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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо контролю доступу до корпоративних систем та аналіз їх реалізації на прикладі Fudo PAM»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

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

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Данило ВОСТРИХ
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
ВОСТРИХ Данило
(прізвище, ім'я)

Керівник ст.. викладач Коровайченко Ю.Ю.
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ВСТУП

Актуальність дослідження. Контроль доступу до корпоративних інформаційних систем є одним з фундаментальних елементів забезпечення інформаційної безпеки організації. У сучасних умовах розвитку кіберзагроз, особливу увагу слід приділяти саме привілейованому доступу — доступу адміністраторів, інженерів, постачальників послуг, що мають широкі повноваження у межах IT-інфраструктури. Саме через такі облікові записи найчастіше відбувається зловживання правами, компрометація або цілеспрямовані атаки.

Наявність привілейованих облікових записів створює значний вектор ризику. За даними міжнародних досліджень, велика частина успішних атак супроводжується викраденням або використанням привілейованих облікових записів. Неконтрольований доступ до критичних систем може призвести до втрати конфіденційних даних, знищення або модифікації інформації, саботажу бізнес-процесів та значних фінансових збитків.

Системи керування привілейованим доступом (Privileged Access Management, PAM) покликані вирішити ці проблеми. Вони забезпечують контроль, моніторинг, обмеження та аудит дій користувачів із підвищеними повноваженнями. Рішення PAM дозволяють впровадити принцип найменших привілеїв, застосовувати тимчасовий доступ (Just-in-Time), вести запис сесій, виявляти аномальну активність та запобігати витоку облікових даних.

Серед доступних на ринку рішень важливе місце займає Fudo PAM — система, яка поєднує в собі функціональність proxy-контролю, запису сесій, автентифікації, інжекції облікових даних та поведінкової аналітики. Простота впровадження та підтримка ключових протоколів (SSH, RDP, HTTP/S тощо) роблять це рішення особливо привабливим для середніх та великих організацій.

Враховуючи вищезазначене, тема цієї кваліфікаційної роботи є актуальною, оскільки забезпечення ефективного контролю доступу до інформаційних ресурсів організації є необхідною умовою для підтримання цілісності, конфіденційності та

доступності даних, а також для відповідності сучасним вимогам нормативного регулювання та стандартів кібербезпеки.

Об'єкт дослідження – система контролю доступу до корпоративних систем.

Предмет дослідження – методи та засоби керування привілейованим доступом.

Мета роботи – дослідити сучасні методи контролю доступу, проаналізувати архітектуру та функціонал PAM систем, а також розробити рекомендації щодо контролю доступу до корпоративних ресурсів.

Наукові завдання:

проаналізувати проблематику контролю доступу до критичних систем у корпоративному середовищі;

дослідити підходи та моделі керування привілейованим доступом;

вивчити архітектуру та функціональні можливості Fudo PAM;

розробити варіант впровадження Fudo PAM;

сформулювати практичні рекомендації щодо контролю доступу за допомогою PAM-рішень.

Методи дослідження:

опрацювання наукової та технічної літератури;

аналіз нормативних документів і стандартів (зокрема ISO/IEC 27001, 27002, NIST SP 800-53, CIS Controls);

вивчення технічної документації Fudo PAM;

моделювання сценаріїв доступу у демо-середовищі;

Практичне значення одержаних результатів

У результаті виконання роботи сформовано практичний приклад організації контролю доступу до корпоративних систем на базі Fudo PAM та розроблено загальні рекомендації щодо контролю доступу до корпоративних систем.

Запропонований підхід може бути адаптований у практичній діяльності фахівців з інформаційної безпеки для захисту IT-інфраструктури від внутрішніх та зовнішніх загроз пов'язаних з привілейованими обліковими записами.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМ КОНТРОЛЮ ДОСТУПУ ДО КОРПОРАТИВНИХ СИСТЕМ

1.1 Аналіз загроз та проблем контролю доступу в корпоративному середовищі

Контроль доступу є фундаментальним компонентом системи інформаційної безпеки, який забезпечує регулювання прав користувачів на доступ до інформаційних ресурсів. Його неефективна реалізація створює значні ризики для конфіденційності, цілісності та доступності даних, що особливо критично для корпоративних систем. Міжнародні стандарти з кібербезпеки, зокрема ISO/IEC 27001 та NIST SP 800-53, приділяють особливу увагу необхідності належної організації процесу керування доступом [1, 2].

Однією з найпоширеніших проблем є надлишкові привілеї, що суперечить принципу найменших повноважень (least privilege). Згідно з даними звіту Verizon DBIR за 2023 рік [3], з 16,312 проаналізованих інцидентів безпеки, в 5,199 було підтверджено витік даних. Ці цифри свідчать про зростаючу загрозу кібербезпеці, зокрема щодо керування привілейованим доступом.

Одним із ключових висновків звіту є те, що 74% усіх порушень безпеки включали людський фактор, включаючи помилки, зловживання привілеями, використання вкрадених облікових даних та соціальну інженерію. Це підкреслює необхідність впровадження ефективних механізмів контролю та моніторингу привілейованого доступу.

Ускладнення керування правами доступу спостерігається в умовах відсутності **централізованої моделі керування обліковими записами**. Такий стан призводить до дублювання прав та неконтрольованого зростання кількості облікових записів. CIS Controls, зокрема 6.6 та 6.7, вимагає централізованого керування доступом з фіксацією усіх змін у правах та облікових записах [4].

Ще одним суттєвим ризиком є **відсутність належного запису та аудиту дій**

користувачів. Без реєстрації спроб входу, сесій адміністраторів та змін до конфігурацій неможливо виявити інциденти або провести ефективне розслідування. NIST SP 800-53 у рамках контролів AU-2 та AU-12 передбачає ведення журналів подій та їх збереження для подальшого аналізу [2].

Окрему увагу варто приділити **питанням автентифікації**, де використання лише одного фактора (наприклад, пароля) не забезпечує достатній рівень захисту. У зв'язку з цим сучасні стандарти рекомендують впровадження багатофакторної автентифікації (MFA), особливо для привілейованих облікових записів. Це зазначено, зокрема, в CIS Control 6.3-6.5[4].

До ключових ризиків, що виникають у разі неефективного контролю доступу, можна віднести:

- несанкціоноване підключення до критичних ресурсів;
- використання облікових даних, що не було відкликано після зміни ролі чи звільнення працівника;
- привласнення привілеїв через ескалацію прав доступу;
- відсутність обліку та контролю дій користувачів з розширеним доступом, що ускладнює розслідуванню інцидентів ;

Ефективна протидія зазначеним загрозам передбачає застосування низки заходів організаційного та технічного характеру, серед яких ключовими є:

- впровадження ролевої (RBAC) або атрибутивної (ABAC) моделі доступу;
- використання засобів централізованого керування обліковими записами;
- аудит і ревізія прав доступу на регулярній основі;
- обов'язкова мультифакторна автентифікація для привілейованих облікових записів;
- запис, зберігання та аналіз сесій користувачів;
- застосування рішень класу PAM, які дозволяють реалізувати комплексний контроль за використанням доступу до критичних ресурсів.

Таким чином, реалізація сучасної системи контролю доступу має базуватись не лише на технічній реалізації механізмів автентифікації та авторизації, а й на

дотриманні вимог міжнародних стандартів, що встановлюють принципи керування доступом як процесу в межах системи інформаційної безпеки організації.

1.2 Підходи та моделі реалізації контролю доступу.

Реалізація контролю доступу до інформаційних систем може ґрунтуватися на різних моделях, які формують основу для визначення, хто, коли і за яких умов може взаємодіяти з певними об’єктами системи. Вибір відповідної моделі повинен базуватися на особливостях організаційної структури, рівні критичності ресурсів та вимогах до безпеки. Сучасні стандарти інформаційної безпеки рекомендують застосування таких моделей, як **DAC, MAC, RBAC, ABAC** тощо.

DAC було вперше визначене у Trusted Computer System Evaluation Criteria (TCSEC) як засіб обмеження доступу до об’єктів на основі ідентичності суб’єктів та/або груп, до яких вони належать. Керування є дискреційним у тому сенсі, що суб’єкт із певним доступом може передавати цей доступ (можливо, опосередковано) будь-якому іншому суб’єкту (якщо це не обмежено обов’язковим керування доступом) [5]. DAC є однією з найперших і водночас найпростіших моделей керування доступом. Її ключова особливість полягає у тому, що контроль над доступом до ресурсів здійснюється на розсуд власника об’єкта. Іншими словами, користувач, який створив об’єкт (файл, каталог, процес тощо), або отримав на нього права власності, має повноваження самостійно визначати, хто з інших користувачів системи може мати доступ до цього ресурсу, а також який саме — читання, запис, виконання тощо.

У класичній реалізації вона передбачає, що права доступу встановлюються для трьох категорій: власника об'єкта, групи, до якої належить власник, та інших користувачів. Ця модель реалізована в більшості UNIX-подібних операційних систем, де використовується система дозволів (rwx для кожної категорії), а також у Windows, де аналогічну роль відіграє Access Control List (ACL), яка визначає, які облікові записи і групи мають доступ до об'єкта і з якими правами.

Попри простоту реалізації та гнучкість, модель DAC має низку суттєвих недоліків з точки зору інформаційної безпеки:

- Політики доступу не налаштовуються централізовано, що ускладнює забезпечення відповідності нормативним вимогам та стандартам безпеки.

Адміністратор не має гарантованого механізму контролю над тим, які об’єкти і кому доступні.

- Користувач, якому було надано доступ до ресурсу, може передати його іншим користувачам (якщо система це дозволяє), навіть без відома або дозволу адміністратора. Це створює ризик неконтрольованого поширення доступу.
- Через залежність від рішень кінцевого користувача існує висока ймовірність помилкового або недбалого надання доступу до конфіденційної інформації. Це особливо критично в корпоративному середовищі, де вимоги до захисту даних є підвищеними.
- Оскільки програми запускаються з правами користувача, який їх ініціює, зловмисне ПЗ може отримати доступ до всіх ресурсів, доступних цьому користувачу.

Схему моделі зображено на рисунку 1.2.1

Рис. 1.2.1 Discretionary Access Control

MAC характеризується централізованим підходом до визначення прав доступу, за якого користувачі не мають можливості самостійно змінювати правила взаємодії з об'єктами. Політики доступу встановлюються адміністраторами системи або уповноваженими суб'єктами безпеки, а їхнє виконання є обов’язковим для всіх користувачів, включно з власниками об’єктів. Унаслідок цього забезпечується жорстке дотримання регламентованих правил доступу, що особливо важливо в середовищах з підвищеними вимогами до захисту інформації.

MAC реалізує політику, засновану на рівнях секретності, які присвоюються як об’єктам, так і суб’єктам. Доступ дозволяється лише за умови, що рівень допуску суб’єкта відповідає або перевищує рівень секретності об’єкта. На додаток до перевірки рівнів конфіденційності та допуску (тобто відповідності класифікацій між суб’єктом і об’єктом), операційні системи також враховують відповідність категорій між суб’єктом і об’єктом. Класифікація «Надсекретно» не надає користувачу автоматичного доступу до файлу, якщо він не є членом необхідної категорії, визначеної для цього об’єкта [6]. Такий підхід дозволяє ефективно запобігати несанкціонованому доступу та витоку конфіденційних даних. Найпоширенішими прикладами впровадження цієї моделі є державні, військові та критичні інфраструктурні об'єкти, де недопущення витоку інформації має пріоритетне значення.

Разом з тим, модель MAC має низку обмежень, які ускладнюють її застосування в динамічному корпоративному середовищі. По-перше, процедура адміністрування таких політик є складною та трудомісткою, оскільки будь-які зміни до системи прав вимагають ручного втручання адміністратора. По-друге, відсутність можливості швидкого внесення винятків або делегування частини повноважень робить систему негнучкою щодо змін у ролях користувачів або організаційній структурі. По-третє, для ефективного функціонування моделі необхідна наявність спеціалізованого програмного забезпечення, чітке налаштування рівнів секретності та відповідна підготовка персоналу, що зумовлює високі витрати на впровадження та супровід.

