

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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління привілейованим доступом інформаційної системи
організації»

зі спеціальності

125 Кібербезпека та захист інформації

(код, найменування спеціальності)

освітньо-професійної програми

Інформаційна та кібернетична безпека

(назва програми)

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

_____ Мар'яна ПЕТУХОВА

(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62

ПЕТУХОВА Мар'яна

(прізвище, ім'я)

Керівник

канд. наук з держ. упр.

СКИБУН Олександр

(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент

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

Київ 2025

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	4
ВСТУП.....	5
1 АНАЛІЗ ПРОБЛЕМИ ПРИВІЛЕЙОВАНОГО ДОСТУПУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ.....	8
1.1. Призначення та завдання привілейованого облікових записів	8
1.2. Аналіз ризиків привілейованого доступу інформаційної системи організації	11
1.3. Підходи до вирішення проблеми управління привілейованим доступом інформаційної системи організацій.....	20
1.4. Аналіз технологій управління привілейованим доступом	24
2 МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА ПРИКЛАДІ FORTIPAM	29
2.1. Архітектура FortiPAM.....	29
2.2. Функції компонентів архітектури FortiPAM.....	31
2.3. Принцип ZTNA для FortiPAM	34
3 ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА ПРИКЛАДІ FORTIPAM	40
3.1. Технологія впровадження та експлуатації FortiPam	40
3.2. Рекомендації мінімізації ризиків при впровадженні технології управління привілейованим доступом інформаційної системи організації	51

ВИСНОВКИ	56
ПЕРЕЛІК ПОСИЛАНЬ	58

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD – Active Directory

API – Application Programming Interface

DBA – Database Administrator **EMS** – Endpoint Management Server

GDPR – General Data Protection Regulation

GUI – Graphical User Interface

HIPAA – Health Insurance Portability and Accountability Act

IdP – Identity Provider

JIT – Just-In-Time

LDAP – Lightweight Directory Access Protocol

MFA – Multi-Factor Authentication

PAM – Privileged Access Management

PASM – Privileged Account and Session Management

PCI DSS – Payment Card Industry Data Security Standard

PoLP – Principle of Least Privilege

RADIUS – Remote Authentication Dial-In User Service

RBAC – Role-Based Access Control

RDP – Remote Desktop Protocol

SAML – Security Assertion Markup Language

SIEM – Security Information and Event Management

SOX – Sarbanes-Oxley Act

SSH – Secure Shell

SSO – Single Sign-On

TCO – Total Cost of Ownership

UEBA – User and Entity Behavior Analytics

ZTNA – Zero Trust Network Access

ВСТУП

Керування привілейованим доступом (РАМ) визначається як метод кібербезпеки, який захищає ідентифікаційні дані з унікальним доступом або можливостями, що перевищують можливості звичайних користувачів. Як і всі інші рішення кібербезпеки, безпека РАМ залежить від поєднання людей, процедур і технологій.

Привілейованийий доступ стосується підвищеного рівня доступу та дозволів, які мають певні користувачі або облікові записи до критично важливих систем, програм і даних в організації. Ці користувачі або облікові записи мають більші привілеї, ніж звичайні користувачі, що дозволяє їм виконувати функції та отримувати доступ до даних, до яких інші не мають доступу.

Привілейованийий доступ зазвичай надається особам, відповідальним за обслуговування та управління критично важливими системами, таким як ІТ-адміністратори, мережеві інженери та адміністратори баз даних. Цим особам потрібні підвищені привілеї для ефективного виконання своїх посадових функцій, таких як встановлення програмного забезпечення, налаштування систем та усунення несправностей.

Управління привілейованим доступом (РАМ) є важливим для безпеки даних в організаціях, оскільки воно забезпечує вирішальний рівень захисту від несанкціонованого доступу привілейованих користувачів до конфіденційних даних і критично важливих систем.

РАМ допомагає організаціям захищати дані, контролюючи та упрвляючи привілейованим доступом до критично важливих і конфіденційних систем. Вона допомагає запроваджувати суворий контроль доступу та політики, щоб гарантувати, що лише авторизовані користувачі мають доступ до привілейованих облікових записів. Це допомагає мінімізувати ризик внутрішніх загроз, зловмисних атак та несанкціонованого доступу до конфіденційних даних.

Крім того, РАМ допомагає організаціям контролювати та перевіряти активність привілейованих користувачів, дозволяючи їм виявляти та реагувати на

потенційні інциденти безпеки в режимі реального часу. Це може допомогти виявити та запобігти витокам даних та іншим інцидентам безпеки до їх виникнення.

РАМ також допомагає організаціям дотримуватися вимог нормативних актів щодо безпеки даних. Багато нормативних актів щодо конфіденційності та безпеки даних вимагають від організацій запровадити суворий контроль за привілейованим доступом до конфіденційних даних. РАМ надає основу, яка допомагає організаціям дотримуватися цих вимог та демонструвати відповідність.

Таким чином, дослідження питань управління привілейованим доступом до інформаційної системи організації на прикладі FortyРАМ забезпечить мінімальні ризики щодо витоку даних та несанкціонованого доступу.

Об'єкт дослідження – управління привілейованим доступом до інформаційної системи організації.

Предмет дослідження – технологія управління привілейованим доступом до інформаційної системи організації на прикладі FortyРАМ.

Метою роботи – є дослідження технології управління привілейованим доступом до інформаційної системи організації та розробка рекомендацій щодо використання стратегії зменшення ризиків при її використанні.

Наукові завдання:

дослідити сутність проблеми управління привілейованим доступом до інформаційної системи організації;

проаналізувати підходи до вирішення проблеми управління привілейованим доступом до інформаційної системи організації;

проаналізувати існуючі технології управління привілейованим доступом до інформаційної системи організації;

проаналізувати методи та засоби управління привілейованим доступом до інформаційної системи організації на прикладі FortyРАМ;

розробити рекомендації щодо впровадження та експлуатації технології управління привілейованим доступом до інформаційної системи організації на прикладі FortyРАМ.

Методи дослідження: опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, практичне використання засобів захисту віддалених користувачів.

Практичне значення одержаних результатів. запропоновано рекомендації щодо використання стратегії зменшення ризиків при використанні технології управління привілейованим доступом до інформаційної системи організації.

Апробація результатів.

Петухова М.О., Мазур А.Т. Технологія управління привілейованим доступом: порівняння рішень. *Актуальні проблеми кібербезпеки:* матеріали всеукраїнської наук.-практ. конф., м. Київ: ДУІКТ, 29 жовт. 2025р. Київ. С. 21-23.

1 АНАЛІЗ ПРОБЛЕМИ ПРИВІЛЕЙОВАНОГО ДОСТУПУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Призначення та завдання привілейованого облікових записів

Управління привілейованим доступом допомагає організаціям керувати та захищати доступ до своїх найважливіших систем, програм і даних, які зазвичай зарезервовані для привілейованих облікових записів. Привілейовані облікові записи мають підвищені дозволи та можливості, що дозволяє цим користувачам виконувати різні адміністративні завдання, отримувати доступ до конфіденційної інформації та вносити зміни, які звичайні користувачі не можуть.

РАМ працює через поєднання людей, процесів і технологій, що дозволяє організаціям захищати свої критично важливі активи, забезпечуючи суворий контроль над тим, хто має доступ до привілейованих облікових записів і як вони можуть їх використовувати. Як результат, організації можуть мінімізувати ризик несанкціонованого доступу до конфіденційних систем і даних, забезпечуючи надійний підхід до управління привілейованими обліковими записами та гарантуючи, що їх можуть використовувати лише уповноважені особи [1].

Керування привілейованим доступом працює шляхом забезпечення процедур безпеки та контролю, які обмежують та контролюють доступ до привілейованих облікових записів. Воно складається з методів безпечної автентифікації, авторизації та аудиту, які допомагають забезпечити доступ до конфіденційних систем і даних лише уповноваженим особам. Крім того, технології РАМ підтримують моніторинг і запис сеансів, що дозволяє вашим ІТ-командам та командам безпеки спостерігати та аналізувати поведінку привілейованих користувачів.

РАМ ґрунтується на принципі найменших привілеїв, який гарантує, що користувачам надаються лише ті рівні доступу, які необхідні для виконання їхніх посадових обов'язків. Цей принцип широко визнаний як найкраща практика

кібербезпеки та слугує вирішальним заходом для захисту привілейованого доступу до ваших цінних даних та ресурсів.

Привілеї стосуються підвищених дозволів та можливостей, наданих користувачам, програмам або процесам в інформаційній системі організації. Ці дозволи дозволяють користувачам або процесам отримувати доступ та виконувати певні дії з критично важливими ресурсами, такими як файли, каталоги, бази даних, конфігурації мережі або адміністративні налаштування.

Приклади привілеїв включають права на читання, запис, виконання, зміну, видалення, створення та адміністрування. Привілеї є важливими для завдань системного адміністрування та управління, але можуть становити ризики для безпеки, якщо ними не керувати належним чином.

Привілейовані облікові записи – це облікові записи користувачів або службові облікові записи, які мають підвищені дозволи, вищі за дозволи звичайних облікових записів користувачів. Ці облікові записи мають адміністративні права та можуть виконувати критично важливі дії, такі як встановлення програмного забезпечення, зміна системних налаштувань, доступ до конфіденційних даних та керування обліковими записами користувачів.

Керування привілейованими обліковими записами контролює весь життєвий цикл облікових записів із підвищеними правами доступу, від створення до виведення їх з експлуатації [2].

Привілейовані облікові записи часто стають ціллю зловмисників, оскільки їх компрометація забезпечує широкий контроль над системами та даними організації. Тому контроль та захист привілейованих облікових записів є ключовими аспектами РАМ. Деякі приклади привілейованих облікових записів [1, 2] включають (рис.1.1):

Права адміністратора. Користувачі з правами адміністратора мають право налаштовувати, керувати та змінювати системні параметри, встановлення програмного забезпечення та облікові записи користувачів.

Root-доступ: У Unix-подібних операційних системах «root» – це обліковий запис суперкористувача, який має необмежений доступ до всіх системних ресурсів і файлів.

Доступ адміністратора бази даних (DBA - Database administrator). DBA керують базами даних та контролюють їх, зокрема створюють, змінюють та видаляють структури та дані бази даних.

Права рівня програми. Деяким програмам потрібні вищі права для виконання певних завдань, таких як доступ до конфіденційних даних або виконання операцій на рівні системи.

Права на налаштування мережі. Користувачі з цими правами можуть налаштовувати параметри мережі, маршрутизатори, брандмауери та інші конфігурації, пов'язані з мережею.

Керування ключами шифрування. Ці користувачі можуть керувати ключами шифрування, які захищають конфіденційні дані організації, та контролювати їх.

Контроль фізичного доступу. Привілеї можуть також поширюватися на фізичний доступ, дозволяючи певним особам входити до захищених зон (наприклад, до центру обробки даних) або взаємодіяти з апаратними компонентами.

Доступ до фінансових систем. Зазвичай це співробітники фінансових та бухгалтерських відділів, ці користувачі мають доступ до фінансового програмного забезпечення та систем для обробки транзакцій та виконання своїх посадових функцій.

Керування хмарною інфраструктурою. Адміністратори хмари мають права керувати хмарними ресурсами, віртуальними машинами, сховищами та мережевими компонентами в хмарних середовищах.

Середовища розробки та виробництва. Розробники можуть мати різні рівні доступу в середовищах розробки та виробництва, що дозволяє їм створювати, тестувати та розгортати програмне забезпечення.

Привілейовані облікові дані – це інформація для автентифікації, пов'язана з привілейованими обліковими записами. Вони включають імена користувачів, паролі, ключі API, криптографічні ключі, сертифікати та будь-які інші облікові дані, необхідні для доступу та роботи з привілейованими обліковими записами.

Привілейовані облікові записи та їхні ролі

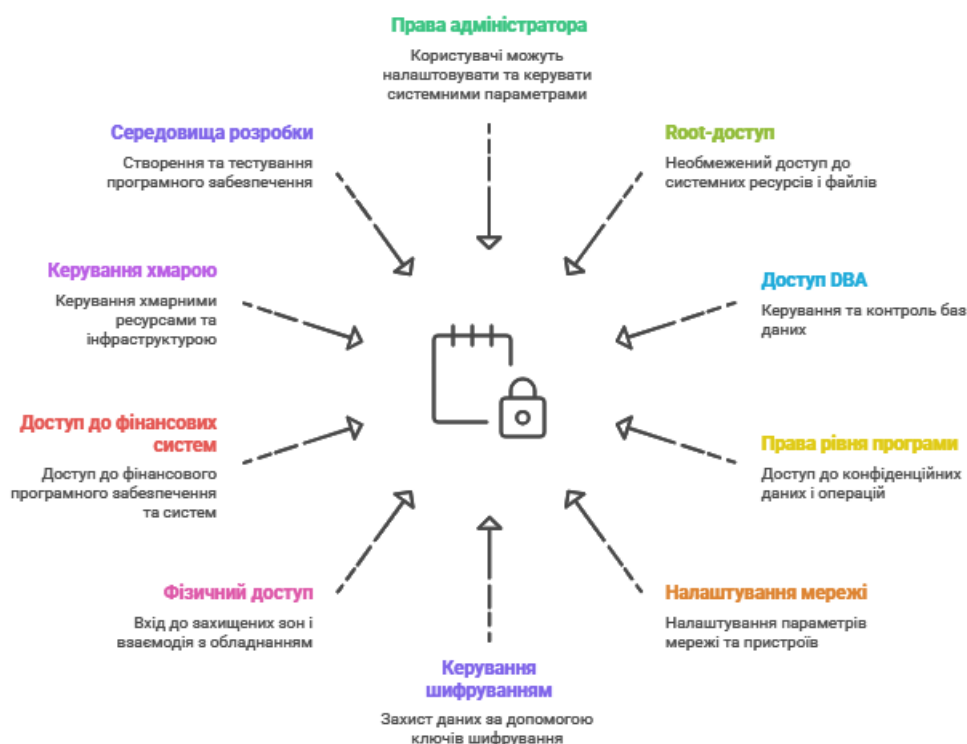


Рис.1.1. Привілейовані облікові записи

Належне управління та захист привілейованих облікових даних є життєво важливими для запобігання несанкціонованому доступу та забезпечення того, щоб лише ваші уповноважені співробітники могли використовувати їх за необхідності.

1.2. Аналіз ризиків привілейованого доступу інформаційної системи організації

Рішення для керування привілейованим доступом мають вирішальне значення для захисту привілейованих облікових записів, що існують у локальних та хмарних середовищах компаній. Привілейовані облікові записи часто містять ключ до конфіденційної та чутливої інформації, яка може завдати величезної шкоди організаціям, якщо потрапить у чужі руки [3-5].

