасове підвищення привілеїв є доречним. Політики, що регулюють будь-яке підвищення привілеїв, повинні включати конкретну причину, через яку воно було схвалене, а також обмежувальні атрибути, серед яких місцезнаходження, пристрій і тип операції.

4.2 Відстеження активів та привілеїв

Оскільки до корпоративної мережі додаються нові компоненти та інші активи - як санкціоновані, так і несанкціоновані - автоматизоване виявлення активів, оцінка прав власності та доступу до них має важливе значення. Методологія оцінки

також повинна мати можливість відкликати привілеї користувачів, якщо виявлено будь-яку невідповідність.

4.3 Розгортання контролю доступу на основі атрибутів

Привілеї, прив'язані до ролей та активів, були основою IAM. Нова методологія, контроль доступу на основі атрибутів (ABAC), надає компаніям новий спосіб створення політик, які встановлюють ще більш жорсткий контроль над поведінкою користувачів. На додаток до ролей та активів, ABAC включає ще два виміри: дії та середовище. Дії - серед них читання, запис, копіювання та видалення - визначають, що користувач намагається зробити з ресурсом. Середовище відноситься до ширшого контексту, де використовується ресурс, включаючи час і дату, місцезнаходження, сам пристрій і будь-які підтримувані протоколи.

4.4 Відстеження розподілу привілеїв та їх використання

Періодична оцінка налаштованих привілеїв, наданих користувачеві або організації, і порівняння їх з фактичним використанням. Наприклад, якщо користувачеві надано права на читання, створення, знищення та модифікацію хмарного сховища, але він ніколи не робив нічого, окрім читання, то повне скасування інших привілеїв або забезпечення автоматичної прив'язки цих дій до багатофакторної автентифікації значно знижує ризик. Одноразова ескалація привілеїв - наприклад, привілеї супер-адміністратора надаються її заступнику, поки вона у відпустці - відбувається, але часто не відкликається після закінчення відпустки. Моніторинг використання привілеїв попередив би адміністраторів про те, що привілеї заступника слід відкликати.

4.5 Впровадження нульової довіри

Це зміна мислення та культури, яка набуває значного поширення. Це модель, яка передбачає, що відбувся компроміс і що кожна дія оцінюється в цьому контексті. З цією метою доступ до ресурсів забороняється доти, доки користувачі та пристрої не будуть перевірені та автентифіковані.

4.6 Облік та аудит

Стандартна найкраща практика PAM полягає в тому, що всі дії користувачів повинні бути записані. Але одного лише запису недостатньо, якщо не впроваджені належні процеси аудиту. Відстеження дій корисне у випадку порушення, пов'язаного з ескалацією привілеїв. Однак, має бути впроваджений процес для регулярного перегляду записів про доступ і, за необхідності, вжиття заходів - зокрема, при порівнянні привілеїв з використанням або в середовищі з нульовою довірою.

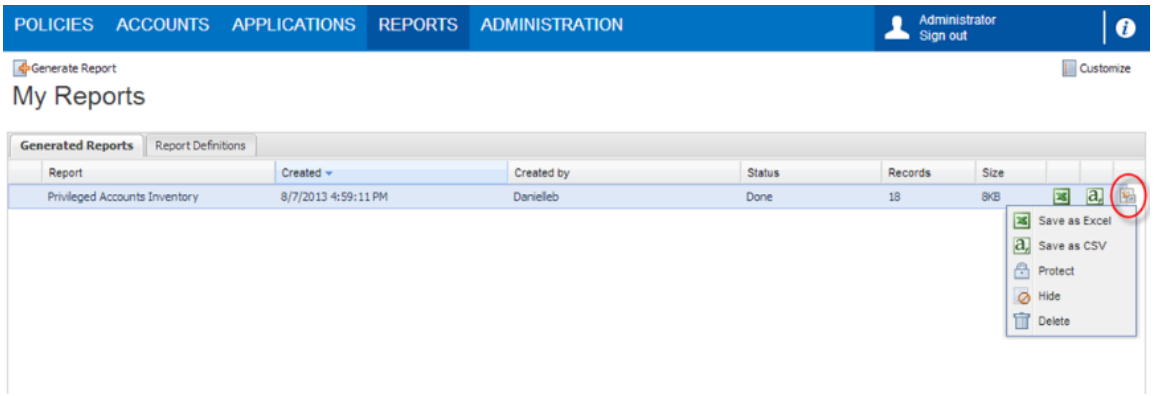


Рис. 4.1. Звіти

4.7 Моніторинг та оповіщення

Будь-яка активність, пов'язана з доступом до активів або виконанням дій, що виходять за межі призначених рівнів привілеїв, повинна генерувати сповіщення. Періодичний моніторинг рутинних дій може надати цінну інформацію про поведінкові та хронологічні зміни. Як результат, базові рівні поведінки можуть бути скориговані, щоб зменшити кількість хибних спрацьовувань і гарантувати, що фактичні відхилення від норми будуть належним чином позначені.