Таким чином, незважаючи на високу ефективність MAC у середовищах з жорсткими вимогами до інформаційної безпеки, її використання вимагає обґрунтованого підходу, враховуючи витрати на адміністрування та потребу в організаційній дисципліні.

Схему моделі зображено на рисунку 1.2.2

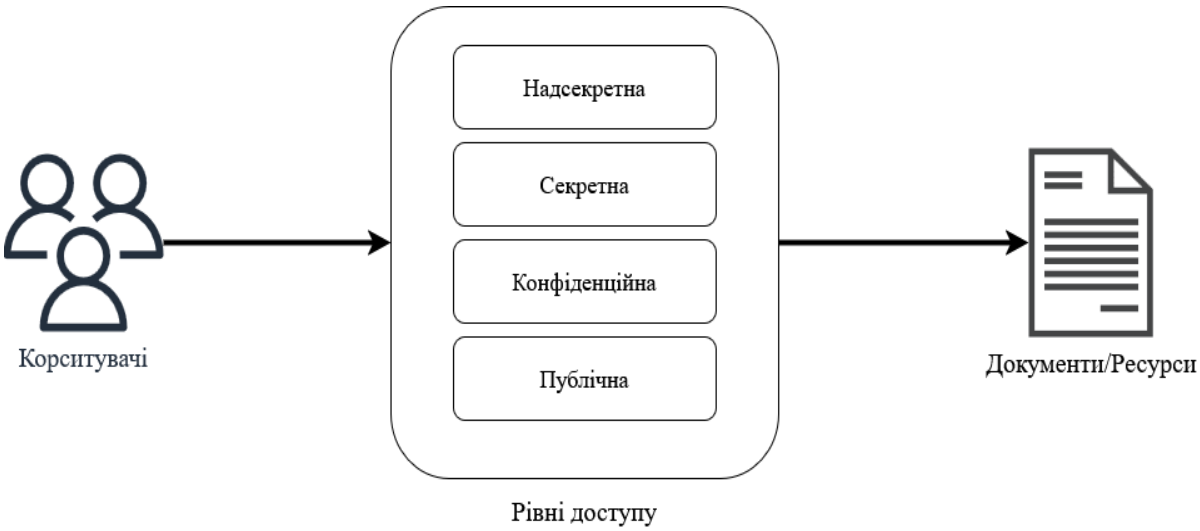

Рис. 1.2.2 Mandatory Access Control

RBAC — одна з найпоширеніших і водночас ефективних моделей керування доступом у корпоративних інформаційних системах. Основний принцип RBAC [7] полягає в тому, що права доступу призначаються не окремим користувачам безпосередньо, а ролям, які відображають функціональні обов’язки або належність до певної категорії в межах організаційної структури. Користувачі, у свою чергу, отримують одну або кілька ролей, що автоматично визначає їхні можливості взаємодії з інформаційними ресурсами.

Такий підхід дозволяє формалізувати та централізувати політики доступу, значно полегшуючи процес адміністрування, особливо у великих або ієрархічно складних організаціях. Наприклад, роль “бухгалтер” може включати доступ до фінансових систем і звітності, тоді як роль “системний адміністратор” охоплюватиме повноваження для керування інфраструктурними ресурсами. Завдяки цьому зміни в посадових обов’язках або переміщення працівників між відділами потребують лише коригування набору ролей без необхідності змінювати індивідуальні права для кожного користувача.

Модель RBAC також сприяє автоматизації процесів контролю доступу, забезпечує кращу відповідність нормативним вимогам та внутрішнім політикам безпеки, а також дозволяє ефективно реалізувати принцип мінімальних привілеїв. Зокрема, вона рекомендована до впровадження відповідно до пункту 6.8 CIS Controls [4] як одна з базових практик керування правами доступу в інформаційних системах.

Таким чином, RBAC є гнучким рішенням для компаній, які прагнуть забезпечити контрольований і структурований розподіл доступу відповідно до функціональних обов’язків персоналу.

Схему моделі зображено на рисунку 1.2.3

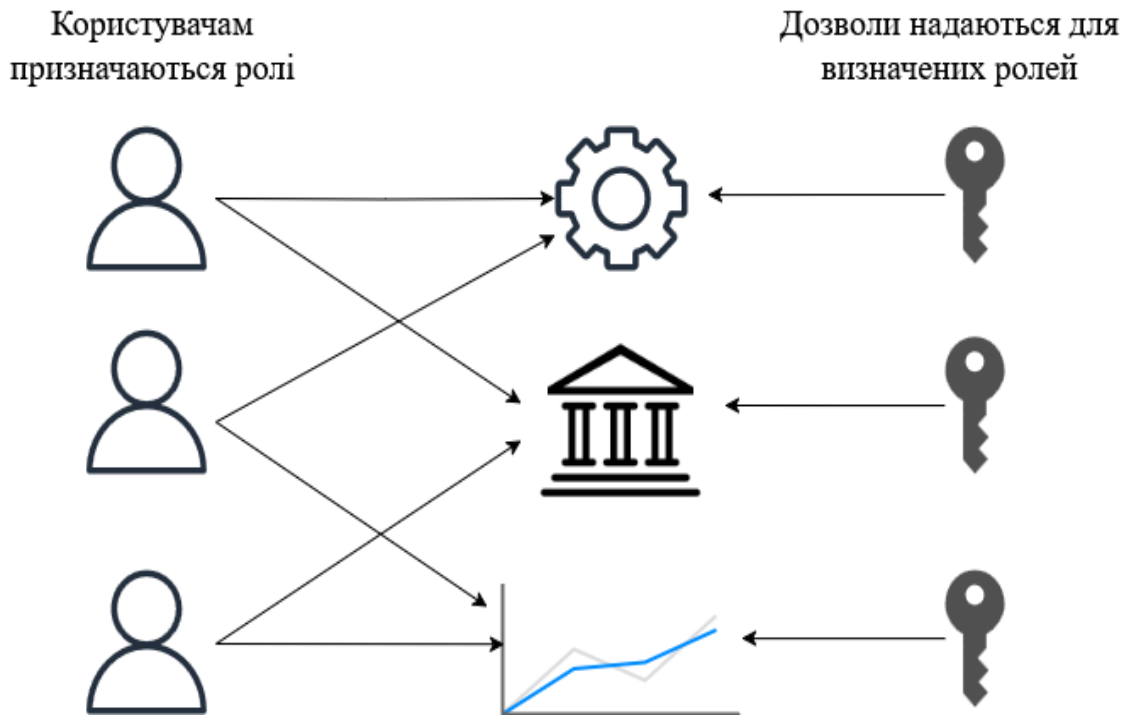

Рис. 1.2.3 Role-Based Access Control

Модель атрибутивного управління доступом (**ABAC**) є контекстно орієнтованою парадигмою контролю доступу, в якій прийняття рішень здійснюється на основі сукупності атрибутів суб'єкта, об'єкта, дії та умов [8]. На відміну від традиційних моделей, таких як DAC або RBAC, у яких контроль доступу базується на обліковому записі чи належності до ролі, ABAC враховує ширший контекст доступу, що дозволяє реалізовувати гнучкі та динамічні політики.

Атрибути, які використовуються для прийняття рішень, можуть включати характеристики користувача (посада, рівень доступу, приналежність до підрозділу), ресурсу (тип даних, рівень конфіденційності), а також умови запиту (час доби, тип пристрою, геолокація тощо). Наприклад, політика може передбачати дозвіл на доступ лише в робочий час, лише з корпоративного пристрою, який відповідає стандартам безпеки, і лише для користувачів із чинним цифровим сертифікатом.

ABAC забезпечує детальний контроль над доступом та здатність адаптувати політики безпеки до складних середовищ, таких як хмарні платформи, медичні системи або фінансові установи, де потрібна точна відповідність регуляторним вимогам та стандартам кібербезпеки, таким як: GDRP, PCI DSS, NIST, HIPPA тощо. Визначальною перевагою ABAC є можливість визначення універсальних політик,

які не потребують явного переліку всіх суб’єктів чи ролей, а натомість базуються на властивостях, що оцінюються в момент запиту.

Однак з плином часу гнучкість цієї моделі може ускладнювати її практичне впровадження. Зі зростанням кількості атрибутів та складності умов виникає потреба в системах керування політиками PAP та централізованому механізмі оцінки політик PDP, що значно підвищує вимоги до архітектури системи доступу. Надмірна деталізація політик може призвести до труднощів в адмініструванні, суперечностей у правилах та потенційних помилок конфігурації, що знижує керованість та прозорість політик доступу.

Схему моделі зображено на рисунку 1.2.4

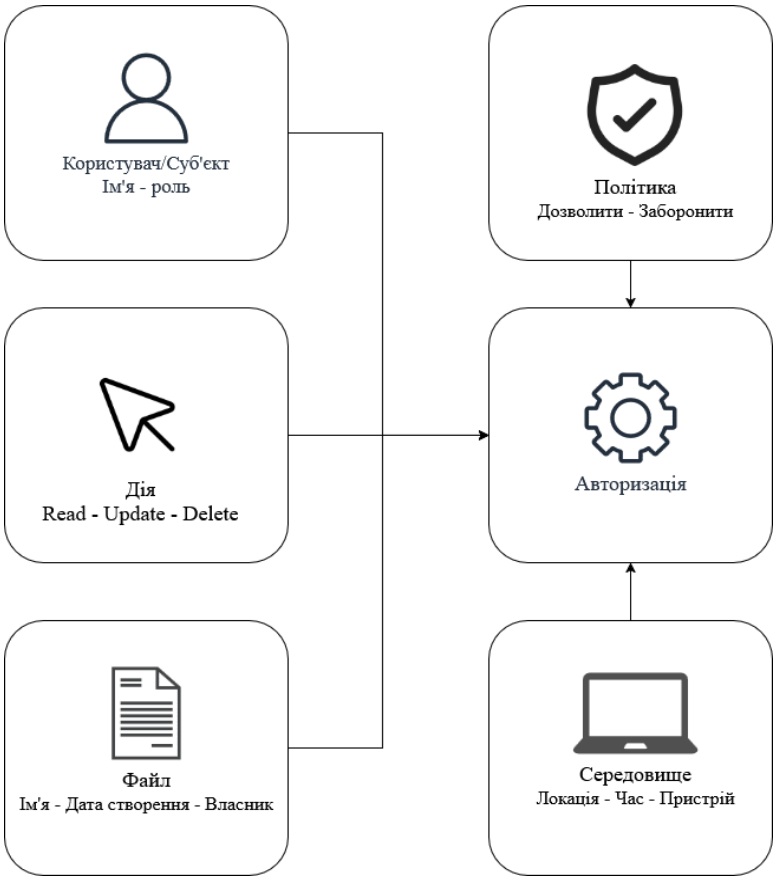

Рис. 1.2.4 Attribute-Based Access Control

Узагальнюючи викладене, можна стверджувати, що моделі управління доступом — DAC, MAC, RBAC та ABAC — є фундаментальними концепціями, які визначають правила взаємодії між суб’єктами й об’єктами в інформаційних системах. Кожна з них має свої переваги й обмеження, що зумовлює доцільність їх використання залежно від організаційного контексту, вимог до безпеки та рівня контролю.

Варто зазначити, що ці моделі не є взаємовиключними, і в сучасних системах доступу часто реалізуються комбіновані підходи, які поєднують переваги кількох моделей. У цьому контексті важливу роль відіграють рішення класу PAM, які спрямовані на захист привілейованих облікових записів, контроль над діями користувачів з розширеними правами, а також зниження ризиків, пов’язаних із несанкціонованим доступом до критичних ресурсів чи зловживання привілеями.