Привілейовані облікові записи особливо вразливі через такі ризики та проблеми:

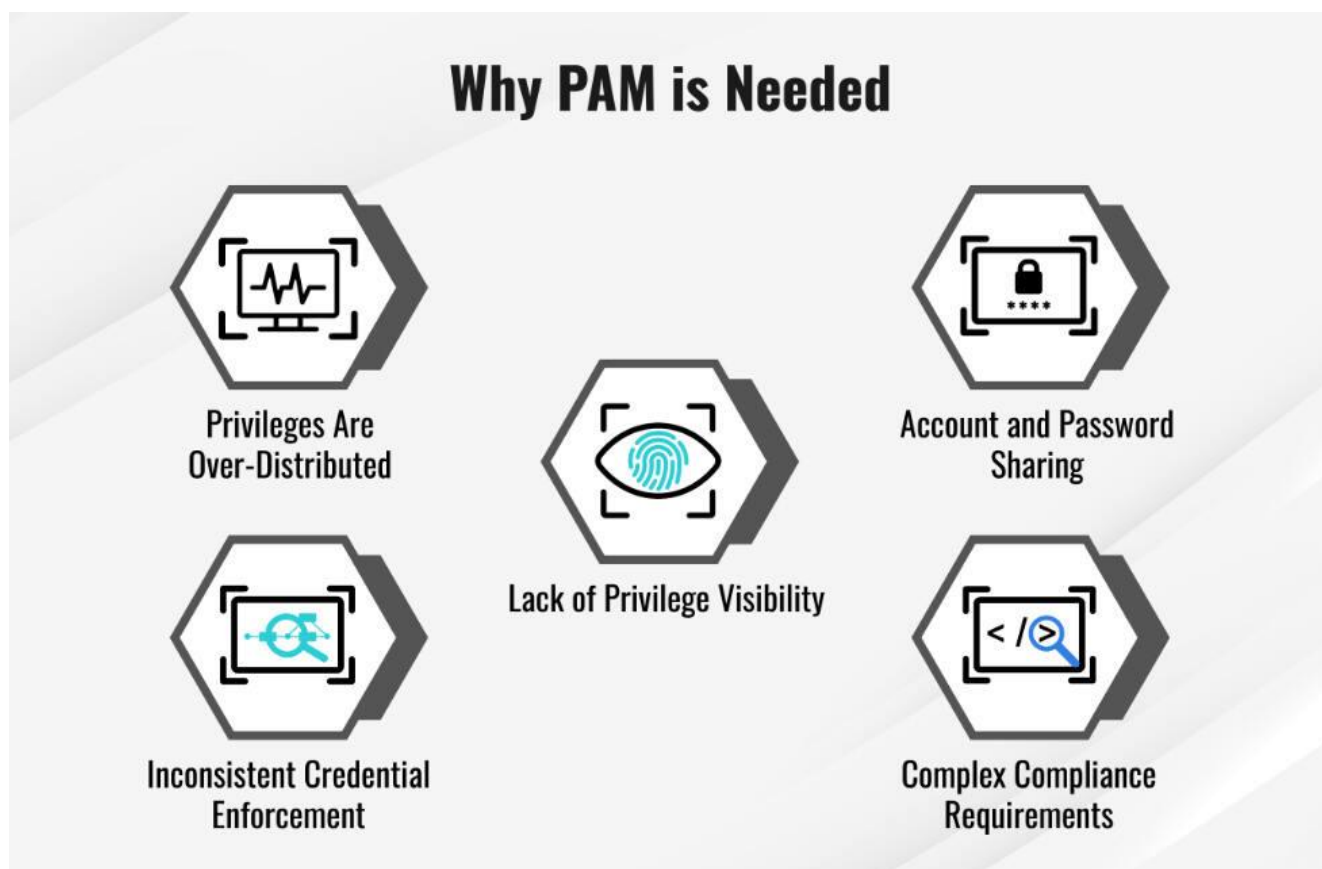


Рис. 1.2. Ризики привілейованих облікових записів

Привілеї надмірно розподілені

Організаціям легко надмірно розподілити права облікового запису для ресурсів, які їх не потребують. Деякі користувачі також накопичують нові права або зберігають права, які їм більше не потрібні, коли змінюється їхня посада. Це надлишок прав, на додаток до зростання впровадження хмарних технологій та цифрової трансформації, може призвести до розширення поверхні атаки організації.

Наявність прав адміністратора облікового запису, що перевищують ті, що потрібні користувачам, збільшує ризик зараження шкідливим програмним забезпеченням та крадіжки паролів хакерами. Це дозволяє неавторизованим особам отримати доступ до всіх прав в обліковому записі, включаючи всі дані на зараженому комп'ютері, або розпочати атаку на інші комп'ютери чи сервери в мережі.

Спільний доступ до облікового запису та пароля

Привілейовані облікові дані для таких служб, як Адміністратор Windows, часто використовуються спільно, щоб обов'язки та робочі навантаження можна було змінювати за потреби. Але спільне використання паролів може унеможливити пов'язування зловмисних дій з одним користувачем, що створює проблеми з аудитом, відповідністю вимогам та безпекою.

Відсутність видимості привілеїв

Для організацій, що розвиваються, поширеною є ситуація, коли по всіх системах розкидані старі привілейовані облікові записи, які більше не використовуються. Наприклад, облікові записи колишніх співробітників можуть бути заблоковані, але при цьому зберігатимуть привілейовані права доступу. Ці неактивні облікові записи вразливі для хакерів і можуть забезпечити їм бекдор у мережі та системи організацій.

Тому організаціям необхідно зберігати повну видимість рівнів доступу до своїх облікових записів та видаляти ті, що мають непотрібні привілеї.

Непослідовне застосування облікових даних

Ізоляція даних в організаціях може призвести до непослідовного застосування привілейованих облікових записів та управління обліковими даними. Великі організації можуть мати тисячі або навіть мільйони привілейованих облікових записів, що ІТ-командам неможливо керувати вручну. Крім того, через таку велику кількість облікових записів, які потрібно керувати, ймовірно виникнуть скорочення ресурсів, а облікові дані можуть бути повторно використані в кількох облікових записах. Ці фактори ставлять під загрозу безпеку всіх облікових записів у системі.

Складні вимоги до дотримання вимог

Безпека РАМ дозволяє керувати ризиками, пов'язаними з програмами, мережевими пристроями та системами, а також допомагає організаціям фіксувати всі дії, пов'язані з критичною інфраструктурою. Це ідеально підходить для створення більш зручного для аудиту ІТ-середовища.

Привілейовані облікові записи є головними цілями для зловмисників через їхні підвищені дозволи та доступ до конфіденційних даних. Рішення РАМ

допомагають зменшити ці ризики, забезпечуючи прозорість та контроль над тим, хто, до чого отримує доступ, коли та як, що робить ці платформи критично важливим компонентом захисту найцінніших ресурсів організації.

Розглянемо основні ризики.

1. Підвищений ризик витоку даних

Витоки даних трапляються, коли неавторизовані особи отримують доступ до конфіденційної інформації організації. Без РАМ організації стикаються з підвищеним ризиком, оскільки привілейовані облікові записи, такі як ті, що належать системним адміністраторам та службовим обліковим записам, часто залишаються без нагляду та керування, що робить їх головними цілями для кіберзлочинців. Якщо привілейований обліковий запис скомпрометовано, кіберзлочинці можуть переміщатися по мережі, підвищуючи привілеї для доступу до критично важливих систем і даних. Потрапивши всередину, вони можуть викрасти, витікати або продавати ці дані в даркнеті [6].

В результаті, організація може зазнати шкоди репутації, що призведе до втрати клієнтів та бізнес-можливостей. Крім того, вона може зіткнутися з юридичними наслідками та фінансовими збитками, включаючи штрафи, судові позови та витрати на відновлення [6].

Яскравим прикладом є витік даних AT&T у 2024 році, коли дані, що зберігалися на сторонній хмарній платформі, були погано захищені. В результаті особиста інформація 7,6 мільйона поточних та 65,4 мільйона колишніх облікових записів AT&T була викрита та опублікована в даркнеті. AT&T не лише стикається з триваючим судовим позовом, але й зі значною шкодою для своєї репутації та втратою довіри клієнтів [6].

РАМ-рішення знижує ризик витоку даних, надаючи такі можливості:

Сховище облікових даних: РАМ забезпечує безпечне, зашифроване сховище для зберігання привілейованих облікових даних. Це допомагає організаціям запобігти розкриттю або небезпечному поширенню облікових даних та обмежує доступ лише авторизованим користувачам.

Керування привілейованими сесіями: РАМ надає організаціям можливість записувати та контролювати привілейовані сесії. Ці записи можна переглянути після інциденту безпеки, щоб визначити, хто до чого мав доступ і коли. Це також допомагає запобігти потенційним порушенням безпеки та зловживанню внутрішніми загрозами, дозволяючи організаціям виявляти підозрілу активність та забезпечувати відповідальність, оскільки кожен дію можна простежити до відповідального користувача.

Принцип найменших привілеїв (PoLP - Principle of Least Privilege). РАМ дозволяє організаціям забезпечити доступ з найменшими привілеями, надаючи користувачам лише ті дозволи, які необхідні для їхніх ролей, і лише на той час, коли вони їм потрібні. Це обмежує потенційний вплив у разі компрометації облікового запису.

2. Вплив внутрішніх загроз

Внутрішні загрози – це кіберризики, що виникають всередині організації, зазвичай стосуються співробітників, підрядників або партнерів, які мають авторизований доступ до критично важливих систем і даних. Ці загрози можуть бути зловмисними, коли інсайдер навмисно завдає шкоди, або ненавмисними, що виникають внаслідок недбалості чи людської помилки. Без РАМ організації не мають прозорості та контролю над привілейованим доступом. Це створює прогалину в безпеці, яка полегшує інсайдерам використання неперевіраних привілеїв без виявлення. Внутрішні загрози особливо небезпечні, оскільки вони походять від довірених користувачів, які мають прямий доступ до конфіденційних систем і даних, що дозволяє їм легко обходити стандартні засоби контролю безпеки [6].

РАМ допомагає зменшити внутрішні загрози, надаючи наступне:

Моніторинг сесій. РАМ надає організаціям можливість моніторити привілейовані сесії в режимі реального часу. Це дозволяє виявляти підозрілу поведінку та вживати заходів за потреби. Кожна дія пов'язана з певним користувачем для забезпечення підзвітності, що запобігає зловживанню користувачами своїми привілеями [6].

Детальний контроль доступу: РАМ дозволяє організаціям визначати та забезпечувати контроль доступу, щоб користувачі мали доступ лише до тих ресурсів, які їм потрібні для виконання їхніх ролей. Це мінімізує кількість користувачів з підвищеним рівнем доступу та зменшує поверхню атаки для внутрішніх загроз.

Сповіщення в режимі реального часу: Найкращі рішення РАМ допомагають організаціям налаштувати сповіщення про підозрілу активність, таку як невдалі спроби входу, незвичайні дії адміністратора або тривалі сесии. Ці сповіщення надають ІТ-командам інструменти для швидкого розслідування та реагування на потенційні внутрішні загрози.

3. Відсутність забезпечення найменших привілеїв

Принцип найменших привілеїв гарантує, що користувачі мають лише мінімальний рівень доступу, необхідний для виконання своєї роботи. Без РАМ організаціям важко забезпечити дотримання цього принципу, оскільки їм бракує інструментів для точного контролю, моніторингу та обмеження привілейованого доступу. Це часто призводить до надмірного доступу, коли користувачі можуть отримувати доступ до систем або даних, не пов'язаних з їхньою роллю, або до постійного доступу, коли підвищені дозволи залишаються чинними ще довго після того, як вони знадобляться. Обидві ситуації створюють ризики для безпеки. Користувач із зайвими привілеями може навмисно чи випадково отримати доступ до конфіденційних систем або зловживати своїми правами. Недотримання PoLP також розширює поверхню для атаки. Коли доступ не контролюється жорстко, командам безпеки стає важче виявити зловживання [6].

РАМ підтримує забезпечення дотримання PoLP, надаючи організаціям можливість:

Встановлення детального контролю доступу: РАМ надає організаціям інструменти для впровадження контролю доступу на основі ролей (RBAC), що дозволяє визначати доступ на основі ролей. Це гарантує, що користувачі обмежені лише тими дозволами, які їм потрібні, та зменшує ризик надмірного доступу.

Впровадження доступу Just-In-Time (JIT): РАМ дозволяє тимчасове підвищення привілеїв лише за потреби. Після завершення завдання доступ може бути автоматично скасовано, щоб зменшити вікно впливу. Це гарантує, що користувачі матимуть мінімальний обсяг доступу, необхідний у будь-який момент часу, мінімізуючи можливість зловживання привілеями [6].

Запис та моніторинг сеансів: РАМ записує та контролює всі привілейовані сеанси в режимі реального часу. Такий рівень видимості дозволяє організаціям перевіряти, чи виконують користувачі лише дії в межах дорученого їм завдання.

4. Невідповідність вимогам та проблеми з аудитом

Такі нормативні акти, як HIPAA, PCI DSS, FISMA та SOX, вимагають від організацій впровадження суворого контролю доступу, щоб обмежити непотрібний доступ до конфіденційних даних та забезпечити відповідність вимогам. Багато з цих стандартів також вимагають можливості аудиту, які відстежують та реєструють доступ до критично важливих систем. Журнали аудиту є важливими для демонстрації того, що контроль доступу працює належним чином. Без рішення РАМ організації часто мають труднощі з послідовним забезпеченням контролю доступу та не мають прозорості, необхідної для створення повних і точних журналів аудиту. Це може призвести до прогалин у документації, що ускладнює доведення відповідності та збільшує ризик штрафів, оштрафів та репутаційної шкоди [6].

РАМ підтримує зусилля з дотримання вимог та спрощує аудит, дозволяючи організаціям:

Ведення детальних журналів аудиту. РАМ реєструє всю привілейовану активність та фіксує, хто, до чого мав доступ, коли та які дії було виконано. Ці записи допомагають організаціям продемонструвати, що доступ належним чином контролюється та відповідає вимогам відповідності.

Запис та перегляд привілейованих сесій. РАМ може надавати повні записи сесій, щоб дати ІТ-командам та командам з дотримання вимог чітке уявлення про те, як здійснювався доступ до систем. Ці записи можуть слугувати доказами під час аудитів.

Забезпечення мінімального рівня доступу. РАМ допомагає застосовувати RBAC, щоб забезпечити користувачам лише мінімальний необхідний рівень доступу. Це вимога більшості регуляторних стандартів, включаючи HIPAA, PCI DSS та SOX [6].

5. Обмежена видимість та контроль

Організаціям потрібна повна прозорість та контроль над доступом до конфіденційних даних, щоб дотримуватися вимог та зменшувати ризики безпеки. Без РАМ важко відстежувати, хто, коли та з якою метою мав доступ до яких систем. Така відсутність аналітики створює сліпі зони, що ускладнює своєчасне виявлення та реагування на підозрілу активність. В результаті загрози можуть залишатися непоміченими, журнали аудиту можуть бути неповними, а дотримання вимог стає складнішим. Без проактивного контролю організації змушені реагувати на інциденти після того, як вони трапляються – часто занадто пізно, щоб запобігти серйозній шкоді [6].

РАМ допомагає усунути ці прогалини, надаючи організаціям інструменти для:

Моніторинг сеансів у режимі реального часу: організації можуть спостерігати та записувати привілейовані сеанси в міру їх виникнення. Це дає змогу негайно реагувати на підозрілу або несанкціоновану активність [6].

Керування активними сесіями. РАМ надає адміністраторам можливість призупиняти, блокувати або завершувати активні привілейовані сесії. Це забезпечує організаціям належний нагляд і можливість швидко втручатися у разі виявлення підозрілої активності [6].