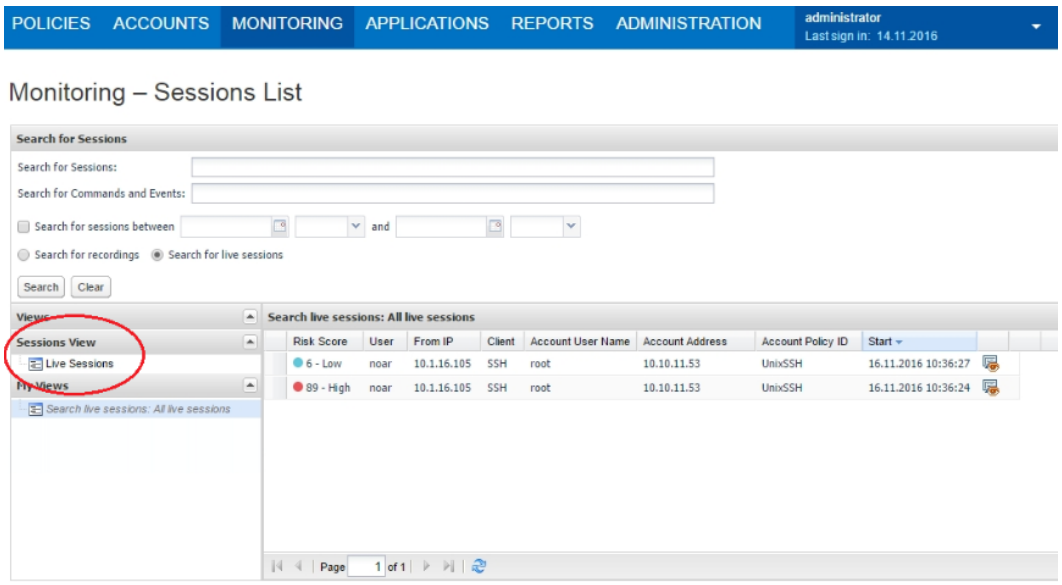


Рис. 4.2. Список активних сеансів

Висновки до четвертого розділу

Розробка рекомендацій щодо ефективного управління доступом привілейованих користувачів є однією з важливих частин для забезпечення інформаційної безпеки в організації. Якщо слідувати цим рекомендаціям, це допоможе зменшити витоки даних та ризики кібератак.

ВИСНОВКИ

По завершенню написання бакалаврської дипломної роботи можна побачити такі результати.

Було розглянуте питання що таке політика контролю доступу, з чого вона складається, як створюється, на які класи поділяється. Кожен клас політик був конкретно розглянутий та проаналізований.

Розкрито питання хто такі привілейовані користувачі, навіщо вони потрібні й наскільки їх захист важливий для інформаційної безпеки організації, де вони знаходяться.

Було визначено за допомогою якого класу рішень інформаційної безпеки можна захистити привілейованих користувачів в системі. Та було проведене дослідження ринку цих рішень, де вони порівнювалися.

Після чого серед переліку PAM систем була вибрана одна - CyberArk Privileged Access Management.

В роботі була розкрита архітектура рішення. Були показані та описані підготовчі етапи для впровадження цієї системи в корпоративну мережу.

Також в роботі були розкриті основні можливості головного адміністратора PAM системи.

По закінченню дослідження цього питання були розроблені рекомендації, які б забезпечували комплексне та ефективне управління доступом привілейованих користувачів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Samarati P., de Capitani di Vimercati S. Access Control: Policies, Models, and Mechanisms. Crema (CR), Italy : Dipartimento di Tecnologie dell'Informazione, Universit`a di Milano Via Bramante, 2001. 196 p.

https://link.springer.com/chapter/10.1007/3-540-45608-2_3

2. Jones C. The Top 10 Privileged Access Management (PAM) Solutions 2023 | Expert Insights. Expert Insights. [Електронний ресурс]. – Режим доступу: https://expertinsights.com/insights/the-top-10-privileged-access-management-pam-solutions/ (date of access: 08.05.2023).