2 АНАЛІЗ МЕТОДІВ ТА КОНТРОЛЮ ДОСТУПУ ДО КОРПОРАТИВНИХ СИСТЕМ НА БАЗІ PAM-СИСТЕМ

2.1 Привілейовані облікові записи

У сучасних інформаційно-комунікаційних системах привілеї визначаються як набір прав або повноважень, що дозволяють користувачеві або обліковому запису виконувати дії, недоступні звичайним користувачам. Це може включати зміну конфігурацій систем, адміністрування мережевих пристроїв, керування обліковими записами, запуск системних процесів або отримання доступу до критично важливої чи конфіденційної інформації тощо.

Крім традиційних облікових записів, що асоціюються з реальними користувачами, у сучасних корпоративних IT системах значну роль відіграють так звані неприв’язані до людини облікові записи (non-human accounts). Ця категорія включає сервісні, програмні (application/service), інтерфейсні акаунти (API accounts), а також облікові записи інтеграцій, які використовуються для автоматизованого обміну даними між системами.

Non-human accounts є невід’ємною частиною цифрової інфраструктури і забезпечують взаємодію між програмними компонентами, сервісами та пристроями. Наприклад, обліковий запис бази даних, що використовується веб-додатком для аутентифікації до серверу СУБД. Зазвичай такі облікові записи мають значні привілеї, оскільки їм необхідно забезпечити виконання складних операцій, як-от зчитування великих обсягів даних, запис, видалення або конфігурування елементів системи. Ці облікові записи в свою чергу можна поділити на ті з якими користувачі не взаємодіють як описано в прикладі вище, а також інтерактивні акаунти. Найбільш поширеною категорією таких облікових записів є системні або адміністративні. Це, зокрема, облікові записи root у середовищах Linux/Unix або Administrator у Windows-системах [9].

Однією з головних проблем у контексті безпеки є те, що non-human accounts рідко змінюють паролі, часто мають однакові облікові дані на кількох системах і не асоціюються з конкретним відповідальним користувачем. Крім того, відсутність належного моніторингу їхньої поведінки може призвести до того, що зловмисник отримає доступ до таких акаунтів і використовуватиме їх для непомітного проникнення в інші частини інфраструктури, приховуючи свою активність за автоматизованими процесами.

Крім того, привілейовані облікові записи загалом часто не підлягають достатньому контролю або моніторингу, що створює додаткову площину для потенційного зловживання. У багатьох організаціях відсутнє належне розмежування обов'язків чи контроль доступу, що може призвести до того, що однин користувач матиме змогу самостійно створювати, змінювати або видаляти критично важливі елементи.

В контексті керування доступом, саме привілейовані облікові записи потребують найвищого рівня захисту, що передбачає як організаційні, так і технічні заходи. Системи PAM є відповіддю на цю потребу, забезпечуючи контроль, обмеження та моніторинг дій користувачів з такими обліковими записами.

2.2 Аналіз технології PAM, історії розвитку та основних моделей впровадження

PAM — це клас рішень кібербезпеки, що спрямований на виявлення облікових записів, аудит, обмеження та контроль доступу привілейованого доступу до критичних IT-ресурсів компанії. У вузькому розумінні PAM включає механізми і політики, що забезпечують безпечне зберігання облікових даних, контроль над їх використанням, а також фіксацію та аналіз дій користувачів, що виконують операції від імені таких облікових записів. Відповідно до Національного інституту стандартів і технологій США (NIST), привілейований доступ слід розглядати як

контрольований та суворо обмежений канал, через який користувач або процес отримує розширені повноваження для виконання дій над об'єктами системи, що перевищують стандартні можливості звичайного користувача [10].

Керування привілейованим доступом охоплює не лише самі облікові записи з підвищеними правами, але й середовище, в якому цей доступ реалізується. PAM виконує роль посередника між користувачем та ресурсом, при цьому ізолюючи критичні об'єкти і знижуючи ризик компрометації шляхом запровадження процедур, таких як: автоматична ротація паролів, мультифакторна автентифікація, обмеження сесій за часом тощо.

Перед тим як заглибитися в технічні особливості PAM варто розглянути історію виникнення цієї технології. Технології керування привілейованим формувалися у відповідь на зростаючі ризики, пов’язані з несанкціонованим або надмірним доступом до критичних IT-систем. Витоки PAM можна прослідкувати до перших концепцій розмежування повноважень у мейнфреймах 1970-х років [11], коли системи потребували базових механізмів обмеження дій адміністратора для уникнення конфліктів інтересів. Однак на той час засоби обмеження доступу були тісно інтегровані з ОС і не забезпечували гнучкого або централізованого контролю. Цей варіант контролю доступу застосовувався для керування доступом до ключових ресурсів, дозволяючи або обмежуючи права доступу до даних після підтвердження особи користувача. Такий підхід допомав блокувати несанкціонований доступ і мінімізувати ризики, пов’язані з помилками авторизованих користувачів. Простіше кажучи, метод визначав, хто, до якої інформації та з якими правами може отримати доступ.

У 1990-х роках, на фоні зростання комп’ютерних мереж та дедалі більшого поширення клієнт-серверної архітектури, компанії почали усвідомлювати, що надмірно широкі повноваження привілейованих користувачів становлять значну загрозу. У той час контроль над такими акаунтами здебільшого зводився до адміністрування вручну: облікові записи root, admin або superuser часто не мали

обмежень, і лише неформальні політики або внутрішні інструкції стримували їх від зловживань.

У 2000-х роках виникла потреба у централізованому підході до управління такими обліковими записами, що призвело до появи перших спеціалізованих рішень, які почали реалізовувати базові принципи PAM: інвентаризацію облікових даних, контрольований доступ, зберігання паролів у зашифрованому сховищі, аудит дій користувачів. У цей період з'являються такі ключові технології, як credential vaulting, запис сесій та ізоляція з'єднань через проксі-сервер. Перші інтерфейси PAM були відносно простими, часто обмежувались консольними або локальними веб-панелями, але вже дозволяли зменшити ризики, пов'язані з використанням привілейованих облікових записів.

Поступово PAM перестав бути внутрішнім адміністративним інструментом і трансформувався у частину стратегії корпоративної безпеки. У 2010-х [12] роках з появою DevOps та хмарних сервісів зміщується фокус з лише людей на машини: виникає потреба у контролі non-human accounts, які використовуються для автоматизації процесів. Рішення PAM починають підтримувати ротацію API-ключів, SSH-ключів, токенів доступу до хмарних сервісів.

На сучасному етапі PAM все більше переходить до адаптації Zero Trust архітектури. Моделі, що ґрунтуються на постійних перевірках, контекстній автентифікації, обмеженні часу доступу та мінімізації привілеїв, а також концепції JIT та Zero Standing Privileges стають загальноприйнятими практиками. Більше того, впроваджується поведінкова аналітика доступу, автоматизоване реагування на аномалії, інтеграція з SIEM та іншими рішеннями кібербезпеки, що дозволяє реалізувати повний цикл - від виявлення до реагування на інцидент.

Одним з інших нововведень стало Cloud PAM – це передбачає використання PAM як послуги (PAM-as-a-Service), що знаходиться у публічному або приватному хмарному середовищі. Цей підхід дозволяє скористатися перевагами швидкого впровадження, автоматизованих оновлень, гнучкого масштабування та високої

доступності. Основні постачальники хмарних платформ (AWS, Azure, GCP) або спеціалізовані постачальники PAM-рішень надають готову інфраструктуру, де клієнт відповідає лише за конфігурацію політик доступу. Cloud PAM особливо зручний для організацій із розподіленими командами або гібридними середовищами. Основним викликом в такій конфігурації стає питання довіри до стороннього провайдера, регуляторних обмеженнь щодо зберігання персональних, конфіденційних та інших даних, а також потенційні труднощі інтеграції з локальними системами.

Традиційною моделлю ж було локальне впровадження. У такій конфігурації система PAM та усі її компоненти розміщуються у внутрішній інфраструктурі компанії. Модель передбачає встановлення програмного забезпечення на фізичні або віртуальні сервери в межах корпоративної мережі. Такий підхід надає повний контроль над конфігурацією, оновленнями, безпекою та доступом до системи. Він є доцільним для компаній із суворими вимогами до зберігання даних, обмеженнями на передачу інформації за межі організації, або для середовищ із ізольованим (air-gapped) доступом. Недоліками є складність масштабування, потреба в окремих фахівцях для адміністрування системи та додаткові витрати на інфраструктуру.

2.3 Аналіз основних концептів, принципів та ключових технічних можливостей керування привілейованим доступом

У попередньому розділі, присвяченому історії розвитку технологій привілейованого доступу, вже частково були згадані ключові принципи та концепції, що лежать в основі сучасних рішень PAM. Зокрема, йшлося про прагнення мінімізувати рівень доступу до критичних ресурсів, забезпечити постійний контроль над сесіями та зменшити обсяг довіри до користувачів. Проте ці підходи є не просто наслідком еволюції практик, а самостійними концепціями,

які формують теоретичну й практичну основу архітектури систем керування привілейованим доступом.

У цьому підрозділі буде розглянуто основні принципи та моделі, що використовуються в межах PAM: принцип найменших привілеїв (Least Privilege), концепція відсутності постійних привілеїв (Zero Standing Privileges), а також принцип розділення обов’язків (Separation of Duties). Кожен із розглянутих принципів має власне призначення, сфери застосування, й переваги, що й обумовлює необхідність їх детального аналізу.

Принцип найменших привілеїв є фундаментальною концепцією в галузі управління доступом і широко застосовується в рамках реалізації систем PAM. Суть цього принципу згідно контролю AC-6 в рамках NIST SP 800-53 [2] полягає в тому, що кожен суб'єкт — користувач, процес або система — повинен мати доступ лише до тих ресурсів та виконувати лише ті дії, які є необхідними для виконання його поточних функціональних обов’язків. Відповідно, будь-яке надання надлишкових або постійних привілеїв розглядається як ризик, що підвищує ймовірність внутрішніх порушень, компрометації облікових записів або несанкціонованої ескалації прав доступу.

У контексті систем PAM, реалізація принципу найменших привілеїв включає автоматизоване управління доступом до критичних систем та ресурсів, при якому права надаються лише на час необхідного виконання завдання. Так, наприклад, адміністратор бази даних отримає доступ до серверу лише протягом визначеного інтервалу часу і лише для виконання конкретної операції, після чого права буде автоматично відкликано. Це може бути забезпечено за допомогою інтегрованих механізмів, таких як JIT, контрольована ескалація привілеїв, а також обмеження доступу до окремих облікових записів за допомогою правил і політик.

Застосування принципу найменших привілеїв дає змогу мінімізувати потенційний вектор атак, зменшуючи кількість потенційних точок входу в системи, які можуть бути скомпрометовані. Водночас це дозволяє зменшити обсяг

шкідливих дій у разі захоплення облікового запису, оскільки зловмисник не отримає ширших прав, ніж ті, що надаються за конкретним призначенням. Важливо підкреслити, що дотримання цього принципу не є одноразовим заходом, а вимагає постійного перегляду і коригування прав доступу відповідно до зміни ролей користувачів та інфраструктури.

Принцип розділення обов'язків (Separation of Duties) є ще одним із ключових елементів моделі керування привілейованим доступом, що спрямований на мінімізацію ризиків, пов'язаних із надмірною концентрацією повноважень в однієї особи. Згідно з цим принципом, що описаний в контролі AC-5 в рамках NIST SP 800-53 [2], виконання критичних або потенційно ризикованих операцій має бути розподілене між кількома суб'єктами, щоб жоден із них не мав повного контролю над усім процесом без залучення інших осіб.