Інтеграція з інструментами управління інформацією та подіями безпеки (SIEM). РАМ підтримує пересилання журналів на платформи SIEM для глибшого аналізу. Це розширює видимість та підтримує проактивне виявлення загроз у всій організації.

6. Операційна неефективність та людські помилки

Організації без РАМ більш вразливі до операційної неефективності та людських помилок. ІТ-команди та команди безпеки часто покладаються на ручні

процеси для відстеження та управління привілейованим доступом, які є трудомісткими та схильними до помилок. Такий ручний підхід ускладнює управління привілейованим доступом і часто призводить до неправильних налаштувань, забутих облікових даних та застарілих дозволів – все це створює значні вразливості безпеки. Відсутність автоматизації також може затримати надання або скасування доступу. Ці затримки не лише уповільнюють бізнес-операції, але й збільшують ризик внутрішнього зловживання та зовнішніх атак [6].

РАМ допомагає організаціям зменшити операційні накладні витрати та людські помилки, підтримуючи:

Автоматизація керування обліковими даними. РАМ надає інструменти для автоматизації обміну та ротації привілейованих облікових даних. За умови правильного налаштування це зменшує ручну роботу та допомагає запобігти забуттю або застарілим обліковим даним [6].

Робочі процеси надання та скасування надання користувачам. РАМ може інтегруватися з системами ідентифікації, такими як Система міждоменного керування ідентифікацією, для оптимізації створення, оновлення та видалення облікових записів користувачів у критично важливих системах. За умови правильного впровадження це допомагає забезпечити користувачам правильний рівень доступу під час адаптації, зміни ролей або скасування надання послуг. Ці інструменти усувають ризик надмірного надання послуг, яке часто спричиняється ручними процесами [6].

Безпечне тунелювання: РАМ підтримує зашифровані з'єднання для зменшення ризику та усунення необхідності ручного налаштування мережі. Це спрощує безпечний доступ до чутливих систем та допомагає обмежити ризик несанкціонованого доступу [6].

7. Вищі витрати після порушення

Фінансовий вплив витоку даних часто значно перевищує вартість впровадження РАМ-рішення. За даними IBM, середня світова вартість витоку даних у 2024 році становила 4,88 мільйона доларів. Ця цифра включає такі витрати,

як очищення, відновлення, юридичні витрати, штрафи регуляторних органів, простої та втрату клієнтів (рис.1.3).

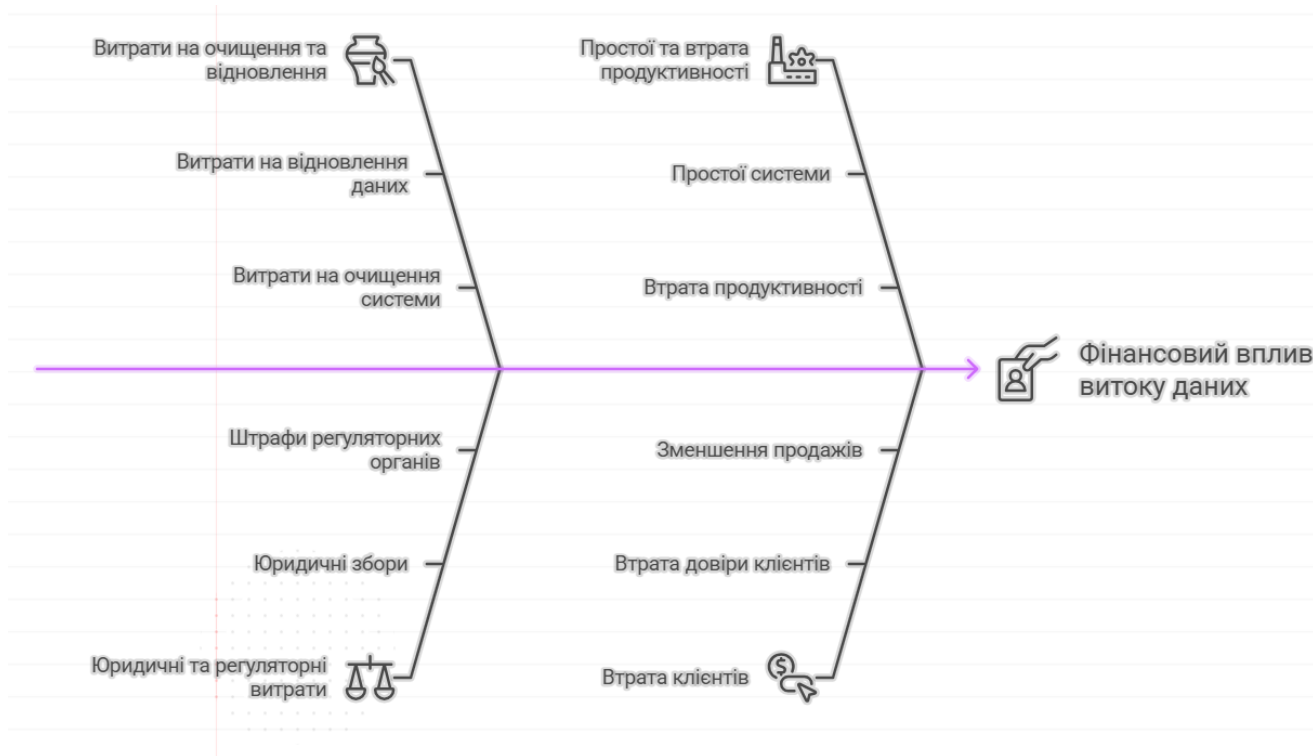


Рис.1.3. Аналіз фінансового впливу витоку даних

Витрати можуть швидко накопичуватися, особливо коли йдеться про конфіденційні дані, такі як фінансові записи або персональна інформація клієнтів (РІІ). Замість того, щоб боротися з наслідками витоку, організації повинні зосередитися на запобіганні несанкціонованому доступу шляхом впровадження РАМ-рішення [7].

Отже, РАМ є технологією, яка може вирішити проблеми інформаційної системи організації щодо відповідності нормативним вимогам та контролю облікових записів для зменшення ризиків кібербезпеки.

1.3. Підходи до вирішення проблеми управління привілейованим доступом інформаційної системи організацій

Очікується, що до 2030 року обсяг світового ринку рішень для управління привілейованим доступом досягне 16,9 мільярда доларів, що зростатиме на 21,1% у середньому протягом прогнозованого періоду.

Керування ідентифікацією є найбільш поширеним рішенням у сфері управління привілейованим доступом завдяки можливостям управління ідентифікацією адмініструвати, контролювати та моніторити доступ до важливих організаційних ресурсів. Отже, очікується, що до 2030 року управління ідентифікацією займе понад 45% ринку. Завдяки цьому рішення організації можуть надавати користувачам своєчасний привілейований доступ до ресурсів та контролювати, що ці користувачі роблять зі своїм доступом (рис 1.4). Зростаючі стандарти захисту даних, такі як Загальний регламент про захист даних (GDPR) та Закон про перенесення та підзвітність медичного страхування (HIPAA), є причиною зростання IDaaS (ідентифікація як послуга). Через ці обмеження різні фірми починають вживати додаткових заходів для захисту профілів співробітників, постачальників та кінцевих користувачів. [7]

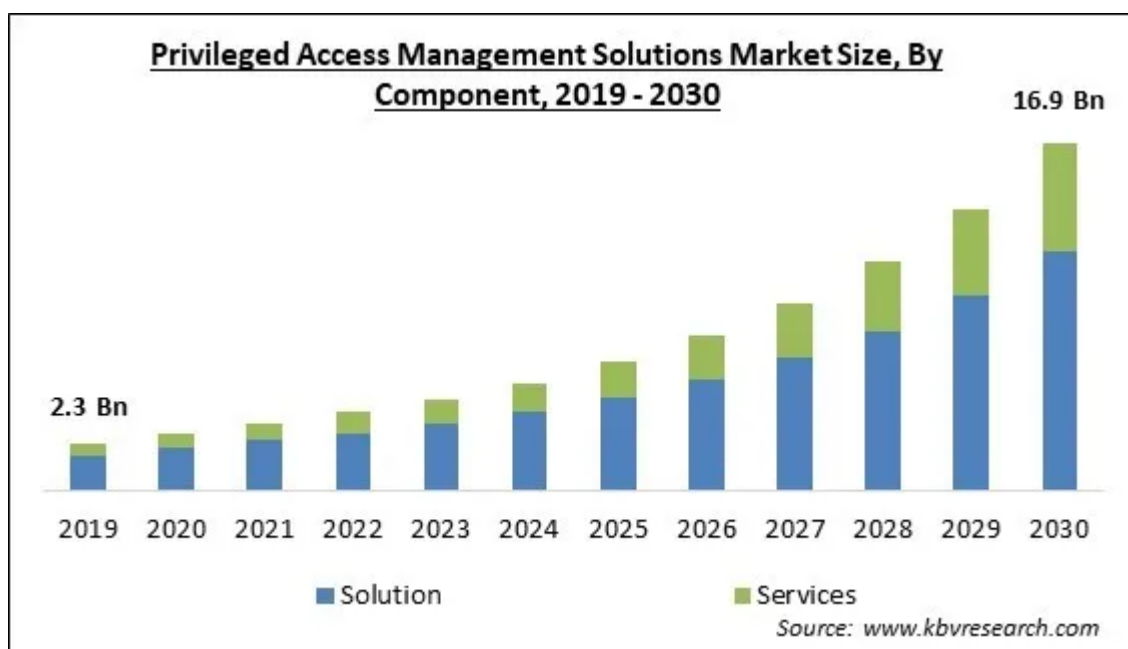


Рис.1.4. Статистика PAM рішень на ринку[7]

Основними стратегіями, яких дотримуються учасники ринку, є запуск продуктів як ключова стратегія розвитку, щоб йти в ногу зі зміною потреб кінцевих користувачів. Наприклад, у березні 2023 року Delinea оголосила про запуск платформи Delinea, рішення для контролю доступу з привілеями, яке використовується для забезпечення наскрізної видимості та гнучкої безпеки. Нова платформа сумісна з секретним сервером та безпечною службою віддаленого

доступу без VPN. Крім того, у березні 2022 року Hitachi ID, тепер відома як Bravura Security, Inc, оголосила про запуск Hitachi ID Bravura Safe для своєї Hitachi ID Bravura Security Fabric. Hitachi ID Bravura Safe надає засоби керування секретними файлами організації, що допомагає захистити дані організації [6].

РАМ пропонує численні переваги для організацій будь-якого розміру:

Посилена безпека. РАМ посилює безпеку, контролюючи доступ до критично важливих систем і конфіденційних даних. Він захищає від несанкціонованого доступу, внутрішніх загроз і зовнішніх атак.

Дотримання вимог. РАМ допомагає організаціям дотримуватися нормативних вимог, таких як HIPAA , PCI DSS та GDPR , шляхом забезпечення суворого контролю доступу та надання журналів аудиту.

Зниження ризику. РАМ мінімізує ризик витоків даних та операційних збоїв, забезпечуючи мінімальні привілеї та моніторинг привілейованої діяльності. Це обмежує вплив скомпрометованих облікових записів.

Підвищена ефективність. РАМ оптимізує ІТ-процеси та зменшує адміністративні накладні витрати шляхом централізації управління привілейованими обліковими записами.

Спрощені операції. РАМ спрощує операції безпеки та зменшує складність управління привілейованим доступом, підвищуючи загальну ефективність.

Можна виділити сім основних найкращих практик для підвищення безпеки та запобігання несанкціонованому доступу з використанням РАМ.

Суворий контроль доступу. Застосовуйте строгу автентифікацію, таку як багатофакторна автентифікація (MFA), та принцип найменших привілеїв. Надавайте доступ лише тим користувачам, хто цього потребує.

Регулярні перевірки дозволів. Регулярно перевіряйте та оновлюйте дозволи користувачів. Видаляйте доступ, який більше не потрібен, щоб мінімізувати потенційні ризики.

Ретельні перевірки. Проводьте регулярні перевірки привілейованої діяльності. Це допомагає виявляти підозрілу поведінку та забезпечує відповідальність.

Керування паролями. Впроваджуйте надійні політики паролів та забезпечуйте регулярну зміну паролів для привілейованих облікових записів. Розгляньте можливість використання сховища паролів.

Моніторинг сесій. Моніторинг та запис привілейованих сесій для виявлення шкідливої діяльності та реагування на неї в режимі реального часу.

Управління вразливостями. Оновлюйте системи та програмне забезпечення останніми оновленнями безпеки, щоб мінімізувати вразливості, які можуть використати зловмисники.

Навчання з питань безпеки. Навчайте користувачів найкращим практикам безпеки та важливості захисту привілейованих облікових даних.

Визначимо основні кроки впровадження РАМ для організації безпечного привілейованого доступу (рис.1.5).



Рис.1.5. Кроки впровадження РАМ

Впровадження РАМ може здатися складним, але поетапний підхід допомагає забезпечити безперебійне та успішне розгортання [6].

1. Оберіть правильне рішення. Оберіть РАМ-рішення, яке відповідає потребам та бюджету вашої організації. Враховуйте функції, масштабованість та можливості інтеграції.

2. Виявлення та інвентаризація привілейованих облікових записів. Визначення всіх привілейованих облікових записів у вашому ІТ-середовищі. Це включає облікові записи адміністраторів, облікові записи служб та облікові записи програм.

3. Захист привілейованих облікових даних. Впроваджуйте безпечне сховище для зберігання та керування привілейованими обліковими даними. Застосовуйте політики надійних паролів та багатофакторну автентифікацію.

4. Забезпечте найменші привілеї. Надайте користувачам лише необхідний доступ для виконання своїх посадових обов'язків. Регулярно переглядайте та оновлюйте дозволи.

5. Моніторинг та аудит. Постійний моніторинг привілейованих сесій та активності. Аналіз журналів для виявлення аномалій та потенційних загроз.

6. Інтеграція з існуючими системами. Інтегруйте своє РАМ-рішення з існуючою інфраструктурою безпеки, такою як SIEM та системи керування ідентифікацією.

1.4. Аналіз технологій управління привілейованим доступом

Для аналізу та вибору технологій привілейованого доступу розглянемо наступні рішення, які пропонують CyberArk, BeyondTrust, Delinea та FortiPAM. Мета цього аналізу — не просто перерахувати функції, а знайти оптимальне рішення, що балансує між безпекою, вартістю володіння та інтеграційними можливостями.

Це беззаперечний «важковаговик» ринку, який часто вважають золотим стандартом для великих ентєрпрайз-структур.

Сильні сторони: Найширший функціонал на ринку, величезна база інтеграцій "з коробки", висока надійність та відповідність найсуворішим комплаєнс-вимогам (SOX, PCI DSS, GDPR).

Слабкі сторони: Надзвичайно висока вартість ліцензування та впровадження. Система складна в архітектурі, потребує виділеної команди для адміністрування та тривалого часу на розгортання.

BeyondTrust Password Safe

Рішення, яке фокусується на управлінні привілеями не лише для серверів, а й для кінцевих точок (Endpoint Privilege Management).

Сильні сторони: Відмінні можливості для керування правами на робочих станціях, потужний функціонал віддаленого доступу (Remote Support), єдина платформа для різних модулів безпеки.