3. JumpCloud Open Directory Platform. [Електронний ресурс]. – Режим доступу: https://jumpcloud.com/

4. Heimdal. [Електронний ресурс]. – Режим доступу: https://heimdalsecurity.com/

5. ARCON | Privileged Access Management. [Електронний ресурс]. – Режим доступу: https://arconnet.com/

6. BeyondTrust Privileged Remote Access. [Електронний ресурс]. – Режим доступу: https://www.beyondtrust.com/

7. Bravura Privilege. [Електронний ресурс]. – Режим доступу: https://www.bravurasecurity.com/

8. Broadcom Symantec Privileged Access Management. [Електронний ресурс]. – Режим доступу: https://www.broadcom.com/

9. CyberArk Privileged Access Management. [Електронний ресурс]. – Режим доступу: https://www.cyberark.com/

10. Delinea Secret Server. [Електронний ресурс]. – Режим доступу: https://delinea.com/

11. Foxpass Privileged Access Management. [Електронний ресурс]. – Режим доступу: https://www.foxpass.com/

12. One Identity Safeguard. [Електронний ресурс]. – Режим доступу: https://www.oneidentity.com/

13. CyberArk Docs. [Електронний ресурс]. – Режим доступу: https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/HomeTilesLPs/LP-Tile1.htm?tocpath=Get%20Started%7C_____0

Демонстраційні матеріали (презентація)

Розробка рекомендацій щодо управління доступом привілейованих користувачів інформаційної системи організації

Виконала студентка групи БСД-43
Яцкова Наталія

Об’єкт, предмет, мета та наукові завдання

Об’єкт дослідження - управління доступом привілейованих користувачів як складова частина забезпечення кібербезпеки корпоративної інформаційної системи.

Предмет дослідження - програмне забезпечення для управління привілейованим доступом CyberArk Privileged Access Management в корпоративній інформаційній системі.

Мета роботи - розробити рекомендації щодо ефективного управління доступом привілейованих користувачів для забезпечення інформаційної безпеки в корпоративній інформаційній системі на основі рішення CyberArk Privileged Access Management.

Завдання наукової роботи:

- Дослідження такої сутності як політика контролю доступу
- Проаналізувати місце та роль користувачів з привілейованими обліковими записами у корпоративній системі
- Проаналізувати ринок PAM рішень та обрати оптимальне рішення
- Визначити та проаналізувати основні можливості програмного продукту CyberArk Privileged Access Management

Політики контролю доступу

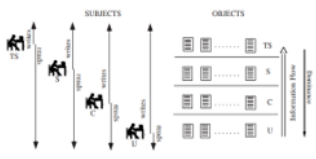
Забезпечення захисту вимагає, щоб кожен доступ до системи та її ресурсів контролювався, і щоб всі і тільки авторизовані доступи могли мати місце. Цей процес називається контролем доступу.

Політика безпеки повинна охоплювати всі різні правила, що підлягають застосуванню, і, крім того, повинна також враховувати можливі додаткові загрози, пов'язані з використанням комп'ютерної системи. Політики контролю доступу можна згрупувати в три основні класи:

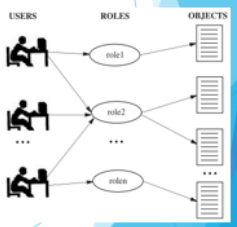
Дискреційні

	File 1	File 2	File 3	Program 1
Ann	own read write	read write		execute
Bob	read		read write	
Carl		read		execute read