В контексті PAM-рішень, реалізація цього принципу передбачає розмежування ролей між користувачами, адміністраторами, аудиторами та іншими учасниками процесів. Наприклад, один адміністратор може мати право на зміну конфігурацій, тоді як інший — лише на їх затвердження. Такий поділ дозволяє ефективно запобігати шахрайству, помилкам та зловживанням

Технічна реалізація у системах PAM зазвичай включає гнучке керування ролями, політиками доступу, журналюванням подій та впровадженням механізмів погодження (approval workflows[13]). У таких сценаріях запити на доступ до критичних ресурсів можуть вимагати схвалення з боку незалежного адміністратора або служби безпеки. Крім того, важливу роль відіграє можливість розмежування доступу до конфіденційної інформації в межах сесій — наприклад, обмеження можливості одночасного перегляду і редагування чи копіювання даних.

Невиконання принципу розділення обов'язків може призвести до ситуацій, коли один працівник може створити обліковий запис, видати йому права адміністратора та приховати свої дії від аудиту, що значно ускладнює виявлення порушень.

І останній концепт - Zero Standing Privileges [14] полягає в усуненні постійно присутніх привілейованих прав доступу у користувачів або сервісів. Замість зберігання адміністративних прав, доступ надається лише на момент виконання конкретного завдання, після чого автоматично відкликається. Такий підхід забезпечує суттєве зменшення площі атаки, обмежуючи можливості зловмисника у разі компрометації облікового запису.

На відміну від традиційних моделей, де адміністратор або сервіс має постійний доступ до критичних систем, ZSP вимагає динамічного запиту доступу з наступною перевіркою і погодженням. Це може включати багатофакторну автентифікацію, оцінку контексту (наприклад, часу, геолокації, типу пристрою) та аналіз поведінки користувача.

Практична реалізація принципу ZSP часто базується на механізмах JIT. У цьому випадку система генерує тимчасові облікові дані або відкриває сеанс лише на необхідний період. Після завершення сесії доступ автоматично припиняється, а всі дії фіксуються. ZSP ефективно доповнює інші принципи безпеки в PAM-системах, зокрема Least Privilege і Separation of Duties, формуючи комплексний підхід до керування доступом.

Системи керування привілейованим доступом реалізують комплекс технічних та адміністративних засобів, які дозволяють забезпечити контроль доступу до критичних ресурсів компанії. Їх можливості можуть відрізнятися залежно від обраної архітектури та рішення, однак існує набір основних можливостей, характерних для більшості рішень [15].

Credential Vault - призначений для безпечного зберігання, управління та контролю доступу до облікових даних привілейованих користувачів та сервісів. Його основною метою є мінімізація ризиків, пов’язаних із витоком або компрометацією облікових даних, шляхом централізації їх зберігання та застосування суворих політик доступу. Credential Vault реалізується як ізольоване програмно-апаратне або віртуалізоване сховище, в якому облікові дані

зберігаються у зашифрованому вигляді із застосуванням криптографічних алгоритмів (наприклад, AES-256 або RSA-2048[16]). Доступ до цих даних обмежується згідно з політик ролей, рівнів привілеїв тощо, що визначаються фахівціями кібербезпеки. Додатково, всі операції доступу до сховища підлягають детальному журналюванню для подальшого аналізу. Одною з ключових можливостей Credential Vault є автоматична ротація облікових даних. Це надає змогу змінювати паролі на кінцевих точках (наприклад, на серверах, базах даних, мережевих пристроях) у заданий час або після кожного використання. Це усуває необхідність ручного керування паролями та зменшує ризик зловживань або повторного використання облікових даних. Однією з переваг використання Credential Vault є зменшення кількості людей, які безпосередньо знають облікові дані для доступу до критичних систем.

JIT [17] - є ключовою функціональною можливістю у сучасних системах керування привілейованим доступом, що реалізує один з основних принципів — zero standing privileges. Основна ідея полягає в тому, що користувачі отримують тимчасовий доступ до ресурсів не на постійній основі, а лише на конкретний, попередньо схвалений або заздалегідь визначений проміжок часу. Після завершення сесії або закінчення дозволеного періоду - доступ автоматично відкликається.

JIT реалізується різними технічними методами. Один із поширених підходів — динамічне створення тимчасових облікових записів з необхідним рівнем прав, які знищуються або деактивуються після завершення сесії. Інший підхід полягає в тимчасовому розширенні прав існуючого облікового запису з подальшим їх автоматичним відкликанням або ж використання одного облікового запису з автоматичною зміною паролю чи ключу після завершення сесії. У багатьох PAM-системах використовується механізм погодження, тобто перед наданням доступу користувач надсилає запит, що має бути схвалений уповноваженим адміністратором або системою на основі політик доступу. Це дозволяє забезпечити

запис використання привілейованих записів, контроль над контекстом (час, цільовий ресурс, причина доступу), а також запобігає зловживанням.

JIT суттєво знижує ризики, пов’язані з наявністю постійних привілеїв які можуть бути використані зловмисниками у разі компрометації облікового запису.

З практичної точки зору, JIT часто поєднується з іншими компонентами PAM, зокрема MFA та контролем сесій.

Запис та моніторинг сесій є одним із ключових елементів, оскільки забезпечує як оперативний контроль за діями користувачів у реальному часі, так і можливість ретроспективного аналізу з метою аудиту або розслідування інцидентів.

Під час сесії PAM здійснює повноцінний запис дій користувача, включаючи натискання клавіш, введені команди, рухи миші, перегляд вмісту вікон, а також доступ до файлів і зміну конфігурацій. Запис може здійснюватися у вигляді відео, журналу команд, збереження копій переданих файлів або їх комбінації, залежно від протоколу та обраних політик. Така інформація зберігається у зашифрованому вигляді і може бути доступною лише уповноваженим особам для перегляду в аналітичному або доказовому контексті.

Окрім запису, сучасні системи PAM надають можливість моніторингу сесій у режимі реального часу. Це означає, що відповідальні особи — наприклад, адміністратори безпеки — можуть спостерігати за поточними сесіями, отримувати сповіщення у разі підозрілих або небезпечних дій, а також виконувати автоматичні або ручні дії для попередження інцидентів. Такі дії можуть включати призупинення сесії, її примусове завершення або підключення адміністратора до сесії для спільної роботи.

Особливу роль у цьому контексті відіграють механізми розпізнавання патернів дій. Наприклад, використання регулярних виразів або модулів машинного навчання може дозволити виявляти ознаки несанкціонованого доступу або

зловмисної поведінки ще до того, як буде завдано шкоди. Це може бути основою для реалізації проактивного захисту привілейованих сесій.

Таким чином, запис і моніторинг сесій в PAM не є лише додатковими інструментами контролю, а становлять невід'ємну складову PAM-систем, що дозволяє забезпечити як запобігання інцидентів, так і документування кожної дії користувачів з привілейованим доступом.

Багатофакторна автентифікація дозволяє значно знизити ризик несанкціонованого доступу до критичних ресурсів навіть у випадку компрометації облікових даних. MFA [18] базується на принципі використання декількох незалежних факторів автентифікації, які зазвичай класифікуються як: щось, що користувач знає (наприклад, пароль), щось, що він має (наприклад, токен або мобільний пристрій), та щось, чим він є (біометричні дані).

Інтеграція MFA в PAM-системи зазвичай реалізується на двох рівнях: при вході до самої системи PAM, а також при доступі до конкретних ресурсів, що захищені PAM (наприклад, при ініціалізації RDP або SSH-сесії). Це дозволяє не тільки убезпечити вхід до самої платформи керування доступом, а й унеможливити пряме проникнення до кінцевих систем, навіть якщо зловмисник обійде перший рівень захисту.

У підсумку, розглянуті функціональні можливості систем PAM демонструють їхню ключову роль у забезпеченні контролю та захисту привілейованого доступу в сучасних корпоративних системах. Credential vault, механізму JIT, запис та моніторинг сесій та багатофакторна автентифікація забезпечують комплексний захист від загроз, що пов'язані з компрометацією облікових записів, зловживанням привілеями та несанкціонованими діями.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ КОНТРОЛЮ ДОСТУПУ ДО КОРПОРАТИВНИХ СИСТЕМ

3.1 Архітектура та компоненти рішення Fudo PAM

Fudo PAM — це рішення для керування привілейованим доступом, що забезпечує контроль, нагляд і захист підключень до критично важливих елементів IT-інфраструктури. Рішення підтримує роботу з різними типами протоколів, включно з SSH, RDP, VNC, HTTP(S), Telnet, MySQL, Oracle, Modbus та іншими, що дозволяє охопити широкий спектр IT-систем. Усі сесії проходять через Fudo PAM, де вони автоматично записуються та перевіряються на наявність підозрілої поведінки. Це дає змогу адміністраторам у режимі реального часу переглядати активні підключення, втручатися в них у разі необхідності — з можливістю призупинення, завершення або спільної участі у сесії з користувачем, а також аналізувати дії з архіву вже завершених сеансів.

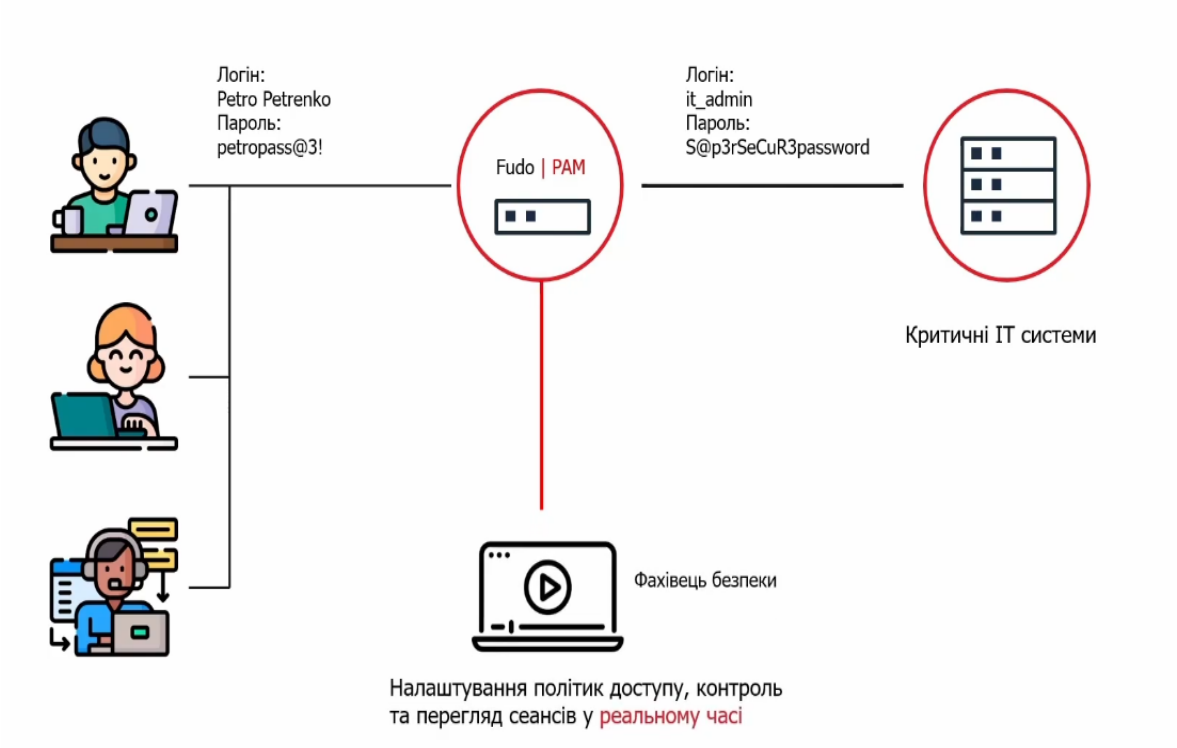

Рис. 3.1 Загальна архітектура рішення Fudo PAM

Режими з’єднання (Connection Modes)

Fudo PAM підтримує чотири режими підключення, які будуть розглянуті далі, що дозволяє інтегрувати систему до існуючої інфраструктури підприємства. Кожен режим визначає спосіб організації доступу користувача до цільового серверу та можливості контролю з боку системи Fudo PAM.