Слабкі сторони: Інтерфейс може бути перевантаженим і складним для новачків. Деякі модулі вимагають окремого налаштування, що ускладнює загальну архітектуру.

Delinea (об'єднані Thycotic та Centrify)

Рішення, відоме своєю простотою та зручністю використання ("Secret Server").

Сильні сторони: Швидке розгортання, інтуїтивно зрозумілий інтерфейс, гнучкість у налаштуванні для середнього бізнесу. Добре співвідношення ціни та якості для базових потреб PAM.

Слабкі сторони: Може поступатися CyberArk у масштабованості для глобальних корпорацій. Після злиття компаній (Thycotic/Centrify) іноді виникають питання щодо уніфікації підтримки та дорожньої карти продуктів.

FortiPAM (Fortinet)

Частина екосистеми Fortinet Security Fabric. Це рішення нового покоління, яке інтегрує PAM безпосередньо в мережеву безпеку.

Сильні сторони: Повна інтеграція з Security Fabric (взаємодія з FortiGate, FortiAuthenticator, FortiClient). Підтримка концепції ZTNA (Zero Trust Network Access) «з коробки». Зручне керування секретами та сесіями без необхідності встановлення агентів (agentless) для більшості сценаріїв.

Слабкі сторони: Як окремий продукт (stand-alone) для компаній без інфраструктури Fortinet може втрачати частину інтеграційних переваг.

Щоб наочно оцінити різницю, виділено ключові параметри впровадження та експлуатації PAM рішень, які представлено у таблиці 1.1.

Таблиця 1.1.

Порівняння технологій PAM за ключовими параметрами

Характеристика	CyberArk	BeyondTrust	Delinea	FortiPAM
Цільова аудиторія	Global Enterprise, банки	Enterprise, великі мережі	SMB / Enterprise	Всі рівні (особливо Forti-екосистема)
Складність впровадження	Висока (місяці)	Середня/Висока	Низька/Середня	Низька (тижні)
Інтеграція з мережею	Через API/плагіни	Через API/агенти	Через API	Нативна (Security Fabric)
ZTNA (Zero Trust)	Окремі модулі	Частково	Окремі налаштування	Інтегровано в ядро
Вартість володіння (TCO)	Дуже висока	Висока	Середня	Оптимальна
Зручність інтерфейсу	Застарілий (Classic) / Новий	Специфічний	Сучасний	Інтуїтивний

Проаналізувавши поточні потреби бізнесу в захисті привілейованого доступу, рекомендовано обрати FortiPAM як найкраще рішення для впровадження.

Чому саме FortiPAM перемагає конкурентів у цьому порівнянні:

Екосистемний підхід. На відміну від ізольованих рішень (як CyberArk або Delinea), FortiPAM є частиною Fortinet Security Fabric. Це означає, що PAM не просто зберігає паролі, а обмінюється даними про загрози з фаєрволами (FortiGate) та системою автентифікації в реальному часі.

ZTNA та безпека доступу. FortiPAM забезпечує доступ до критичних ресурсів за принципом Zero Trust. Це критично важливо в сучасних умовах, коли периметр мережі розмитий. Ви отримуєте не просто "сейф для паролів", а захищений тунель до цільового ресурсу.

ROI та швидкість впровадження. Впровадження FortiPAM займає значно менше часу, ніж CyberArk, а ліцензійна політика є більш прозорою та вигідною. Ви отримуєте Enterprise-функціонал без необхідності наймати окремий штат для підтримки системи.

Отже, для побудови сучасної, інтегрованої та економічно ефективної системи безпеки FortiPAM є безальтернативним лідером, особливо якщо ваша мета — отримати комплексний захист, а не просто виконати формальні вимоги аудиту.

Висновки до розділу 1

1. Визначено критичну роль привілейованих облікових записів. Встановлено, що привілейовані акаунти (адміністратори домену, root-користувачі, сервісні акаунти) є найбільш чутливими елементами ІТ-інфраструктури. Відсутність належного контролю над ними створює значні вектори атак, оскільки такі записи надають необмежені права на керування конфігураціями, доступ до конфіденційних даних та можливість обходу засобів захисту.

2. Аналіз загроз показав, що основними ризиками, пов'язаними з неконтрольованим доступом, є витоки даних, зловживання внутрішніх порушників (інсайдерів) та неможливість проведення якісного аудиту інцидентів. Підтверджено, що фінансові та репутаційні втрати від реалізації цих загроз значно перевищують вартість впровадження спеціалізованих захисних систем.

3. На основі кращих світових практик визначено, що ефективна система PAM повинна базуватися на принципі найменших привілеїв (PoLP), забезпечувати

запис та моніторинг сесій у реальному часі, автоматизувати ротацію паролів та підтримувати механізми Just-In-Time доступу. Також критично важливою є відповідність регуляторним нормам.

4. Проведено порівняльний аналіз провідних РАМ-платформ: CyberArk, BeyondTrust, Delinea та FortiPAM. За результатами порівняння за критеріями функціональності, вартості володіння, складності впровадження та інтеграційних можливостей, обрано рішення FortiPAM.

2 МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА ПРИКЛАДІ FORTIPAM

2.1. Архітектура FortiPAM

Архітектура FortiPAM побудована за модульним принципом і є невід'ємною частиною екосистеми Fortinet Security Fabric та зображено на рис 2.1. Вона реалізує модель захисту, де FortiPAM виступає єдиним шлюзом для адміністративного доступу, ізолюючи користувачів від прямих з'єднань з критичними активами.

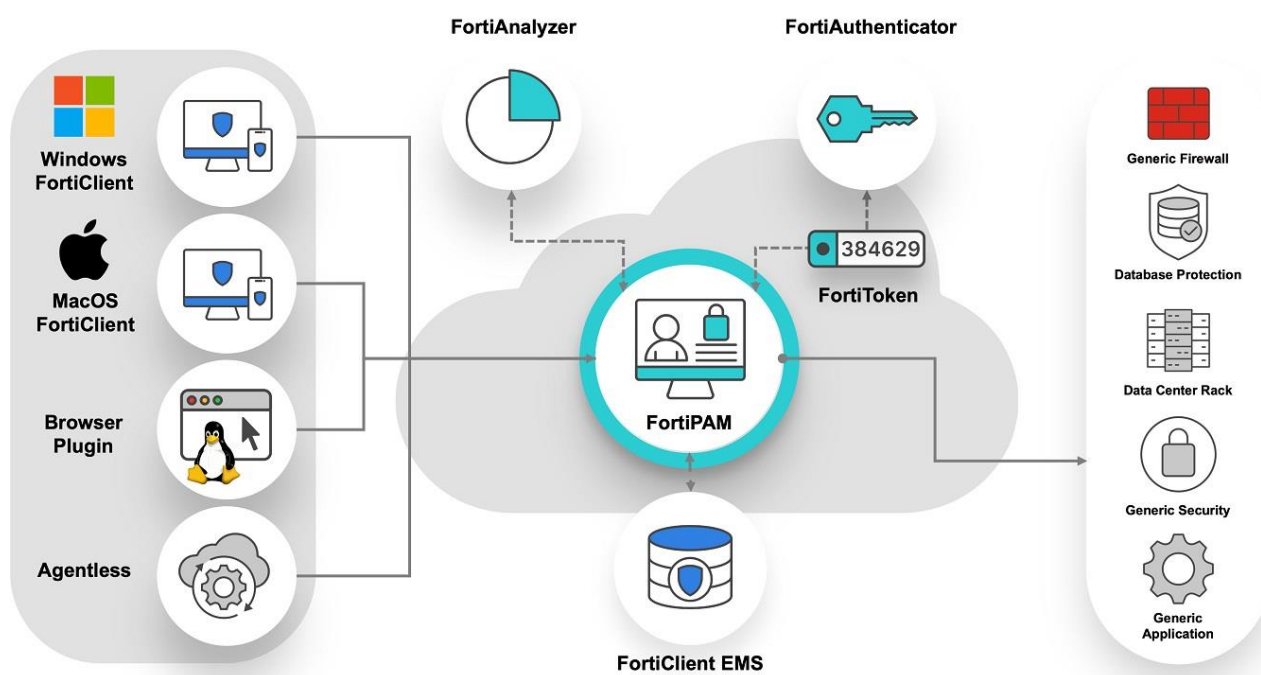


Рис.2.1. Архітектура FortiPAM

Згідно з наведеним рисунком 2.1., архітектуру FortiPAM можна розділити на три логічні рівні:

1. Рівень доступу (Access Layer)

Зліва на рисунку зображено суб'єктів доступу (користувачів/адміністраторів). Архітектура підтримує гнучкість підключення, дозволяючи обирати метод залежно від контексту безпеки:

Windows/MacOS FortiClient. Використання «товстого клієнта» для забезпечення повного тунелювання та перевірки стану пристрою.

Browser Plugin. Легковагові розширення для браузерів, що дозволяють безпечно підставляти облікові дані у веб-інтерфейси цільових систем.

Agentless. Доступ через веб-портал FortiPAM без необхідності встановлення додаткового ПЗ. Це зручно для підрядників або тимчасового доступу.

2. Ядро керування та інтеграції

Центральна частина схеми відображає ядро системи, де FortiPAM взаємодіє з допоміжними компонентами Security Fabric для забезпечення комплексного захисту:

FortiPAM. Головний компонент, що виконує функції сховища секретів, проксі-сервера для сесій та точки застосування політик доступу. Весь трафік проходить крізь нього.

FortiAuthenticator + FortiToken. Забезпечує сувору ідентифікацію користувачів. FortiPAM делегує перевірку автентичності цьому компоненту, вимагаючи багатфакторну автентифікацію (MFA) через токени FortiToken перед наданням доступу.

FortiClient EMS. Реалізує принципи Zero Trust. EMS передає на FortiPAM інформацію про «здоров'я» пристрою користувача (наявність антивірусу, оновлень, відсутність вразливостей). Якщо пристрій скомпрометовано, FortiPAM автоматично блокує доступ, навіть якщо пароль вірний.

FortiAnalyzer. Відповідає за централізований збір логів, аналітику та зберігання відеозаписів сесій. Це дозволяє проводити ретроспективний аналіз інцидентів та формувати звіти для аудиту.

3. Рівень цільових ресурсів (Target Layer)

Справа на рис 2.1. розташовані об'єкти захисту — ресурси, до яких надається доступ. FortiPAM підтримує роботу з гетерогенною інфраструктурою:

Generic Firewall / Security Мережеве обладнання (FortiGate, Cisco, Juniper тощо).

Database Protection. Бази даних (SQL, Oracle), де FortiPAM може автоматично змінювати паролі сервісних акаунтів.

Data Center Rack. Сервери (Windows, Linux), віртуальні машини.

Generic Application. Корпоративні додатки (CRM, ERP), що потребують захищеного входу.

Логіка роботи архітектури полягає у наступних кроках:

5. Користувач ініціює з'єднання через клієнт або браузер.
6. FortiPAM перевіряє облікові дані та запитує підтвердження MFA через FortiAuthenticator.
7. Одночасно через FortiClient EMS перевіряється відповідність пристрою політикам безпеки (Compliance).
8. Якщо всі перевірки пройдено, FortiPAM встановлює сесію з цільовим ресурсом (наприклад, сервером), підставляючи привілейовані облікові дані зі свого сховища. Користувач не бачить реального пароля.
9. Всі дії в рамках сесії записуються та передаються на FortiAnalyzer для архівації.

Розглянемо більш детально кожний компонент архітектури у наступному підрозділі.

2.2. Функції компонентів архітектури FortiPAM

FortiPAM — це рішення для керування привілейованим доступом. Рішення FortiPAM є важливою частиною корпоративної мережі, надаючи доступ на основі ролей, аудит та параметри безпеки для привілейованих користувачів (користувачів, які мають доступ до системи окрім звичайного користувача).

FortiPAM надає такі функції:

Зберігання облікових даних. Користувачам не потрібні облікові дані, що зменшує ризик їх витоку, оскільки після сеансу в системі користувача не зберігається конфіденційна інформація. Паролі змінюються автоматично.

Контроль доступу до привілейованих облікових записів. Користувачі можуть отримувати доступ до ресурсів FortiPAM лише на основі своїх ролей (стандартний користувач або адміністратор).

FortiPAM пропонує секретний контроль дозволів для доступу до цільового сервера. Адміністратори можуть визначати загальні політики та ієрархічну систему затвердження для звичайних користувачів доступу до конфіденційної інформації. FortiPAM також надає опції для контролю ризикованих дій користувачів, таких як спроба користувача зашифрувати диск.

FortiPAM пропонує керування доступом на основі тегів ZTNA та протоколів (RDP, SSH, VNC та WEB) і дозволяє доступ з будь-якого місця, включаючи власний веб-доступ.

Моніторинг та запис привілейованої активності. FortiPAM може контролювати, записувати та перевіряти активність привілейованих користувачів.

FortiPAM надає інформацію про сеанси, натискання клавіш користувачами та події миші.

Отже, доступ до пристроїв Security Fabric без FortiPAM збільшує ризик витоку облікових даних, несанкціонованого доступу та ускладнення відстеження активності користувачів.

FortiPAM допомагає підвищити безпеку в корпоративній мережі, надаючи доступ на основі ролей, аудит та параметри безпеки для привілейованих користувачів. Привілейовані користувачі мають доступ до системи, окрім звичайного користувача.

Пропонуючи функції, що включають сховище облікових даних, контроль доступу до привілейованих облікових записів, а також моніторинг і запис привілейованої активності, FortiPAM допомагає зменшити ризики безпеки, пов'язані з активністю привілейованих користувачів у корпоративній мережі.