Мандатні



Політики на основі ролей



Дослідження ринку PAM рішень

JumpCloud Open Directory Platform™

jumpcloud

ARCON | Privileged Access Management

Arcon

BeyondTrust Privileged Remote Access

BeyondTrust

Heimdal™ Privileged Access Management

Bravura Privilege

Bravura Security

Дослідження ринку PAM рішень

Broadcom Symantec Privileged Access Management

Symantec
A Division of Broadcom

Delinea Secret Server

Foxpass Privileged Access Management

FOXPASS

CyberArk Privileged Access Management

CYBERARK

One Identity Safeguard

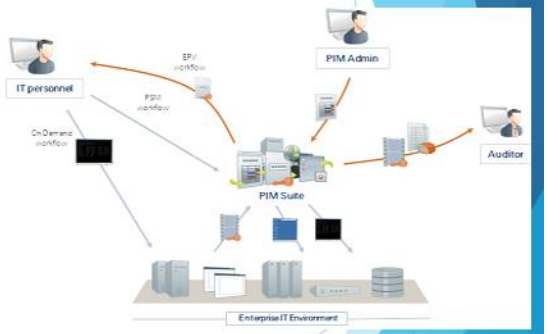
ONE IDENTITY

Архітектура CYBERARK PRIVILEGED ACCESS MANAGEMENT

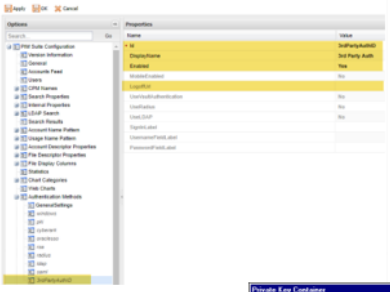
Архітектура рішення PAM складається з двох основних елементів.

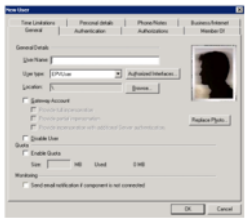
Одним з них є механізм зберігання даних.

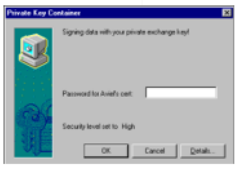
Другим елементом є інтерфейс.

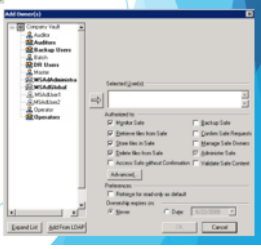


Керування користувачами

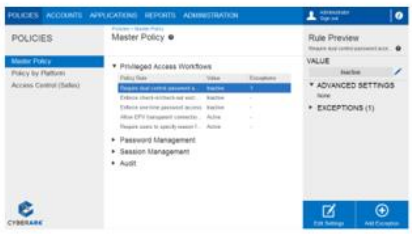


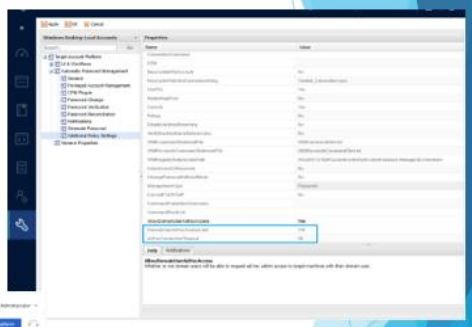


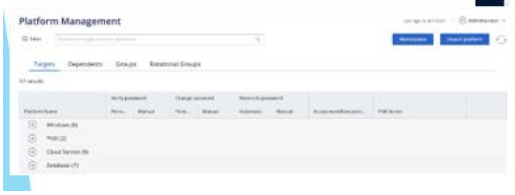




Робота з привілейованими обліковими записами

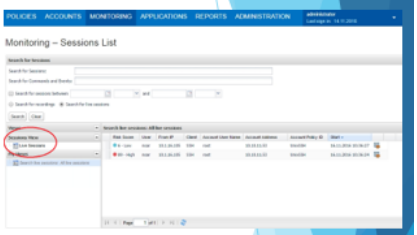


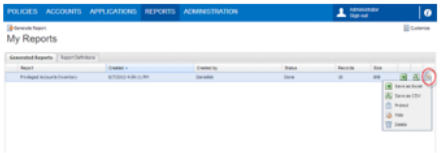




Рекомендації щодо управління доступом

- Використання тимчасової ескалації привілеїв
- Відстеження активів та привілеїв
- Розгортання контролю доступу на основі атрибутів
- Відстеження розподілу привілеїв та їх використання
- Впровадження нульової довіри
- Облік та аудит
- Моніторинг та оповіщення





Висновки за результатами роботи

Було розглянуте питання що таке політика контролю доступу.

Хто такі привілейовані користувачі, наскільки їх захист важливий для інформаційної безпеки організації.

За допомогою класу PAM рішень можна захистити привілейованих користувачів в системі.

В роботі була розкрита архітектура рішення.

Розкриті основні можливості головного адміністратора PAM системи, за допомогою яких можна управляти привілейованими користувачами.

Розроблені рекомендації, які б забезпечували комплексне та ефективне управління доступом привілейованих користувачів