Transparent Mode - користувачі підключаються до цільового сервера, використовуючи його реальну IP-адресу. Fudo PAM перехоплює трафік, не змінюючи його структуру, що дозволяє зберегти існуючі мережеві налаштування. Такий підхід мінімізує необхідність змін у конфігурації клієнтських пристроїв.
Схему [19] роботи режиму зображено на рисунку 2.1.2.

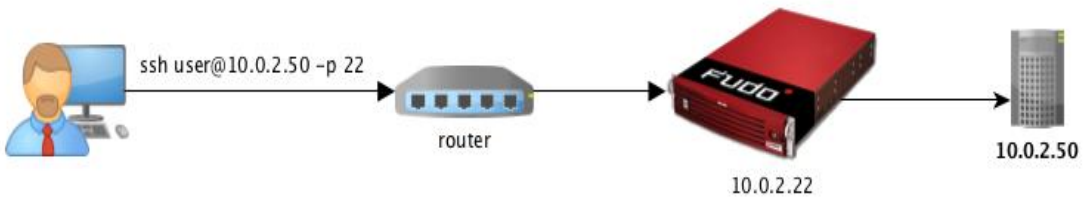

Рис. 3.1.2 Схема роботи режиму Transparent Mode

Gateway Mode — режим, у якому користувачі підключаються до цільового сервера, вказуючи його реальну IP-адресу. При цьому з’єднання проходить через Fudo PAM, який виступає як посередник на шляху трафіку. Fudo ініціює окреме з’єднання до сервера зі своєї IP-адреси, контролюючи увесь сеанс. Це дозволяє забезпечити повний моніторинг, запис дій користувача, застосування політик безпеки та, за необхідності, втручання в активну сесію.
Схему [19] роботи режиму зображено на рисунку 2.1.3.

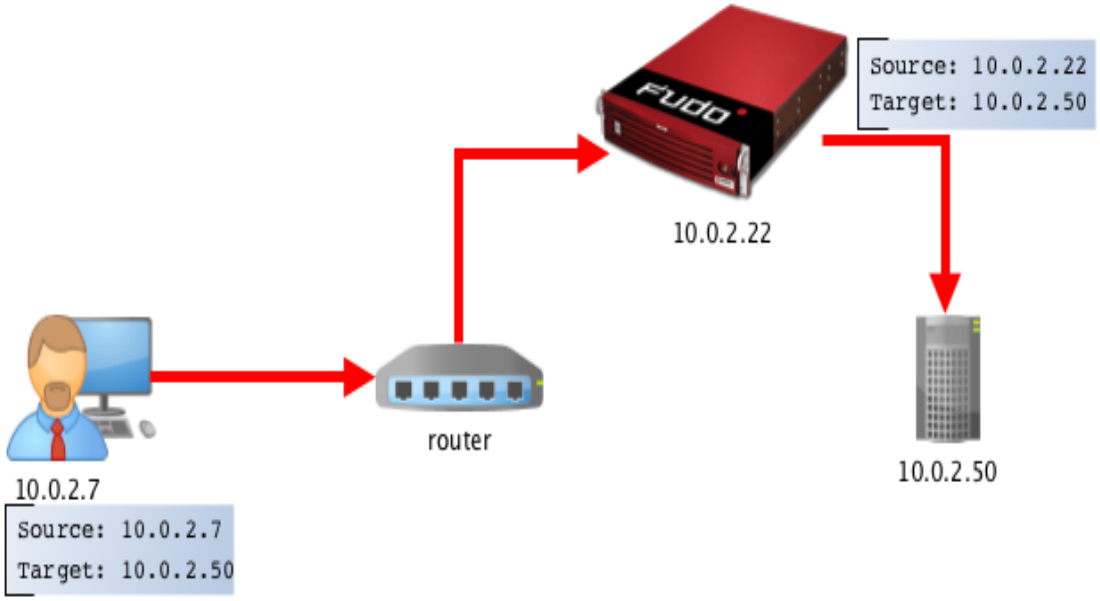

Рис. 3.1.3 Схема роботи режиму Getaway Mode

Proxy Mode - режим, у якому користувачі встановлюють з'єднання, вказуючи IP-адресу Fudo PAM разом із унікальним портом, що відповідає конкретному цільовому серверу. Завдяки цьому реальні IP-адреси серверів залишаються прихованими від користувачів, що підвищує рівень безпеки. Увесь трафік скеровується через Fudo PAM, що дозволяє приховати реальні IP-адреси серверів.

Схему [19] роботи режиму зображено на рисунку 2.1.4.

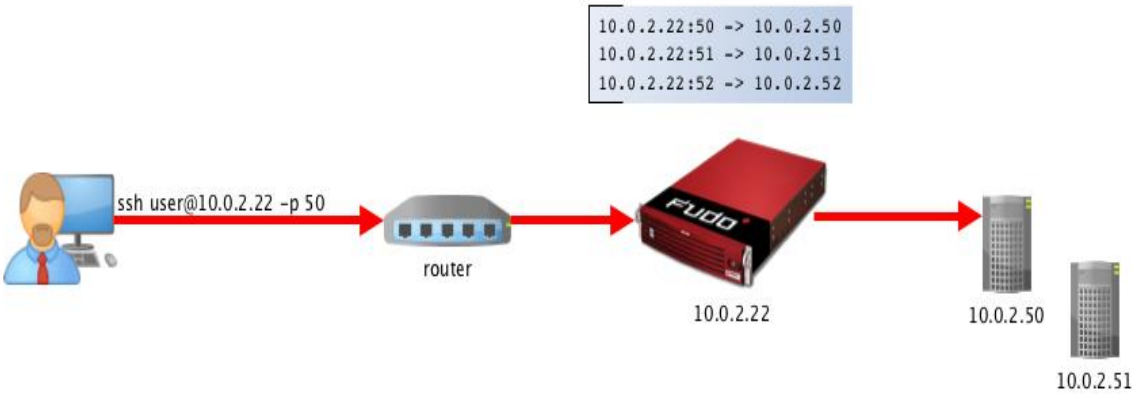

Рис. 3.1.4 Схема роботи режиму Proxy mode

Bastion Mode - режим, у якому інформація про цільовий обліковий запис або хост вбудовується безпосередньо в ім'я користувача при підключенні. Наприклад, формат ssh john_smith#admin@10.0.2.22 дозволяє Fudo PAM розпізнати, до якого сервера та під яким обліковим записом користувач намагається підключитися. Цей режим дозволяє здійснювати з'єднання до цільових серверів через єдину IP-адресу та порт Fudo PAM.

Схему [19] роботи режиму зображено на рисунку 2.1.5.

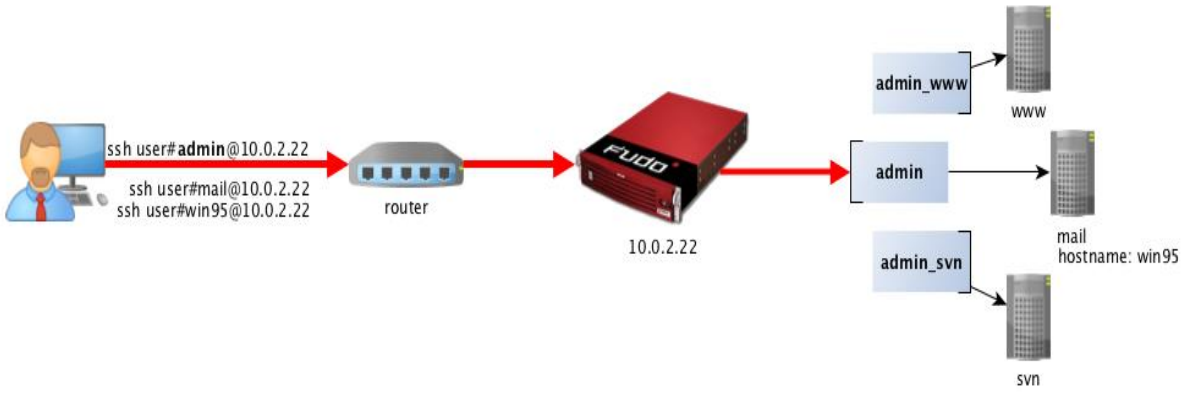

Рис. 3.1.5 Схема роботи режиму Bastion Mode

Варіанти розгортання (Deployment Scenarios)

Fudo PAM пропонує кілька сценаріїв розгортання, що дозволяє адаптувати систему до специфіки інфраструктури організації та забезпечити оптимальну інтеграцію. Серед варіантів є як апаратний так віртуалізований.

Bridge Mode — варіант, у якому Fudo PAM функціонує як міст між користувачами та цільовими серверами, не змінюючи схеми маршрутизації та не потребуючи конфігураційних змін на клієнтах чи серверах. Трафік проходить через Fudo PAM, що дозволяє здійснювати моніторинг, запис сесій та контроль доступу. Цей варіант зберігає сумісність з існуючими мережевими налаштуваннями та

політиками міжмережевих екранів.

Схему [19] роботи зображено на рисунку 2.1.6.

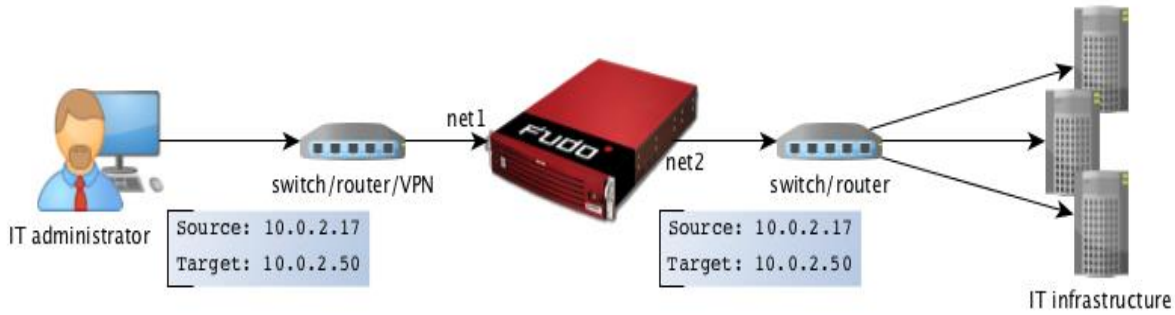

Рис. 3.1.6 Схема роботи режиму Bridge Mode

Forced Routing — варіант, що передбачає використання попередньо налаштованого маршрутизатора для примусового перенаправлення адміністративного трафіку через Fudo PAM. У цьому випадку контроль здійснюється на мережевому рівні (3 рівень моделі OSI), що дозволяє вибірково перенаправляти лише ті з'єднання, які потребують моніторингу або контролю. Решта трафіку надсилається напряму до цільових серверів, минаючи Fudo PAM.