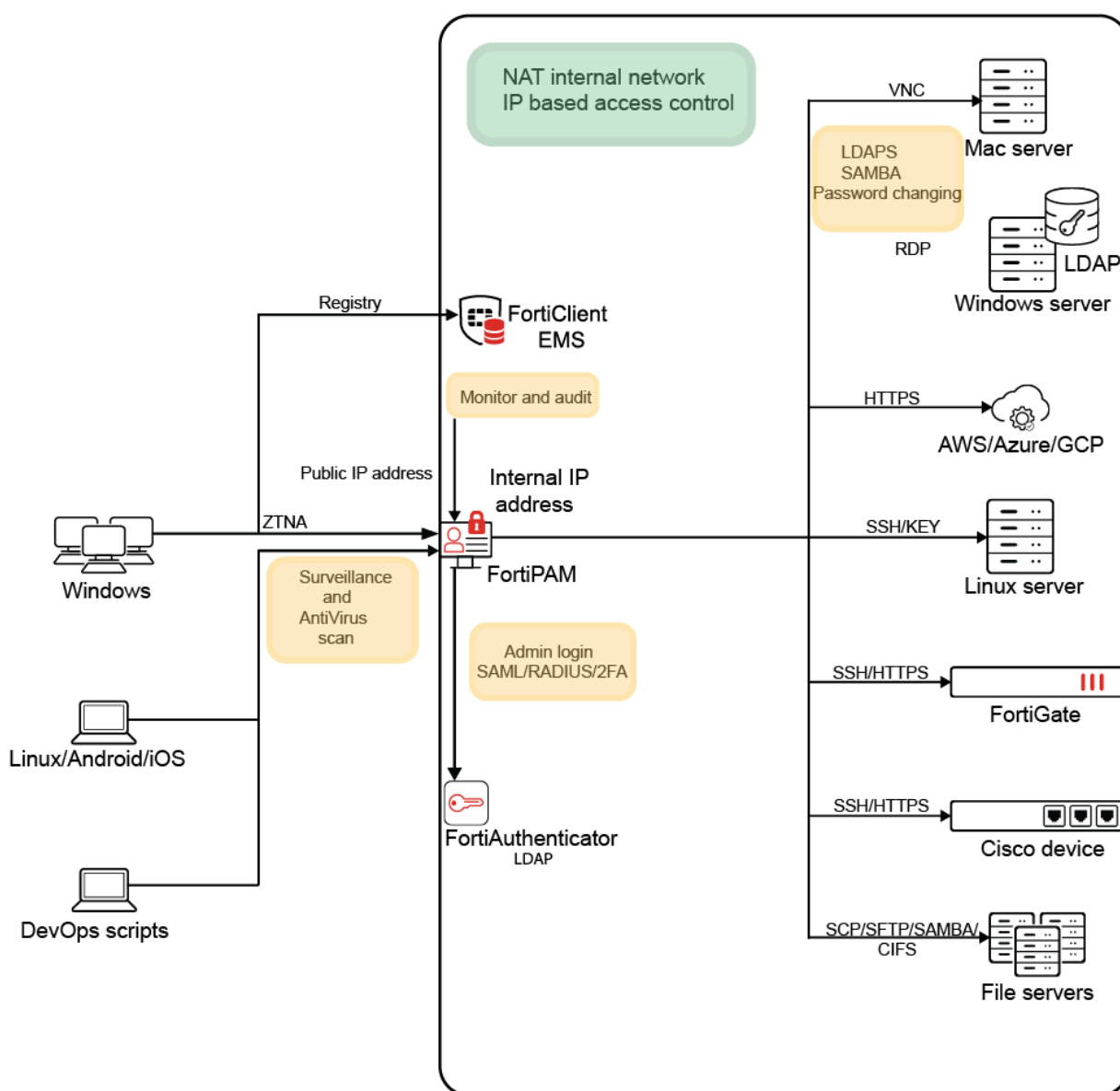


Рис. 3.2. Привілейовані активи FortiPAM

Керування привілейованими обліковими записами та сеансами (PASM)

FortiPAM забезпечує керування життєвим циклом привілейованих облікових записів та облікових даних, постійно виявляючи та додаючи некеровані облікові дані, застосовуючи детальні політики. Він забезпечує безпечне зберігання паролів, ключів SSH, токенів API та сертифікатів. Він також пропонує автоматизоване створення, ротацію та звітність паролів. FortiPAM надає, підвищує та скасовує доступ через робочі процеси управління на основі ідентифікації користувача, ролі та тегів ZTNA. Використовуючи внутрішній/зовнішній IdP та рішення IAM від

Fortinet, FortiPAM пропонує безпарольне керування, єдиний вхід та адаптивну багатофакторну автентифікацію (MFA).

Моніторинг та запис сеансу

Комплексний моніторинг і запис сеансів забезпечує повну видимість і детальний контроль над діями користувачів у режимі реального часу. Це включає відстеження та запис входу в систему, натискань клавіш і подій миші, що дозволяє швидко реагувати на підозрілу активність. Адміністратори можуть застосовувати фільтрацію команд і елементи керування фільтрами SSH, щоб обмежити дії привілейованих користувачів. Усі сеанси ізольовані, а облікові дані безпечно доставляють на цільовий пристрій, що захищає конфіденційну інформацію. Крім того, записи сеансів і аудитовані записи всіх дій допомагають досягти відповідності вимогам.

2.3. Принцип ZTNA для FortiPAM

За допомогою проксі-сервера доступу ZTNA формується безпечне з'єднання без використання dial-up VPN, це може звужити поверхню доступу до певних програм, що зменшує поверхню атаки [11]. Наведемо приклади поширених випадків використання ZTNA та зберемо їх для зручності у таблицю 3.1.

Таблиця 3.1.

Варіанти використання ZTNA

Випадок використання	Опис
Проксі-сервер для доступу до веб-застосунків	Доступ до вебзастосунків через HTTPS за допомогою проксі-сервера доступу ZTNA
Проксі-сервер прямого доступу TCP (TFAP)	Доступ до інших програм за допомогою проксі-сервера прямого доступу ZTNA TCP
Ідентичність та позиція ZTNA	Використовуйте правила ZTNA для позначення кінцевих точок за допомогою телеметрії ідентифікації або положення
Інтеграція постачальників ідентифікаційних даних (IdP)	Інтеграція різних типів постачальників ідентифікаційних даних для використання з багатофакторною автентифікацією (MFA)

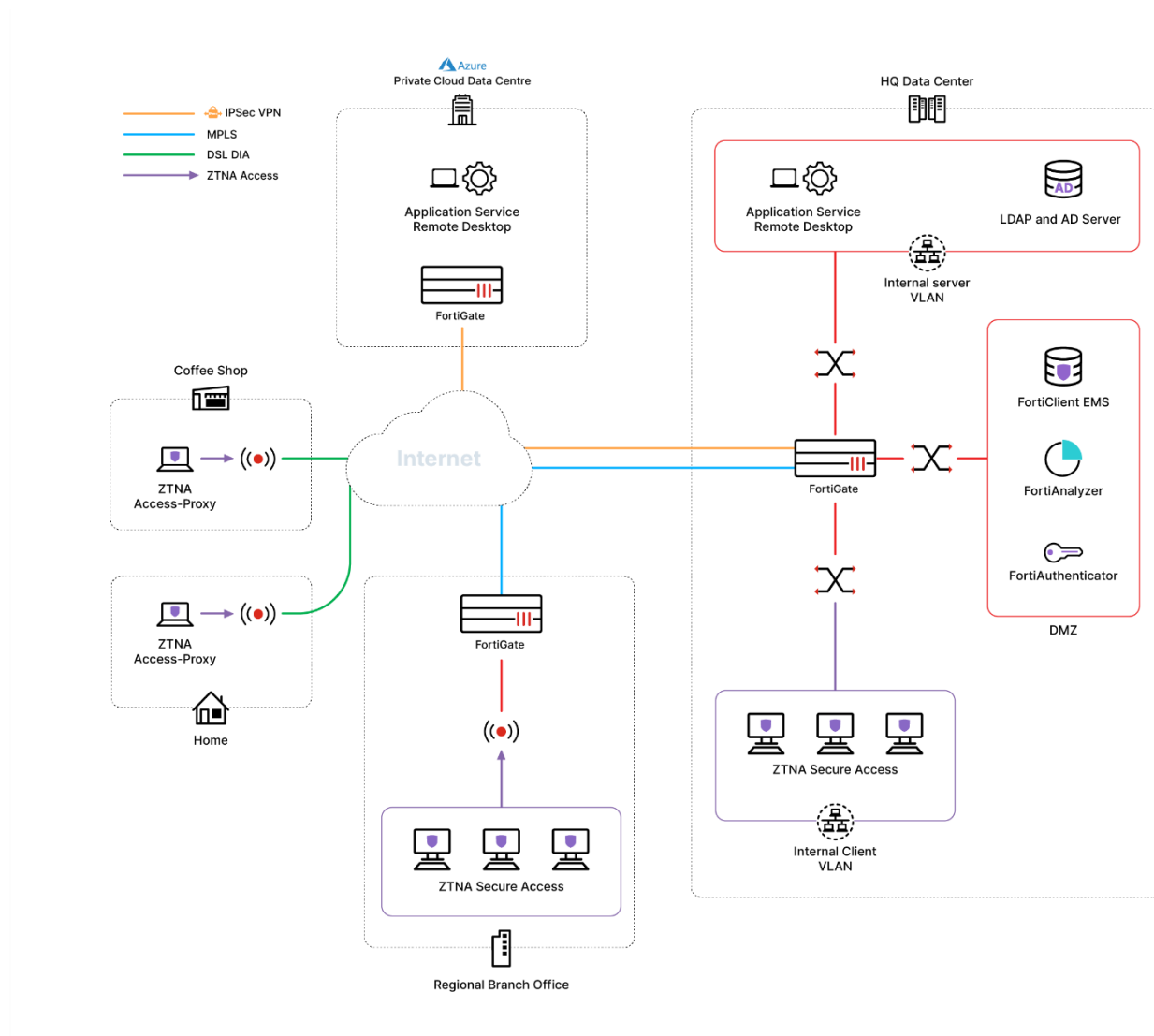


Рис. 3.3. Архітектура ZTNA

Незалежно від того, чи знаходяться користувачі в корпоративній мережі в офісі, чи віддалено в кав'ярні, вдома чи у філії, вони можуть безпечно отримувати доступ до внутрішніх ресурсів за допомогою ZTNA без додаткових VPN-підключень. Проксі-сервер доступу FortiGate перевіряє ідентифікацію пристрою, ідентифікацію користувача, стан пристрою, геолокацію, час і дозволи програм, перш ніж дозволити доступ, щоб забезпечити узгоджений користувацький досвід всередині та за межами корпоративної мережі.

Мережевий доступ із нульовою довірою (ZTNA) – це метод контролю доступу, який використовує ідентифікацію клієнтських пристроїв, автентифікацію та теги Zero Trust для забезпечення доступу до програм на основі ролей. Це надає

адміністраторам гнучкість в управлінні мережевим доступом для локальних користувачів мережі та віддалених користувачів поза мережею. Доступ до програм надається лише після перевірки пристрою, автентифікації особи користувача, авторизації користувача та виконання контекстних перевірок стану за допомогою тегів Zero Trust [11].

Рішення складається з вбудованих компонентів, які включають:

- Брандмауер наступного покоління FortiGate (NGFW)
- Сервер керування кінцевими точками FortiClient (EMS)
- FortiClient

Залежно від складності та вимог замовника, також може бути додано наступне:

- FortiManager
- FortiAnalyzer
- FortiAuthenticator
- FortiToken

Для рішення ZTNA можна виділити два варіанта впровадження [11]:

1. Проксі-сервер доступу до ZTNA

- Рішення та архітектура проксі-доступу HTTPS та TCP.
- Стосується як віддаленого, так і внутрішнього доступу.
- Постійне з'єднання (наприклад, VPN) не потрібне.

2. Проксі-сервер без доступу ZTNA (також відомий як безпечний доступ ZTNA)

- Віддалені користувачі продовжують отримувати доступ до мережі за допомогою VPN, але з додатковими рівнями ідентифікації пристроїв ZTNA та перевірки стану ZTNA за допомогою правил та тегів.
- Локальним користувачам надається доступ через локальні політики доступу з перевітками стану ZTNA.

У архітектурі (рис. 3.3) метою є підвищення безпеки або зменшення навантаження на персонал служби безпеки під час надання доступу до програм

віддаленим користувачам. Підвищення безпеки досягається завдяки безшовній інтеграції перевірки ідентифікації пристрою, ідентифікації користувача та стану. Це полегшує навантаження на безпеку, зменшуючи кількість точкових продуктів, які керують сертифікатами пристроїв, перевірками стану та іншими технологіями перевірки ідентифікації.

Розглянемо приклад архітектури компанії, яка має кілька застосунків, розміщених як всередині компанії, так і в приватній хмарі Azure.

Перед впровадження ZTNA, віддалені користувачі використовували VPN для отримання доступу до внутрішньої мережі, а потім отримують доступ до веб-програм за допомогою веббраузера. Доступ до невеб-програм здійснюється за допомогою віддаленого робочого столу (RDP) через VPN для переходу до місць, де встановлено клієнт-серверні програми.

Після того, як в компанії стався спалах шкідливого програмного забезпечення, яке поширювалося з однієї точки мережі на багато кінцевих точок, підключених до внутрішньої мережі, включаючи ті, що підключені через VPN. У ході розслідування компанія виявила, що шкідливе програмне забезпечення походило з некерованого пристрою без патчів, підключеного до мережі через VPN. Компанія зобов'язала впроваджувати архітектуру нульової довіри. Були детально описані такі критерії успіху:

1. Блокування некерованих пристроїв.
2. Вимагати багатофакторної автентифікації.
3. Для віддалених користувачів обмежити прямий доступ до внутрішньої мережі для веб-застосунків або служб віддаленого робочого столу.
4. Дозволити лише визначеним групам користувачів доступ лише до певних програм, які їм потрібні.
5. Динамічно забороняти доступ пристроям із критичними вразливостями як у внутрішній мережі, так і в мережі віддаленого доступу.
6. Динамічно дозволяти доступ після усунення вразливостей.
7. Зменшити залежність від dial-up VPN.

Для досягнення вищезазначених цілей розгляньте запропоновано рішення ZTNA які представлено у таблиці 3.2.

Цілі безпеки	Рішення ZTNA
Блокування некерованих пристроїв	Використовуйте FortiClient
Немає прямого доступу до внутрішніх мереж для веб-застосунків або віддаленого робочого столу	Використовуйте проксі-сервери доступу ZTNA HTTPS та TCP-forwarding
Дозволити лише визначеним групам користувачів доступ лише до певних програм, які їм потрібні	Використовуйте проксі-сервери доступу ZTNA та перевірку стану безпечного доступу ZTNA з інтеграцією з існуючими користувачами та групами IdP, FortiAuthenticator або брандмауера
Динамічно забороняти доступ до скомпрометованих або вразливих пристроїв і динамічно дозволяти доступ до пристроїв після виправлення	Використовуйте перевірку стану безпечного доступу ZTNA
Вимагати багатофакторної автентифікації (MFA)	Використовуйте проксі-сервери доступу ZTNA, налаштовані за допомогою IdP та FortiToken
Зменште залежність від dial-up VPN	Дозволити використання VPN з перевіркою стану безпечного доступу ZTNA та багатофакторною автентифікацією лише ІТ-персоналу та персоналу служби безпеки

Отже, ZTNA вирішує деякі з цих проблем, захищаючи трафік через SSL-з'єднання, перевіряючи ідентифікацію пристрою, перевіряючи, чи ввімкнено відповідні функції безпеки кінцевих точок, та автентифікацію користувача. Ці заходи допомагають зменшити фактори ризику безпеки, щоб надати віддаленим користувачам рівень доступу, подібний до того, який доступний під час роботи локально в офісі. Це також призводить до доступу до програм на основі ролей, де доступ надається на основі ролей користувача та пристрою, а не джерела трафіку.

Висновки 2 розділу

1. Встановлено, що архітектура FortiPAM побудована за модульним принципом і є ключовим елементом екосистеми Fortinet Security Fabric. Система реалізує трирівневу модель захисту (рівень доступу, ядро керування, цільові ресурси), що дозволяє ізолювати користувачів від прямої взаємодії з критичними активами, виступаючи єдиним захищеним шлюзом.

2. Визначено, що FortiPAM забезпечує повний цикл управління привілейованим доступом (PASM). До ключових функцій належать: безпечне зберігання та автоматична ротація секретів, гранульований контроль доступу на основі ролей (RBAC), а також моніторинг і відеофіксація сесій у реальному часі, що критично важливо для аудиту та розслідування інцидентів.

3. Обґрунтовано ефективність використання принципу ZTNA (Zero Trust Network Access) у FortiPAM. На відміну від традиційних VPN, ZTNA надає доступ до конкретних застосунків, а не до всієї мережі, і лише після перевірки ідентичності користувача та стану безпеки його пристрою через інтеграцію з FortiClient EMS.

4. Доведено, що інтеграція FortiPAM з іншими компонентами фабрики безпеки (FortiGate, FortiAuthenticator, FortiAnalyzer) дозволяє мінімізувати поверхню атаки, блокувати скомпрометовані пристрої та забезпечити захищений доступ як для локальних, так і для віддалених адміністраторів без необхідності постійного VPN-з'єднання.

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА ПРИКЛАДІ FORTIPAM

3.1. Технологія впровадження та експлуатації FortiPam

Впровадження та експлуатація технології FortiPAM здійснюється за логічним алгоритмом, який забезпечує повний цикл захисту привілейованих облікових записів (рc.3.1).



Рис.3.1. Технологія впровадження та експлуатації FortiPAM

Процес складається з наступних кроків:

Моніторинг стану системи: Перевірка здоров'я системи, ліцензій та навантаження на ресурси через головну інформаційну панель.

Управління користувачами та ролями: Створення облікових записів адміністраторів та аудиторів, визначення рольової моделі доступу (RBAC) для розмежування повноважень.

Налаштування автентифікації: Інтеграція із зовнішніми системами (LDAP/RADIUS/SAML) для забезпечення централізованого входу та багатофакторної автентифікації.

Класифікація та створення секретів: Використання шаблонів для додавання цільових активів (серверів, баз даних, мережевого обладнання) у сховище.

Налаштування політик сесії: Визначення параметрів підключення (RDP/SSH), активація запису сесій та моніторингу дій.

Аудит та звітність: Налаштування автоматичної генерації звітів про активність користувачів та використання секретів.

1. Моніторинг стану системи (Dashboard)

Робота з системою починається з головного вікна моніторингу. На рисунку 3.2 відображено «Інформаційну панель» (Dashboard), яка надає адміністратору миттєвий зріз стану безпеки та продуктивності:

System Information. Містить базові дані, такі як Hostname, серійний номер, версія прошивки (Firmware v1.7.1) та системний час.

Licenses. Статус ліцензій, включаючи підписку, підтримку FortiCare та оновлення антивірусних баз/DLP.

Hardware Monitor. Графіки навантаження на CPU та Memory (відображено використання 32.3% пам'яті), що дозволяє оцінити запас ресурсів.

Sessions & Bandwidth. Статистика активних сесій та пропускної здатності мережевих інтерфейсів (вхідний/вихідний трафік).

System Events. Журнал критичних подій, наприклад, невдалі спроби входу адміністратора або втрата з'єднання з FortiAnalyzer.

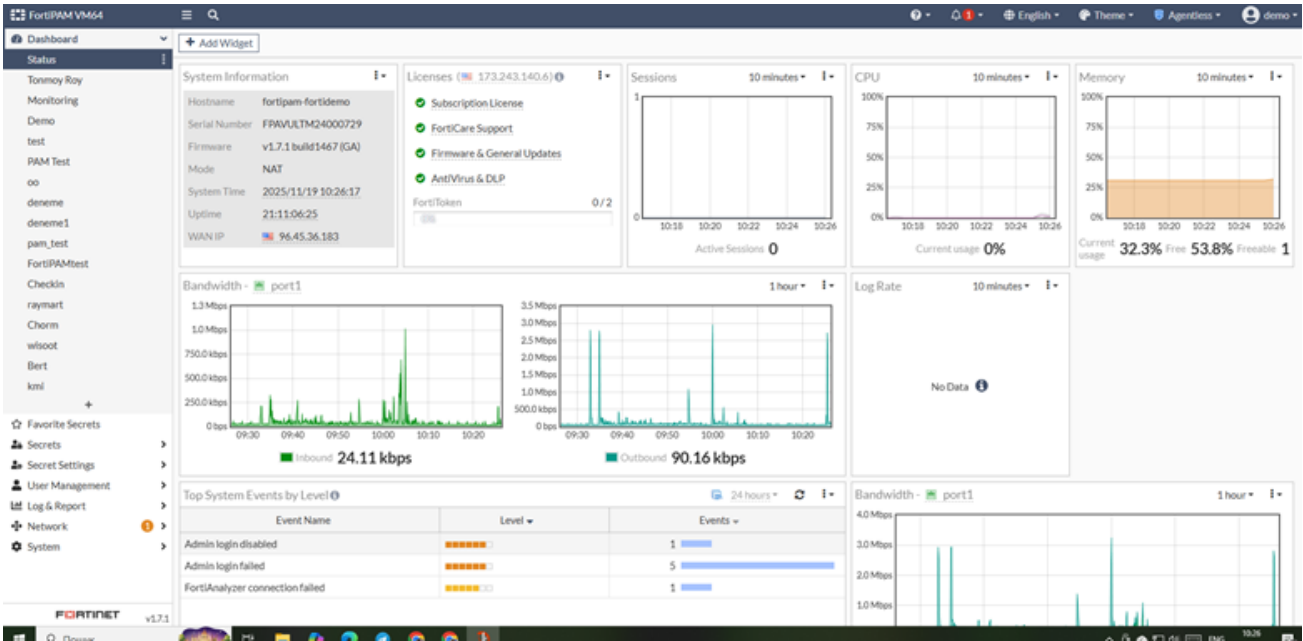


Рис. 3.2. Інформаційна панель

2. Керування секретами (Secrets Management)

Основною функцією РАР є зберігання та управління обліковими даними.

Список секретів (Рис. 3.3).

Ім'я	Поля	Запуск	Зміна пароля	Тип сервера	Опис
Користувач Cisco (SSH-секрет)	Хост Ім'я користувача Пароль	PuTTY Веб-SSH	Користувач Cisco (SSH-секрет)	Cisco	
VNC-сервер	Хост Ім'я користувача Пароль	Веб VNC VNC-переглядач TightVNC		Інше	
vCenter	URL-адреса Ім'я користувача Пароль	Перегляд веб-сторінок	Веб-API (vCenter)	Інше	
Сертифікат	Сертифікат Закритий ключ Парольна фраза			Інше	
FortiGate/FortiOS (веб)	Хост Ім'я користувача	PuTTY Веб-SSH Перегляд веб-сторінок	Веб-API (FortiGate/FortiOS)	FortiOS	
Пари ключ-значення				Інше	
Файл	Ім'я файлу			Інше	
MySQL	Хост Ім'я користувача Пароль	Командний рядок MySQL Оболонка MySQL		Інше	
Машина	Хост Ім'я користувача Пароль	PuTTY Веб-SSH		Інше	
FortiGate/FortiOS (ключ SSH)	Хост Ім'я користувача	PuTTY Веб-SSH	SSH-ключ (FortiGate/FortiOS)	FortiOS	
Облікові дані Azure	Ідентифікатор орендаря			Інше	

Рис.3.3. Інформація про секрет яка знаходиться на сервері Secret

На рис.3.3 показано таблицю, яка є головною таблицею активів. Для кожного запису відображаються ключові параметри:

Для кожного секрету за замовчуванням відображаються такі стовпці:

- Ім'я
- Цільова адреса
- Опис
- Автоматична зміна пароля
- Час останнього запуску
- Остання зміна пароля
- Останнє підтвердження пароля
- Папка
- Шаблон

Щоб створити секрет необхідно в розділі Секрети знайти папку, куди потрібно додати секрет. Після чого відкриється сторінка «Вибір шаблону секрету». Кожен шаблон має свою відповідну піктограму.



Рис 3.4.. Шаблони секретів

Шаблони секретів поділено на категорії та їх можна фільтрувати в залежності від пристрою до якого буде створено секрет.

Для уніфікації налаштувань система пропонує бібліотеку шаблонів.

Шаблони категоризовані за типом обладнання: Windows (Domain Account, Machine), Unix-like (SSH Key/Password), FortiOS, Cisco, Database (MySQL, PostgreSQL) та Cloud (AWS, Azure) .

Вибір правильного шаблону автоматизує процес підключення, оскільки вже містить специфічні для платформи скрипти перевірки та зміни паролів.

Система дозволяє проглядати деталі секрету (Рис. 3.5.).

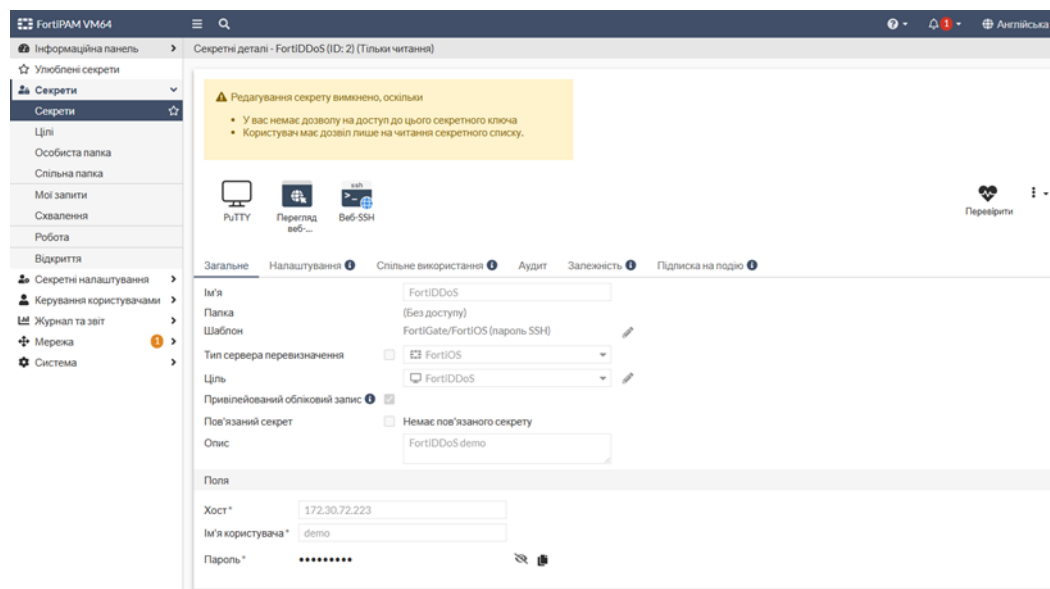


Рис.3.5. Розділ інформації про секрет

При створенні або перегляді конкретного секрету (наприклад, "FortiDDoS") адміністратор в розділі деталей секрету –налаштування може коригувати і змінювати такі позиції:

Методи доступу. Кнопки швидкого запуску через PuTTY, Web-SSH або перегляд веб-сторінки .

Облікові дані. Поля для введення Хоста (IP), імені користувача та прихованого поля Пароля.

Власність. Визначення папки та пов'язаних секретів.

На рис 3.6. показано вкладку налаштувань політик сесій та безпеки Це критично важливий етап налаштування, що визначає, як саме користувач взаємодіє з активом.

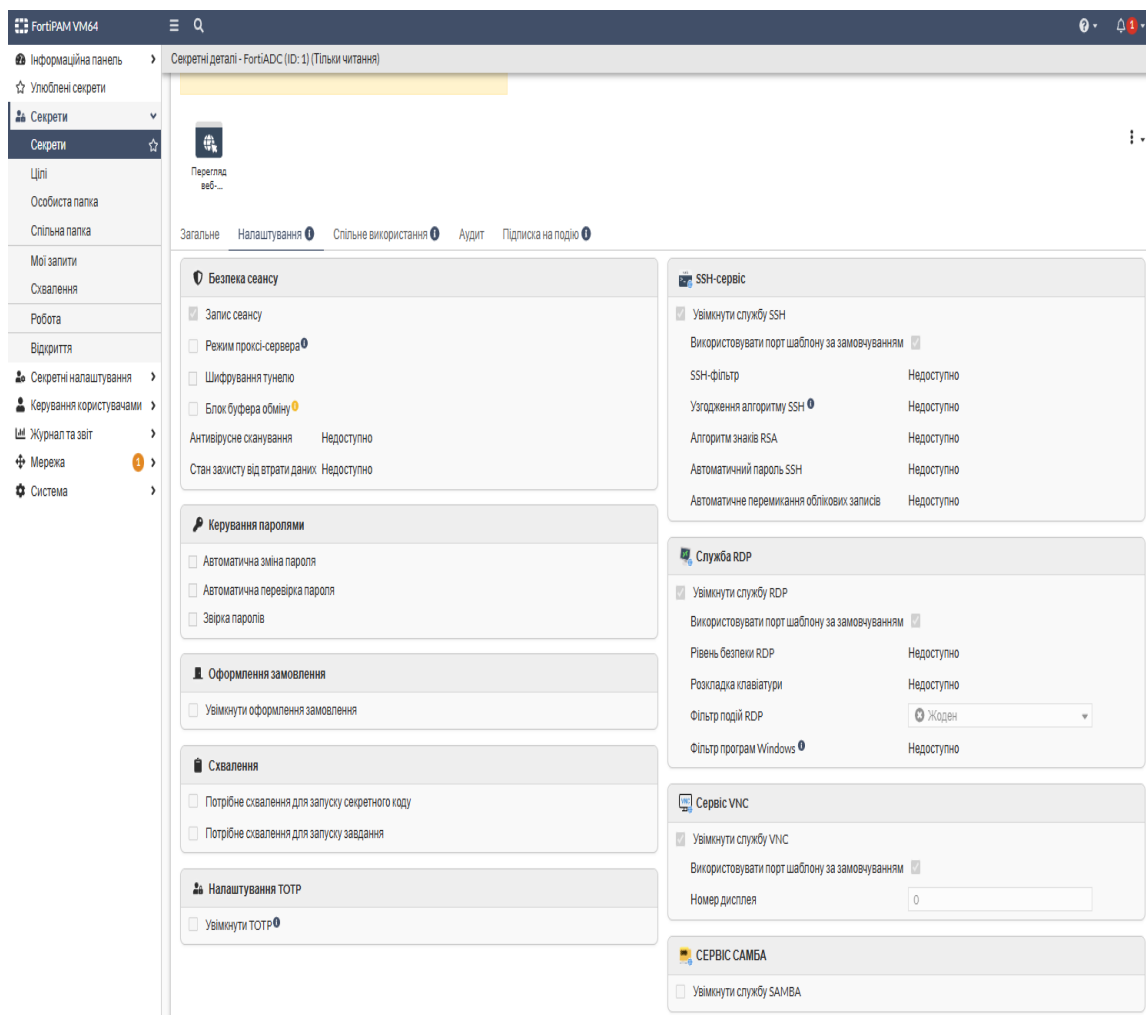


Рис.3.6. Налаштування політик сесій та безпеки

Отже, політики сеансів і безпеки включають:

Безпека сеансу

Активація опції "Запис сеансу" гарантує відеофіксацію дій. Опція "Режим проксі-сервера" приховує реальну адресу сервера від користувача .

Керування службами

- SSH-сервіс. Налаштування фільтрів команд та алгоритмів шифрування.
- Служба RDP. Визначення рівня безпеки та фільтрація буфера обміну .

Керування пароллями.