Схему [19] роботи зображено на рисунку 2.1.7

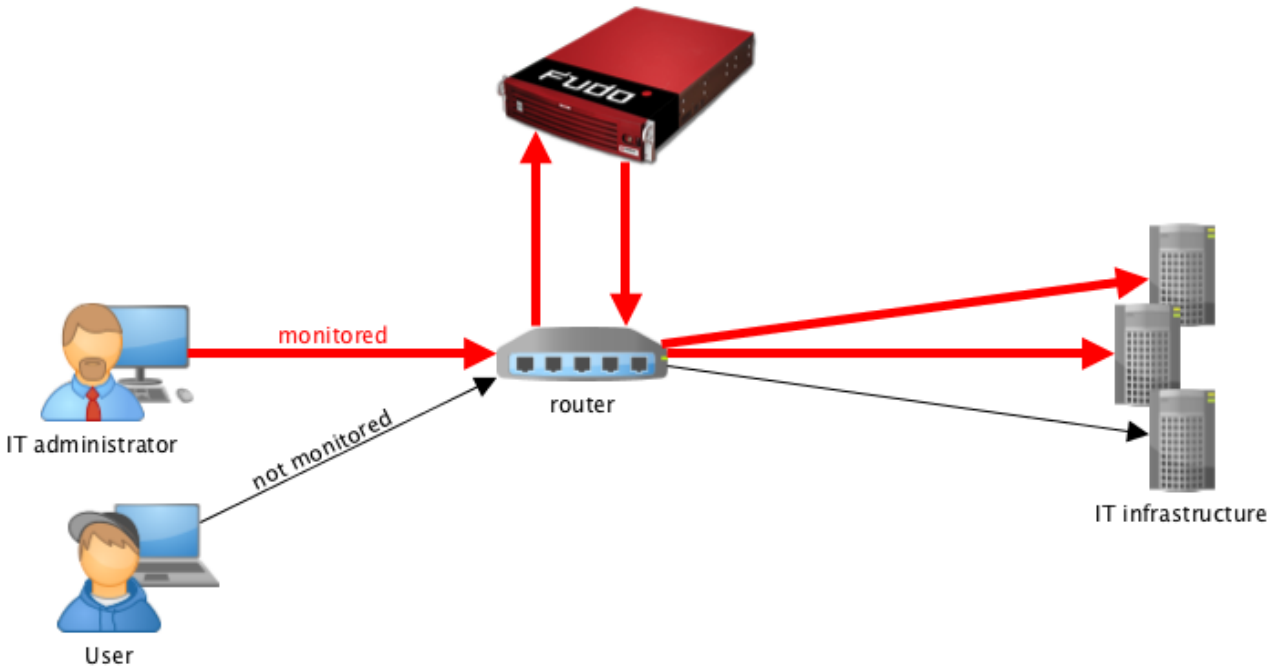

Рис. 3.1.7 – Схема роботи режиму Forced Routing

Fudo PAM також підтримує кластеризацію для забезпечення відмовостійкості. В такій конфігурації кластер працює в режимі multimaster, де кожен хост містить повну копію конфігурації системи — включно з інформацією про підключення, сервери та сесії. У випадку відмови одного з хостів - обробку підключень автоматично перебирають інші доступні хости, що забезпечує безперервний доступ до системи для користувачів.

Для забезпечення відмовостійкості та розподілу навантаження використовуються віртуальні IP-адреси, які об’єднуються в групи. Це дозволяє організувати стійкий доступ до кластеру без втрати функціональності при збої окремих компонентів.

Схему [19] роботи кластерів при працездатності всіх хостів а також відмови одного з них зображено на рисунку 2.1.8

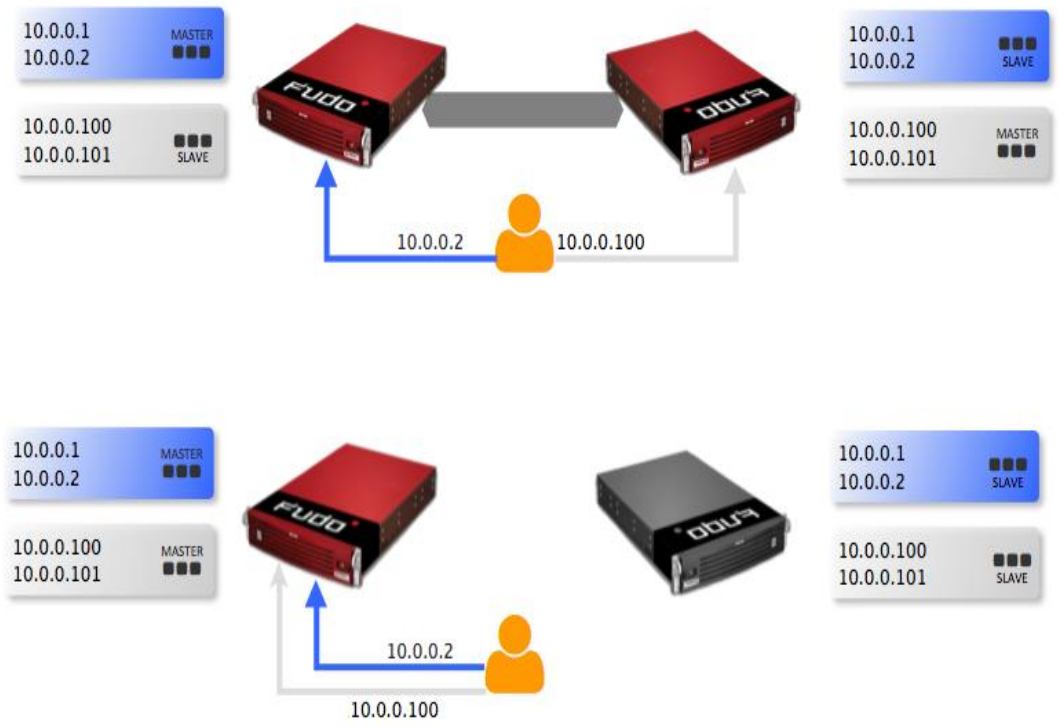

Рис. 3.1.8 Схема роботи в кластерній конфігурації

Основні функції, компоненти та їх призначення

Система Fudo PAM складається з ряду компонентів, кожен з яких виконує окрему роль у забезпеченні контролю доступу, автентифікації користувачів, запису сесій, керування обліковими даними та моніторингу дій користувачів тощо.

У структурі системи Fudo PAM важливу роль відіграють компоненти, які забезпечують централізоване керування та зручний доступ користувачів до дозволених ресурсів. Їхнє розділення дозволяє уникнути конфлікту ролей, спрощує навігацію в інтерфейсі та підвищує прозорість взаємодії між адміністративною частиною та кінцевими користувачами. Вони поділяються на дві окремі функціональні зони, кожна з яких виконує своє завдання в рамках загальної архітектури:

- Administrative Portal — веб-портал для адміністраторів системи, який надає можливість налаштовувати усі компоненти Fudo PAM. Через

адміністративний портал здійснюється конфігурація ключових компонентів системи, включно з управлінням користувачами, обліковими записами, цільовими серверами, підключеннями та правами доступу. Адміністратор має змогу створювати і застосовувати політики безпеки, налаштовувати механізми автентифікації, визначати правила для сесій та аудиту, а також контролювати всі дії, пов’язані з привілейованим доступом. Інтерфейс порталу також дозволяє переглядати детальні журнали подій, проводити аудит дій користувачів у реальному часі та отримувати доступ до відеозаписів або текстових транскриптів сесій. Наявність централізованого доступу до всіх функцій адміністрування забезпечує зручність керування, високу керованість безпековими політиками та оперативне реагування на інциденти безпеки.

- User Portal — веб-портал, призначений для кінцевих користувачів, який забезпечує зручну та контрольовану взаємодію з системою Fudo PAM. Портал відображає перелік сесій, доступ до яких дозволено відповідно до призначених політик, а також надає можливість запуску з’єднань із цільовими серверами. Користувач може ініціювати підключення безпосередньо з браузера, що усуває потребу у встановленні додаткового клієнтського ПЗ, спрощує доступ та знижує технічні вимоги до робочого середовища, а вбудовані механізми обмеження доступу гарантують, що користувач може взаємодіяти лише з дозволеними йому ресурсами та в межах встановлених правил. Наявність окремого User Portal значно підвищує зручність взаємодії з системою PAM для кінцевих користувачів. Завдяки підтримці веб-доступу без додаткового ПЗ забезпечується доступність для систем які не підтримують або не дозволяють використання необхідних додатків.

Чітке розмежування між адміністративною та користувацькою частинами сприяє підвищенню ефективності керування привілейованим доступом, мінімізує ризики змішування ролей та підтримує дотримання принципів розподілу обов’язків і захисту критичних ресурсів.

У контексті забезпечення контролю над привілейованим доступом одним із ключових напрямів є моніторинг та аналіз активності користувачів під час сесій. Сучасні PAM-системи інтегрують спеціалізовані механізми, що дозволяють здійснювати не лише фіксацію самих фактів підключення, але й детальний контроль над кожною дією, виконаною користувачем у процесі взаємодії з цільовими системами. Це включає в себе можливість запису сесій, виявлення відхилень у поведінці, побудову поведінкових профілів, а також вимірювання ефективності використання доступу.

У Fudo PAM відповідний функціонал реалізується через такі компоненти:

- Session Monitoring & Recording — модуль, який фіксує дії користувача під час сесії у вигляді відеозапису або текстових логів, залежно від протоколу. Це дозволяє не лише здійснювати аудит дій користувачів, але й оперативно реагувати на порушення політик або потенційні інциденти. Записи сесій можна відтворювати, позначати тегами, здійснювати пошук по ключовим словам та часу дій, що допомагає у розслідуванні інцидентів.
- Behavior Analytics — механізм, що дозволяє відстежувати поведінку користувачів порівнюючи її з типовими шаблонами. В разі виявлення аномалій система може автоматично призупинити сесію, створити повідомлення або передати інформацію до обраного отримувача.
- Productivity Analyzer — механізм, призначений для детального аналізу активності користувача під час сесії, що дає змогу оцінювати ефективність використання часу та ресурсів. Система відстежує співвідношення активного часу (наприклад, виконання завдань, взаємодія з інтерфейсом) до неактивного (періоди бездіяльності), кількість виконаних дій (кліки, введення даних, переходи між розділами), а також динаміку використання (швидкість взаємодії, частота використання певних функцій). Цей інструмент є корисним для внутрішнього аудиту продуктивності співробітників, контролю роботи зовнішніх підрядників (наприклад, відстеження виконання завдань за графіком), а також для виявлення шаблонів поведінки користувачів, які можуть бути використані для подальшого аналізу чи виявлення аномалій.

Застосування цих механізмів дозволяє, оперативно реагувати на порушення політик безпеки, а також формувати доказову базу для розслідувань інцидентів або внутрішніх аудитів.

Для забезпечення керованого, безпечного та контекстно-орієнтованого доступу до інформаційних систем важливим є не лише контроль користувацької поведінки, але й здатність системи оперативно реагувати на події, що відбуваються під час сесій. З цією метою сучасні PAM-рішення включають механізми, які дозволяють автоматизовано виявляти відхилення або порушення політик, а також здійснювати відповідні дії без участі оператора. Окреме значення має також компонент, який забезпечує приймання вхідних з'єднань і визначає технічні параметри для подальшої маршрутизації трафіку.

До таких функціональних елементів у Fudo PAM належать:

- Policies — це шаблони поведінки або умов, які дозволяють системі PAM здійснювати проактивний моніторинг привілейованих сесій у режимі реального часу. Вони використовуються для виявлення підозрілих або заборонених дій, що можуть свідчити про зловмисну активність або порушення політик доступу. Якщо система фіксує відповідність активності в сесії одному з визначених шаблонів, вона може автоматично виконати заздалегідь задані дії, а також надіслати сповіщення відповідальним особам для подальшого реагування. Такий механізм дозволяє зменшити час виявлення інцидентів та оперативно реагувати на потенційні загрози без потреби в постійному ручному моніторингу.

  Політики поділяються залежно від основного механізму виявлення:

  - При використанні модуля штучного інтелекту система аналізує поведінкові шаблони сесій та порівнює їх із моделями нормальної активності. Реакція ініціюється при досягненні встановленого порогу ймовірності загрози, що дозволяє виявляти аномалії навіть у разі неявної або складної для формального опису поведінки. Цей метод ефективний для виявлення нових, раніше невідомих сценаріїв атак.

- При використанні регулярних виразів система здійснює синтаксичний аналіз вхідних або вихідних даних сесії — наприклад, команд, що вводяться у термінал, або результатів запитів — з метою виявлення ключових слів, шаблонів чи виразів, які вказують на небажану активність. Це дозволяє точно описати потенційно небезпечні дії, зокрема спроби виведення паролів, виконання шкідливих скриптів або доступу до критичних конфігурацій та запобігти їм.