Опції автоматичної зміни та звірки паролів для забезпечення їх актуальності

3. Управління користувачами та ролями (User Management)

Система підтримує гнучку модель доступу, яка заснована на ролевій моделі доступу. Список користувачів можна побачити на вкладці (рис. 3,6), яка відображає всіх суб'єктів доступу.

Ім'я	Спонсорована група	Роль	Тип	Останній вхід	Статус	Двофакторна автентифікація	Посилання
Адміністратор							
адміністратор		Суперадміністратор	Місцевий	2025-11-18 21:27:02	Увімкнено	Вимкнути	9
Налаштований користувач							
демоверсія		demo_user	Віддалений	2025-11-19 10:36:13	Увімкнено	Вимкнути	5
Гість							
фортіпам		Гість	Місцевий	0	Увімкнено	Вимкнути	1

Рис. 3.6. Список привілейованих користувачів

Якщо зайти в налаштування кожного користувача, то з'являються інші списки можливих налаштувань (рис.3.7).

- Поділ користувачів на Локальних та Віддалених.
- У списку вказано роль (наприклад, "Суперадміністратор", "Гість"), статус двофакторної автентифікації та статус активності .
- Налаштування користувача (Рисунок): При редагуванні профілю (наприклад, користувача `admin`) задаються:
 - Тип ролі: Вибір рівня доступу (Administrator, User).
 - Дані входу: Логін, пароль, email.
 - Безпека: Увімкнення двофакторної автентифікації (Two-Factor Authentication) та обмеження доступу за IP-адресами (IPv4 Trusted Hosts) .

Рис. 3.7. Деталі налаштувань користувача

Рольова модель, яка використовується в системі дозволяє використовувати попередньо налаштовані профілі ("Суперадміністратор", "Гість", "Стандартний користувач"), які визначають набір прав. Ролі користувачів або профілі доступу визначають, що може робити користувач після входу у FortiPAM.

	Ім'я	Коментарі	Секрет	Система	Користувач і пристрій
Профілі за замовчуванням (не редагуються)					
Гість			Користувальця	Жоден	Жоден
Адміністратор спонсора			Користувальця	Користувальця	Жоден
Стандартний користувач			Користувальця	Жоден	Жоден
Адміністратор за замовчуванням			Читання / Запис	Читання / Запис	Читання / Запис
Досвідчений користувач			Читання / Запис	Жоден	Жоден
Суперадміністратор			Читання / Запис	Читання / Запис	Читання / Запис
Користувальчі профілі					
demo user			Користувальця	Користувальця	Користувальця

Рис 3.8. Попередньо налаштовані профілі за ролями

Для кожної ролі надається деталізація прав доступу (Рис. 3.9.). Налаштування ролей є гранулярним. Для кожного модуля (Secrets, User Management, System) можна встановити рівень прав: None (Немає), Read (Читання), Read/Write (Запис) .

Наприклад, можна заборонити перегляд логів (View Logs - Disable) або дозволити доступ до GUI (Access FortiPAM GUI - Enable).

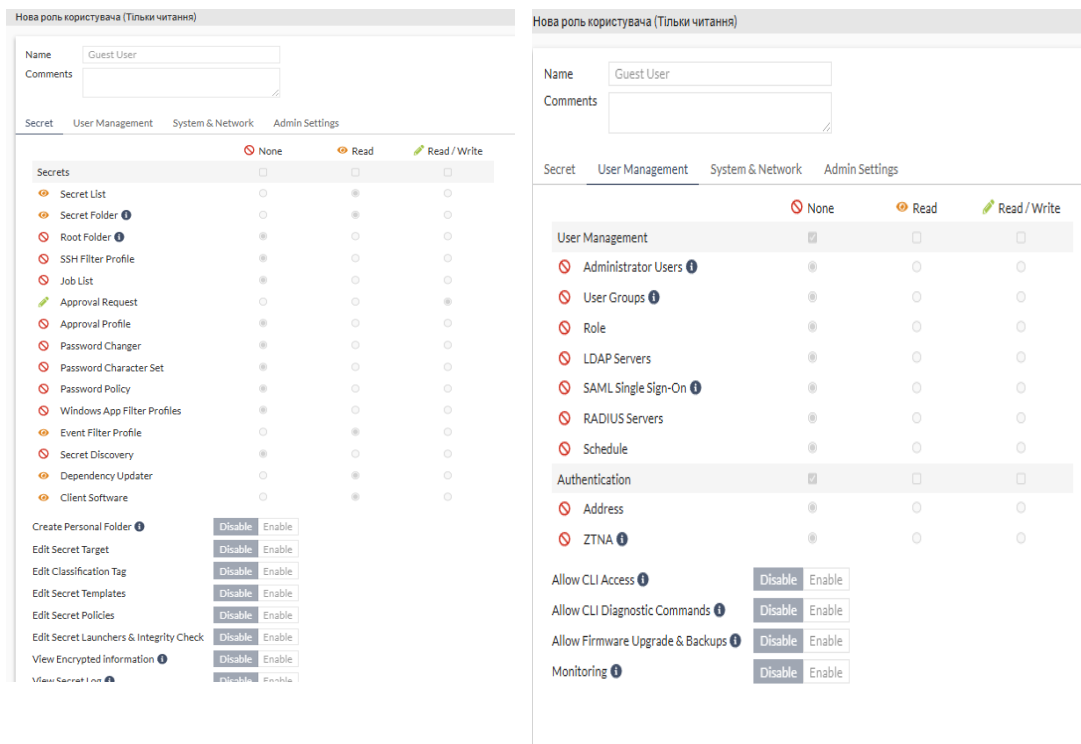


Рис. 3.9. Налаштування модулів Secrets, User Management, System для обраної ролі

4. Інтеграція та зовнішня автентифікація

Для масштабування системи використовуються зовнішні сервіси. SAML Single Sign-On (Рис. 3.10). Налаштування єдиного входу (SSO), де FortiPAM виступає як Service Provider.

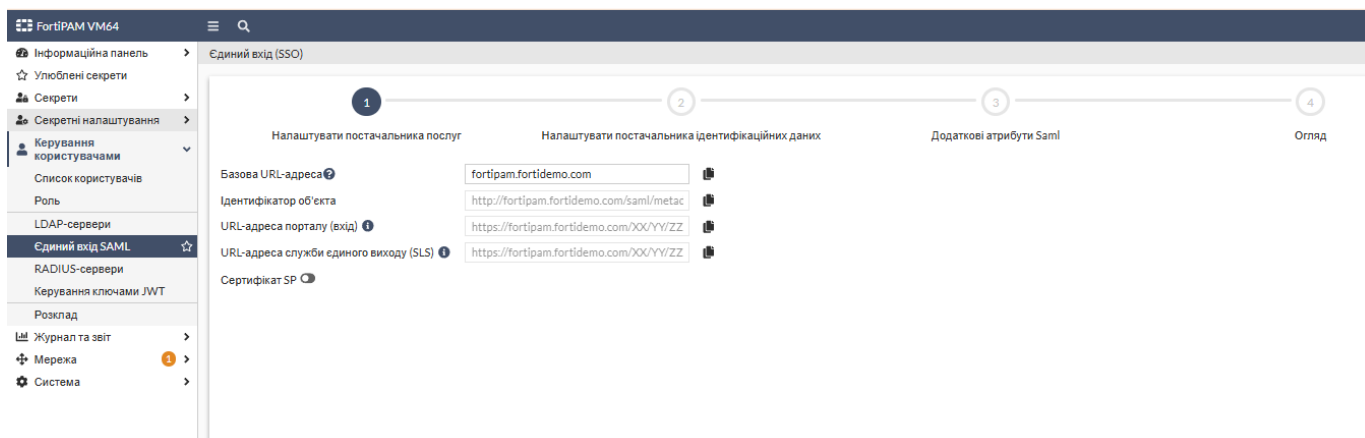


Рис.3.10 Налаштування аутентифікації

FortiPAM виконує роль інтернет-провайдера в SAML-аутентифікації, сервер SAML визначає конфігурацію між інтернет-провайдером та постачальником ідентифікаційних даних. IDP може автентифікувати віддалених користувачів FortiPAM та надавати групи для цілей авторизації.

Сервери Radius зберігають інформацію про користувачів, включаючи облікові дані та деякі атрибути тощо, які можуть автентифікувати віддалених користувачів FortiPAM та надавати групи для цілей авторизації.

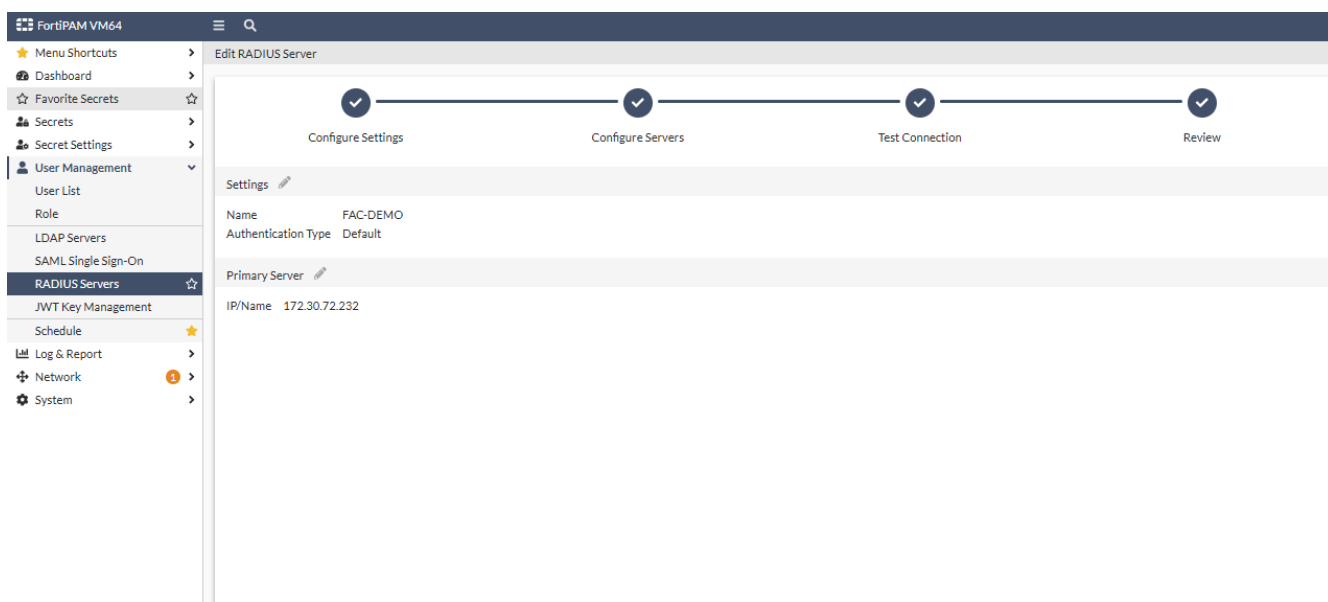


Рис. 3.11 Сервери Radius

Тип автентифікації, дозволений для цього RADIUS-сервера. За замовчуванням використовуються PAP, MS-CHAP-V2 та CHAP.

Це дозволяє автентифікувати віддалених користувачів через корпоративні системи ідентифікації. Процес налаштування включає 4 кроки, починаючи з вибору імені та типу автентифікації (PAP, MS-CHAP-V2).

5. Звітність та аналітика (Log & Report)

Завершальним елементом технології є контроль. Налаштування макету звіту (Рис. 3.12). Система дозволяє конструювати звіти (наприклад, "KMCBL").

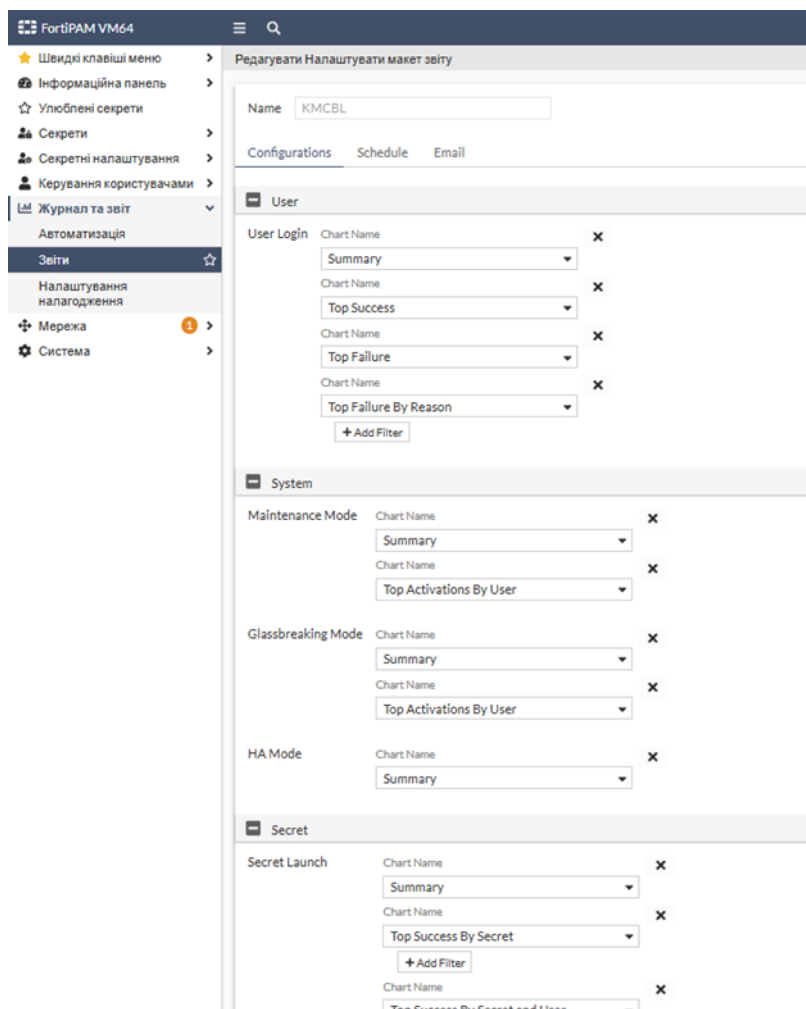
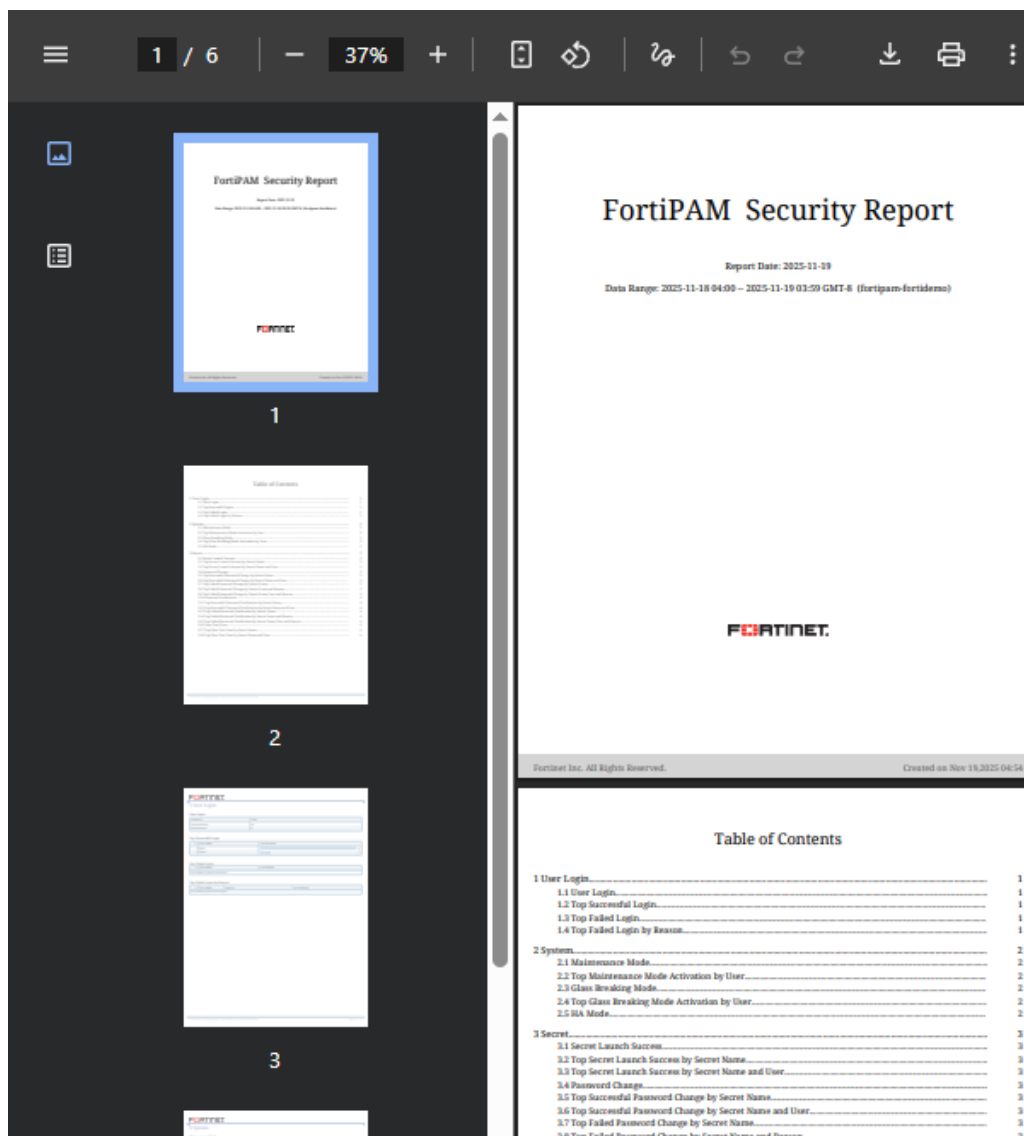