- Listeners — компоненти, що відповідають за приймання вхідних підключень від користувачів до цільових серверів або сервісів. Вони виступають як точка входу до інфраструктури та контролюють параметри з'єднання, визначаючи спосіб маршрутизації трафіку, автентифікації та ініціалізації сеансів. До основних характеристик належать тип протоколу (SSH, RDP, HTTPS, Telnet тощо), порт прослуховування, IP-адреса прив’язки, а також режим з’єднання (наприклад, transparent, proxy або relay). Завдяки listener’ам забезпечується гнучка адаптація до різних інфраструктурних сценаріїв, а також реалізується контрольований і захищений канал для встановлення привілейованих сесій через систему PAM.

Автентифікація є ключовим етапом, що визначає рівень довіри до користувача перед наданням доступу до критичних ресурсів. Від якості реалізації механізмів автентифікації залежить стійкість всієї системи до несанкціонованого проникнення. Особливу увагу в сучасних PAM-рішеннях приділяють двом концепціям, які значно підвищують рівень безпеки: JIT доступом та багатофакторній автентифікації. Вони дозволяють не лише верифікувати користувача, але й обмежити обсяг і тривалість наданих привілеїв.

До цієї категорії належать такі компоненти системи Fudo PAM:

- Just-in-Time (JIT) Access — механізм, що забезпечує тимчасове надання привілейованого доступу до ресурсів лише у разі необхідності, мінімізуючи ризики, пов’язані з постійною наявністю облікових даних. Доступ ініціюється користувачем шляхом подання запиту, який повинен пройти

процедуру схвалення відповідальною особою або системним модулем згідно з визначеними політиками. Облікові дані при цьому не розкриваються користувачу напряму: автентифікація та ініціалізація сесії виконується автоматизовано через механізм credential injection. Після завершення сесії, наданий доступ автоматично відкликається, а у разі використання паролів вони можуть бути негайно змінені, що запобігає повторному несанкціонованому використанню. JIT-доступ також дозволяє фіксувати мету підключення, час доступу та контекст дій, що забезпечує повний аудит та контроль привілейованої активності.

- Система підтримує багатофакторну автентифікацію (MFA), яка забезпечує підвищений рівень безпеки шляхом комбінації кількох незалежних методів перевірки особи користувача. MFA реалізується за допомогою вбудованих засобів, таких як генерація одноразових паролів на основі часу (TOTP) через мобільні додатки (наприклад, Google Authenticator, Microsoft Authenticator) або відправлення кодів через SMS. Крім того, система підтримує інтеграцію з зовнішніми платформами, такими як для централізованого управління доступом або SSO-платформи, включаючи SAML, OAuth або OpenID Connect, що забезпечує автентифікацію в складних корпоративних середовищах. Багатофакторна автентифікація може застосовуватися на двох етапах: під час входу до порталу для захисту початкового доступу до системи, а також безпосередньо перед підключенням до цільового серверу, що дозволяє додатково убезпечити доступ до критичних ресурсів. MFA значно підвищує захист інформаційних систем, ускладнюючи несанкціонований доступ навіть у разі компрометації облікових даних.

Застосування цих механізмів дозволяє суттєво зменшити ризики, пов’язані з постійним або неконтрольованим доступом, а також мінімізувати наслідки у разі компрометації окремих автентифікаційних факторів. Такий підхід відповідає сучасним підходам до безпеки, включаючи принципи Zero Standing Privileges та Least Privileges.

У контексті PAM-систем питання безпечного зберігання, ротації та передачі таких даних набуває критичного значення. Для цього призначений спеціалізований модуль, який забезпечує централізоване управління обліковими записами без необхідності розкриття їх кінцевим користувачам. Такий підхід дозволяє не лише зберігати паролі у зашифрованому вигляді, а й автоматизувати зміну паролів та застосовувати механізм credential injection при ініціалізації сесій.

У системі Fudo PAM цю функцію виконує компонент Secret Manager. Компонент дозволяє зберігати паролі у зашифрованому вигляді, обмежити їхнє відображення користувачам, а також реалізувати автоматичну зміну паролів після завершення сесій. При використанні механізму ін’єкції облікових даних система ініціює з’єднання самостійно, не розкриваючи пароль користувачеві. Це забезпечує безпечний тимчасовий доступ без ризику компрометації облікових записів.

Зміна паролів на цільових серверах працює через транспортний рівень, наприклад SSH, LDAP, Telnet або WinRM, що забезпечує інтеграцію з різними системами.

Fudo PAM підтримує зміну паролів для таких систем [19]:

- Unix
- MySQL
- Cisco
- Cisco Enable Password
- MS Windows

Окрім вбудованих шаблонів, можливо створювати власні скрипти для розширення функціональності та забезпечення точного керування обліковими даними на контрольованих серверах. Такий підхід до управління обліковими даними є важливим з кількох причин. По-перше, він забезпечує високий рівень безпеки, оскільки знижує ймовірність компрометації облікових записів через доступ до паролів. Автоматична зміна паролів після кожної сесії гарантує, що навіть у разі несанкціонованого доступу до облікових даних, зловмисник не зможе

використати їх для подальших атак. По-друге, ін’єкція облікових даних забезпечує зручний та безпечний процес підключення, що важливо для адміністраторів та користувачів, яким не потрібно вручну управляти паролями. Це також дозволяє забезпечити відповідність політикам безпеки, таким як принцип мінімальних привілеїв і нульової довіри, що є критично важливим для захисту від внутрішніх та зовнішніх загроз.

Узагальнюючи розгляд функціональних компонентів системи Fudo PAM, слід зазначити, що її архітектура побудована на модульному принципі, де кожен елемент виконує чітко визначену роль у забезпеченні контролю, безпеки та аудиту привілейованого доступу. Такий підхід дозволяє досягти високої гнучкості при розгортанні системи, її масштабуванні та інтеграції в існуюче середовище інформаційної безпеки.

Компоненти адміністрування та користувацького доступу забезпечують централізоване керування, зручну взаємодію та відповідність ролям і політикам. Модулі обробки сесій дозволяють здійснювати постійний моніторинг, запис і аналіз активності користувачів, що є основою для подальшого реагування на інциденти. Інструменти безпеки, як-от механізми динамічного реагування, політики, багатофакторна автентифікація та Just-in-Time доступ, забезпечують дотримання сучасних вимог до контролю над привілейованими правами. Зокрема, важливу роль відіграє Secret Manager, що дозволяє повністю автоматизувати процеси зберігання та використання облікових даних без їх розкриття користувачам.

Сукупність цих функцій формує повноцінне рішення для побудови захищеної системи керування привілейованим доступом.

3.2 Варіант розгортання системи контролю доступу до корпоративних систем на базі Fudo PAM

Перед впровадженням системи контролю доступу на базі Fudo PAM доцільно здійснити комплексний огляд IT-інфраструктури, що охоплює як технічні ресурси, так і облікові записи користувачів. Такий підхід дозволяє створити цілісну картину поточного стану системи контролю доступу в організації, виявити потенційні вразливості, зокрема надмірні привілеї, облікові записи з незрозумілим призначенням або ті, що більше не використовуються, а також сформувати оптимальні правила керування доступом.

Першим кроком є інвентаризація критичних систем і сервісів, до яких необхідно забезпечити контрольований привілейований доступ. Це можуть бути сервери (як фізичні, так і віртуальні), мережеві пристрої, бази даних, інструменти керування інфраструктурою, системи резервного копіювання, а також хмарні платформи. Для кожного з ресурсів необхідно зафіксувати тип, операційну систему, IP-адресу або доменне ім’я, протокол доступу (наприклад, RDP, SSH, HTTPS), а також поточний метод автентифікації.

Далі необхідно виконати мережеві налаштування, а також забезпечити коректну роботу сервісів на кінцевих точках. Оскільки система базується на використанні стандартних мережевих протоколів для встановлення з’єднань, слід попередньо впевнитися, що відповідні служби на цільових серверах активовані та працюють стабільно.

Окрім цього, необхідно внести зміни у міжмережеві екрани, щоб забезпечити безперешкодну взаємодію між компонентами системи. Також слід переконатися у відсутності мережевих обмежень або політик безпеки, які можуть блокувати встановлення сесій або передачу даних.

У разі використання проксі-серверів або VPN, необхідно внести відповідні зміни в конфігурації, щоб маршрутизація запитів до цільових ресурсів відповідала вимогам системи.

Першим кроком налаштувань виконується прив’язка системи до відповідної часової зони. Це є критично важливим аспектом для подальшої коректної роботи журналювання, синхронізації доступу, аудиту подій та інтеграції з іншими сервісами (зокрема, службою Active Directory або зовнішніми сервісами автентифікації). У процесі ініціалізації було обирано регіон Європа. Наступним

кроком є визначення конкретного міста, що дозволяє точніше встановити часовий пояс. У досліджуваному варіанті впровадження обрано місто Київ (Europe/Kyiv), що відповідає дійсному часовому поясу для корпоративного середовища, у якому планується експлуатація рішення.

Після завершення процесу початкового налаштування та першого завантаження системи було виконано автентифікацію за допомогою облікового запису за замовчуванням, передбаченого розробником. При першому вході система ініціює примусову зміну пароля, що дозволяє уникнути потенційного зловживання стандартними обліковими даними. Після проходження початкової автентифікації відкривається доступ до системного меню, реалізованого через консольний інтерфейс, у якому передбачено базові можливості адміністрування. Серед доступних опцій - функціонал для перегляду поточного стану ключових компонентів системи, включаючи моніторинг доступного дискового простору та технічного стану накопичувачів, зміну мережевих налаштувань, відновлення системи до заводських параметрів, а також завершення сесії.

У межах первинної конфігурації було виконано налаштування мережевого інтерфейсу. Зокрема, було вибрано активний мережевий адаптер (net0), до якого вручну призначено фіксовану IP-адресу 192.168.31.192, а також вказано шлюз за замовчуванням.

Рис. 3.2.1 Мережеві налаштування

Після завершення конфігурації мережевих параметрів було відкрито веб-браузер, де за вказаною IP-адресою було здійснено перехід до захищеного веб-інтерфейсу системи. Через HTTPS-з’єднання було виконано вхід до адміністративної панелі, що надалі слугувала основним інструментом конфігурації й керування функціональністю рішення.

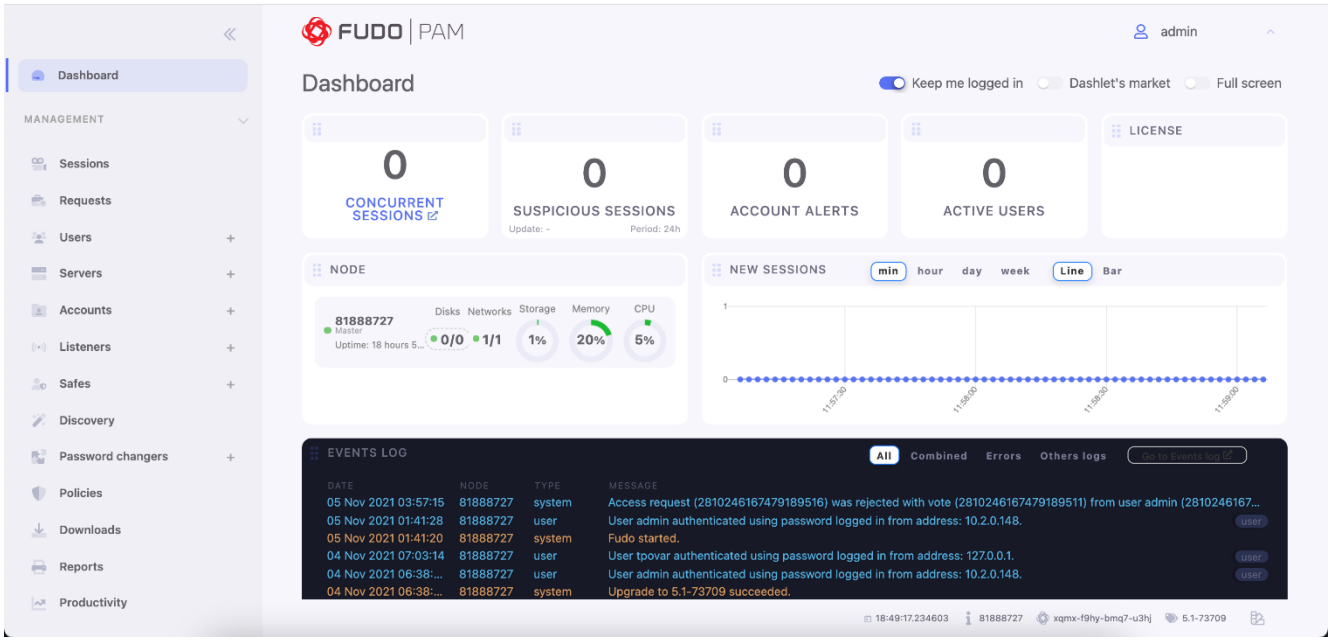

Рис. 3.2.2 Адміністративна панель

Для забезпечення централізованого керування доступом до критичних IT-ресурсів компанії, у рамках впровадження рішення Fudo PAM було налаштовано створення керованих сесій. Структура системи передбачає модульний підхід, де кожен компонент виконує окрему функцію в логіці контролю доступу. Створення сесій потребує попередньої конфігурації кількох ключових об’єктів системи, серед яких: користувачі, сервери, облікові записи, інтерфейси підключення (Listeners), політики доступу (Safes) та веб-портал користувача.