Рис.3.12. Формування звіту

Адміністратор обирає діаграми для включення до звіту, такі як "Summary" (Підсумок), "Top Success/Failure" (Успішні/Невдалі входи) для користувачів. Системні події: Включення статистики по режиму обслуговування (Maintenance Mode) та використанню секретів.

Деякі діаграми підтримують фільтри. Налаштувавши фільтри, ви можете фільтрувати інформацію, щоб у звіті залишалися лише ті частини, які вас цікавлять. У розкритому списку фільтрів відображаються доступні типи фільтрів. Ви можете додавати однакові або різні фільтри кілька разів. Однакові фільтри показують результати об'єднання, тоді як різні фільтри показують результати перетину.



3.13. Сформований звіт

Звіти про аудит дозволяють аналізувати ефективність використання системи та розслідувати інциденти.

3.2. Рекомендації мінімізації ризиків при впровадженні технології управління привілейованим доступом інформаційної системи організації

Впровадження технології управління привілейованим доступом є критичним кроком для захисту сучасної ІТ-інфраструктури. Привілейовані облікові записи, за своєю природою необхідні для адміністрування, але в руках зловмисників перетворюються на ключі від усіх дверей організації. Щоб перетворити цю

вразливість на керований актив та уникнути поширених помилок, компаніям необхідно дотримуватися кількох ключових практик.

Фундаментом безпеки є розуміння повного життєвого циклу загрози. Обране РАМ-рішення не повинно обмежуватися лише пасивним моніторингом або захистом периметра. Ефективна система має охоплювати всі етапи, починаючи від виявлення активів і захисту до детекції аномалій та реагування на інциденти.

Важливим аспектом, який часто недооцінюють, є простота впровадження та використання. Складні, неінтуїтивні рішення часто стають причиною провалу проєктів через виснаження бюджету та ресурсів команди безпеки. Тому при виборі продукту слід враховувати сукупну вартість володіння, яка включає не лише ціну ліцензії, а й витрати на консалтинг, налаштування та, що найважливіше, навчання персоналу. Зміна поведінки користувачів є такою ж важливою складовою успіху, як і технічні налаштування.

З технічної точки зору, головним орієнтиром має стати принцип найменших привілеїв. Це означає відмову від надлишкових прав, коли кожен користувач або сервіс повинен мати лише той мінімум доступу, який необхідний для виконання завдання. Процес починається з інвентаризації та ідентифікації власників облікових записів, після чого відбувається обмеження та ліквідація зайвих прав. Щоб зберегти баланс між суворим контролем та ефективністю роботи адміністраторів, доцільно використовувати інструменти запису сесій, що дозволяє моніторити дії без блокування робочих процесів.

Сучасні загрози вимагають також переходу від статичних прав до контекстного контролю доступу. Автоматизація політик безпеки дозволяє враховувати час доби, геолокацію та тип пристрою при наданні доступу. Наприклад, якщо адміністратор намагається залогінитися в неробочий час з підозрілої IP-адреси, система автоматично заблокує таку спробу. Це нівелює цінність вкрадених облікових даних для хакерів, які діють ззовні.

Наостанок, критично важливо ліквідувати практику використання спільних облікових записів (наприклад, загальний "admin" для групи людей) та жорстко закодованих паролів у скриптах. Кожна дія в системі повинна бути персоніфікована

для забезпечення підзвітності. РАМ-система має взяти на себе роль централізованого сховища, забезпечуючи регулярну автоматичну зміну паролів та їх динамічне підставлення для додатків, що усуває ризики людського фактору та витоку облікових даних.

Отже, рекомендації щодо використання систем управління привілейованим доступом, які базуються на сучасних стандартах кібербезпеки та підходах Zero Trust виходять за межі простого налаштування програмного забезпечення і стосуються процесів та політик безпеки.

Впроваджувати підхід «Just-in-Time» доступ. Замість того щоб надавати адміністраторам постійні права, необхідно перейти до моделі доступу за запитом.

Такий підхід надає користувач нульові права за замовчуванням. На час виконання завдання користувач запитує доступ. Система надає права лише на конкретний проміжок часу (наприклад, на 2 години), після чого автоматично їх відкликає. Це різко зменшує вікно можливостей для зловмисників.

Застосовувати обов'язкову багатофакторну автентифікацію (MFA). Ніколи не покладатися лише на пароль для входу в РАМ-систему або доступу до критичних активів. Необхідно налаштувати MFA при вході на РАМ-систему, тобто повторний запит другого фактора безпосередньо перед підключенням до найкритичніших серверів (наприклад, контролерів домену або баз даних з персиданими), навіть якщо користувач вже всередині системи.

Ізоляція сесій. Уникати прямого підключення з робочої станції адміністратора до цільового сервера. Робочі станції часто мають доступ до інтернету і можуть бути заражені шкідливим ПЗ. РАМ має виступати як «Jump Server» або проксі. Адміністратор підключається до РАМ, а РАМ відкриває сесію до цільового сервера. Адміністратор не повинен бачити або знати пароль цільового облікового запису. Система сама підставляє його. Це запобігає фішингу та записуванню паролів на папірцях.

Захист «нелюдських» ідентичностей. У сучасних ІТ-середовищах кількість сервісних акаунтів, ботів, API-ключів та скриптів значно перевищує кількість

живих користувачів. Додатки повинні звертатися до РАМ-системи через API, щоб отримати необхідні облікові дані «на льоту».

Поведінкова аналітика (UEBA). Простого запису екрана недостатньо — ніхто не переглядає тисячі годин відео, доки не станеться інцидент. Необхідно налаштувати систему на виявлення аномалій. Вхід у нетиповий час (3 година ночі), доступ до нетипової кількості серверів за короткий час, виконання деструктивних команд (наприклад, видалення бази даних). Система має автоматично розривати такі сесії. Регулярне оновлення облікових даних. Статичний пароль — це вразливий пароль. Необхідно налаштовувати РАМ на автоматичну зміну паролів для високопривілейованих облікових записів (наприклад, root, Administrator) після кожного використання або за розкладом (наприклад, кожні 24 години).

Безперервне виявлення для виявлення нових облікових записів. ІТ-інфраструктура динамічна. Нові віртуальні машини та сервіси з'являються щодня. Необхідно налаштувати регулярне автоматичне сканування мережі для виявлення нових облікових записів, які ще не взяті під контроль РАМ, щоб уникнути появи «тіньового ІТ».

Висновки до розділу 3

1. Формалізовано алгоритм впровадження та експлуатації системи FortiPAM, який складається з шести етапів. Такий підхід забезпечує повний цикл захисту облікових записів.

2. Реалізовано механізми керування секретами та доступом. Продемонстровано, що використання шаблонів секретів дозволяє уніфікувати та автоматизувати процес підключення гетерогенних активів (Windows, Unix, мережеве обладнання). Налаштування рольової моделі (RBAC) з гранулярним розподілом прав доступу дозволило реалізувати принцип найменших привілеїв, обмежуючи можливості адміністраторів лише необхідним функціоналом.

3. Забезпечено контроль та підзвітність. Налаштування підсистеми аудиту та звітності (Log & Report) дозволило отримати інструмент для глибокого аналізу активності користувачів. Створення кастомізованих звітів та відеофіксація сесій

забезпечують можливість розслідування інцидентів та контроль за дотриманням політик безпеки.

4. Розроблено стратегію мінімізації ризиків. На основі аналізу кращих практик сформовано рекомендації щодо підвищення рівня захисту інформаційних систем організацій.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

1. Визначено критичну роль привілейованих облікових записів. Встановлено, що привілейовані акаунти (адміністратори домену, root-користувачі, сервісні акаунти) є найбільш чутливими елементами IT-інфраструктури. Відсутність належного контролю над ними створює значні вектори атак, оскільки такі записи надають необмежені права на керування конфігураціями, доступ до конфіденційних даних та можливість обходу засобів захисту.

2. Аналіз загроз показав, що основними ризиками, пов'язаними з неконтрольованим доступом, є витіки даних, зловживання внутрішніх порушників (інсайдерів) та неможливість проведення якісного аудиту інцидентів. Підтверджено, що фінансові та репутаційні втрати від реалізації цих загроз значно перевищують вартість впровадження спеціалізованих захисних систем.

3. На основі кращих світових практик визначено, що ефективна система PAM повинна базуватися на принципі найменших привілеїв (PoLP), забезпечувати запис та моніторинг сесій у реальному часі, автоматизувати ротацію паролів та підтримувати механізми Just-In-Time доступу. Також критично важливою є відповідність регуляторним нормам.

4. Проведено порівняльний аналіз провідних PAM-платформ: CyberArk, BeyondTrust, Delinea та FortiPAM. За результатами порівняння за критеріями функціональності, вартості володіння, складності впровадження та інтеграційних можливостей, обрано рішення FortiPAM.

5. Встановлено, що архітектура FortiPAM побудована за модульним принципом і є ключовим елементом екосистеми Fortinet Security Fabric. Система реалізує трирівневу модель захисту (рівень доступу, ядро керування, цільові ресурси), що дозволяє ізолювати користувачів від прямої взаємодії з критичними активами, виступаючи єдиним захищеним шлюзом.

6. Визначено, що FortiPAM забезпечує повний цикл управління привілейованим доступом (PASM). До ключових функцій належать: безпечне зберігання та автоматична ротація секретів, гранульований контроль доступу на основі ролей (RBAC), а також моніторинг і відеофіксація сесій у реальному часі, що критично важливо для аудиту та розслідування інцидентів.

7. Обґрунтовано ефективність використання принципу ZTNA (Zero Trust Network Access) у FortiPAM. На відміну від традиційних VPN, ZTNA надає доступ до конкретних застосунків, а не до всієї мережі, і лише після перевірки ідентичності користувача та стану безпеки його пристрою через інтеграцію з FortiClient EMS.

8. Доведено, що інтеграція FortiPAM з іншими компонентами фабрики безпеки (FortiGate, FortiAuthenticator, FortiAnalyzer) дозволяє мінімізувати поверхню атаки, блокувати скомпрометовані пристрої та забезпечити захищений доступ як для локальних, так і для віддалених адміністраторів без необхідності постійного VPN-з'єднання.

9. Розроблено рекомендації мінімізації ризиків безпеки при використанні технології управління привілейованим доступом до інформаційної системи організації, яка забезпечить рівень захисту від витоку даних та несанкціонованого доступу.

ПЕРЕЛІК ПОСИЛАНЬ

1. What Is Privileged Access Management (PAM)? [Електронний ресурс] // CrowdStrike. URL: <https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/privileged-access-management-pam/> .
2. What is privileged access management (PAM)? [Електронний ресурс] // IBM. URL: <https://www.ibm.com/think/topics/privileged-access-management>.
3. Senhasegura Business X-Ray – July 2024 [Електронний ресурс] : [звіт]. – Режим доступу: URL: <https://lp.senhasegura.co/hubfs/website%20assets/Rich%20Materials/senhasegura%20BXR%20-%20July%202024.pdf.pdf> .
4. Access Management Security Risks and How to Mitigate Them [Електронний ресурс] // Netwrix Blog. URL: <https://netwrix.com/en/resources/blog/access-management-security-risks/> .
5. What is Privileged Access Management (PAM)? [Електронний ресурс] // Fortinet Cyber Glossary. URL: <https://www.fortinet.com/uk/resources/cyberglossary/privileged-access-management>.
6. Global Privileged Access Management Solutions Market Size, Share & Industry Trends Analysis Report [Електронний ресурс] // KBV Research. URL: <https://www.kbvresearch.com/privileged-access-management-solutions-market/> .
7. Senhasegura Documentation [Електронний ресурс]. URL: <https://docs.senhasegura.io/v4/docs/pt/senhasegura> .
8. FortiPAM: Privileged Access Management [Електронний ресурс] // Fortinet. URL: <https://www.fortinet.com/uk/products/fortipam>.
9. Introduction [Електронний ресурс] // FortiPAM Administration Guide (Version 1.7.1). URL: <https://docs.fortinet.com/document/fortipam/1.7.1/administration-guide/462068/introduction> .

10. User list [Електронний ресурс] // FortiPAM Administration Guide (Version 1.7.1). URL: <https://docs.fortinet.com/document/fortipam/1.7.1/administration-guide/952142/user-list> .

11. What is ZTNA architecture? [Електронний ресурс] // ZTNA Architecture Guide (FortiOS 7.0.0). URL: <https://docs.fortinet.com/document/fortigate/7.0.0/ztna-architecture/800134/what-is-ztna-architecture> .

12. Петухова М.О., Мазур А.Т. Технологія управління привілейованим доступом: порівняння рішень. *Актуальні проблеми кібербезпеки: матеріали всеукраїнської наук.-практ. конф.*, м. Київ: ДУІКТ, 29 жовт. 2025р. Київ. С. 21-23.