Кожен із зазначених компонентів виконує специфічну функцію:

- **Users** — об'єкти, що відображають кінцевих користувачів, яким буде надано привілейований або обмежений доступ до об’єктів кінцевих точок.
- **Servers** — сервери, до яких здійснюється підключення.
- **Accounts** — облікові записи, які використовуються Fudo PAM для встановлення з’єднання із серверами від імені користувача, часто із застосуванням технології credential injection.
- **Listeners** — логічні об'єкти, які приймають підключення від користувачів, формуючи проміжну точку доступу між користувачем і сервером.
- **Safes** — це логічні контейнери, що поєднують у собі налаштування користувачів, цільових серверів, облікових записів та налаштувань функціоналу протоколів для створення політики доступу.

- **User Portal** — веб-інтерфейс, доступний кінцевим користувачам, через який реалізується початок сесій, подача запитів на тимчасовий доступ та взаємодія з призначеними ресурсами.

У межах практичного впровадження було налаштовано можливість створення сесій за протоколами **RDP** (для доступу до системи на базі Windows) та **SSH** (для керування UNIX-подібною системою). Налаштування сесій для цих протоколів дозволяє охопити переважну більшість типових сценаріїв адміністрування та технічної підтримки у корпоративному середовищі.

Початковим етапом конфігурації стала процедура створення об'єкта користувача. У межах цього процесу було надано можливість визначити унікальний логін, який надалі використовуватиметься як ідентифікатор користувача під час автентифікації. Окрім цього, було встановлено статус облікового запису — заблокований, що забороняє його використання до зміни статусу (що корисно для періоду налаштувань, перед тим як надати його користувачу). З міркувань обмеження доступу для тимчасового персоналу або зовнішніх підрядників також передбачено можливість вказати термін існування облікового запису.

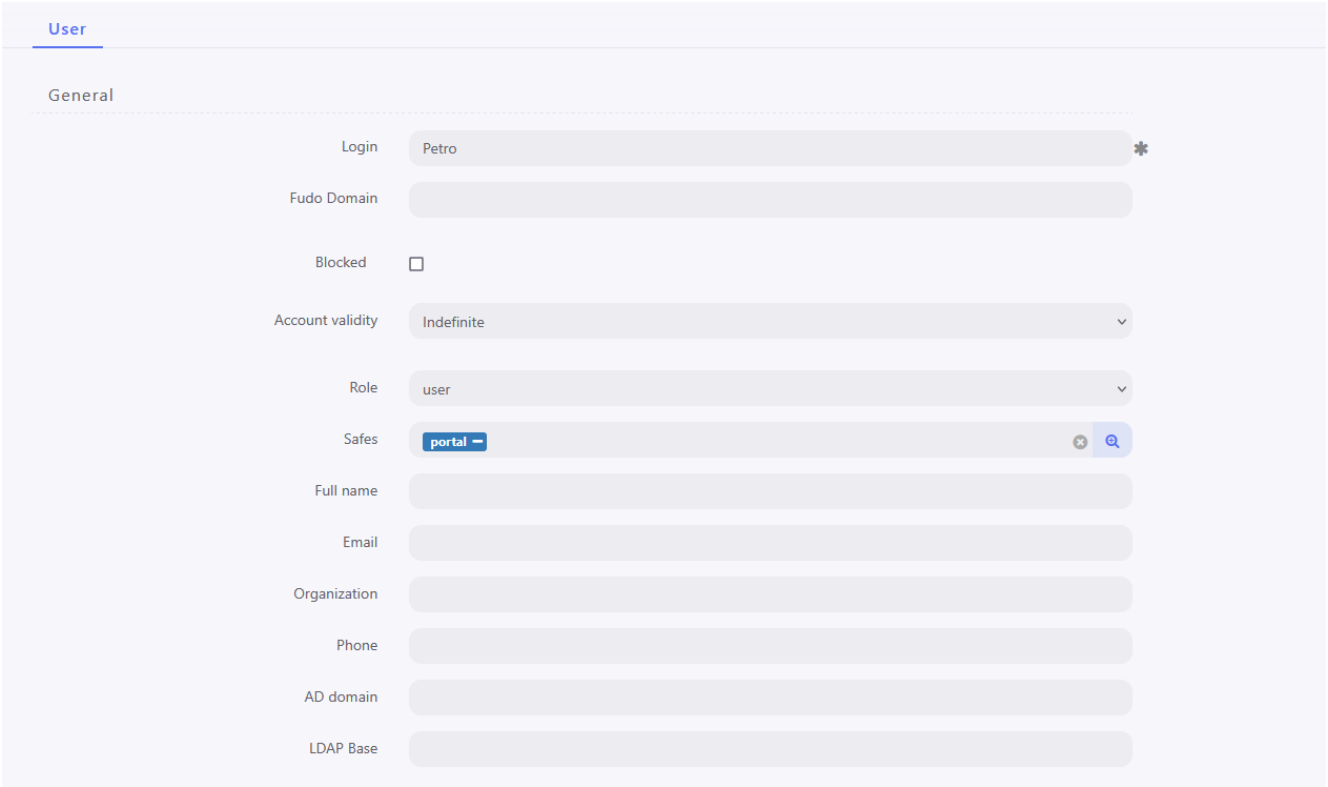

Рис. 3.2.3 Створення користувача

Наступним етапом було обрано методи автентифікації. Fudo PAM надає широкі можливості з налаштування цього аспекту безпеки. Зокрема, було вказано допустиму кількість невдалих спроб входу до моменту автоматичного блокування облікового запису. Це дозволяє запобігти атакам перебором паролів (brute-force), а також зменшити ризик компрометації облікових даних.

Серед доступних методів автентифікації, які було протестовано:

- **Зовнішня автентифікація**, що реалізується через інтеграцію з Active Directory або зовнішнім сервісом аутентифікації (IdP) за протоколами SAML або LDAP;
- **OATH (Open Authentication)** — механізм одноразових паролів на основі часу (TOTP), який підтримується низкою програм (Google Authenticator, Microsoft Authenticator тощо);
- **Статичний пароль**, що задається вручну під час створення користувача;
- **SSH-ключі**, які можуть бути завантажені в систему або згенеровані автоматично.

Для підвищення рівня безпеки було також протестовано можливість примусової зміни пароля після першого входу, що дозволяє запобігти використанню стандартних паролів після отримання облікового запису. Додатково було реалізовано можливість активації багатофакторної автентифікації (MFA), що значно знижує ймовірність несанкціонованого доступу навіть у разі компрометації основного фактора.

Наступним етапом впровадження стала конфігурація цільових серверів, до яких у подальшому здійснюватимуться підключення користувачів через контрольований доступ. З метою забезпечення повного охоплення типових корпоративних сценаріїв було створено два типи серверів — на основі операційної системи Windows для з’єднань по протоколу RDP та на основі Linux для сеансів SSH.

Схему архітектури зображено на Рис. 3.2.4

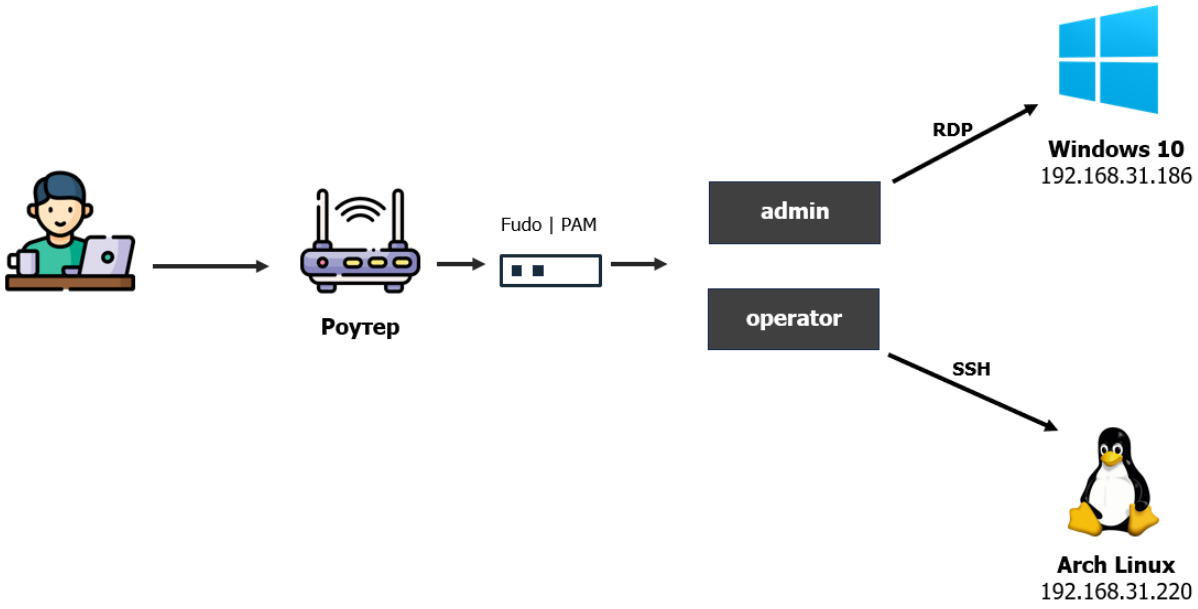

Рис. 3.2.4 Схема розгорнутої інфраструктури

Під час додавання нового запису до конфігурації системи Fudo PAM передбачено можливість задати його унікальну назву, яка використовується для ідентифікації об’єкта в межах інтерфейсу адміністратора. Також можна зафіксувати поточний статус сервера — активний або заблокований — що дозволяє тимчасово виводити вузли з обслуговування без необхідності їх видалення з конфігурації.

У процесі налаштування зазначається бажаний протокол взаємодії (наприклад, RDP або SSH), що визначає спосіб встановлення сесії та формат передачі даних. Окремо конфігурується IP-адреса та порт цільового серверу, що дозволяє системі Fudo PAM правильно маршрутизувати підключення через визначений інтерфейс. Також, у разі використання шифрування або сертифікатів, система дозволяє додати або завантажити відповідний сертифікат сервера для подальшої перевірки справжності під час встановлення з’єднання.

Для сервера Windows було вибрано протокол RDP, із зазначенням IP-адреси машини, відкритого порту 3389, а також мережевого інтерфейсу, до якого прив’язано вхідні з’єднання. У випадку з Linux-сервером для доступу був налаштований протокол SSH із параметрами шифрування та автентифікації, характерними для відповідного середовища.

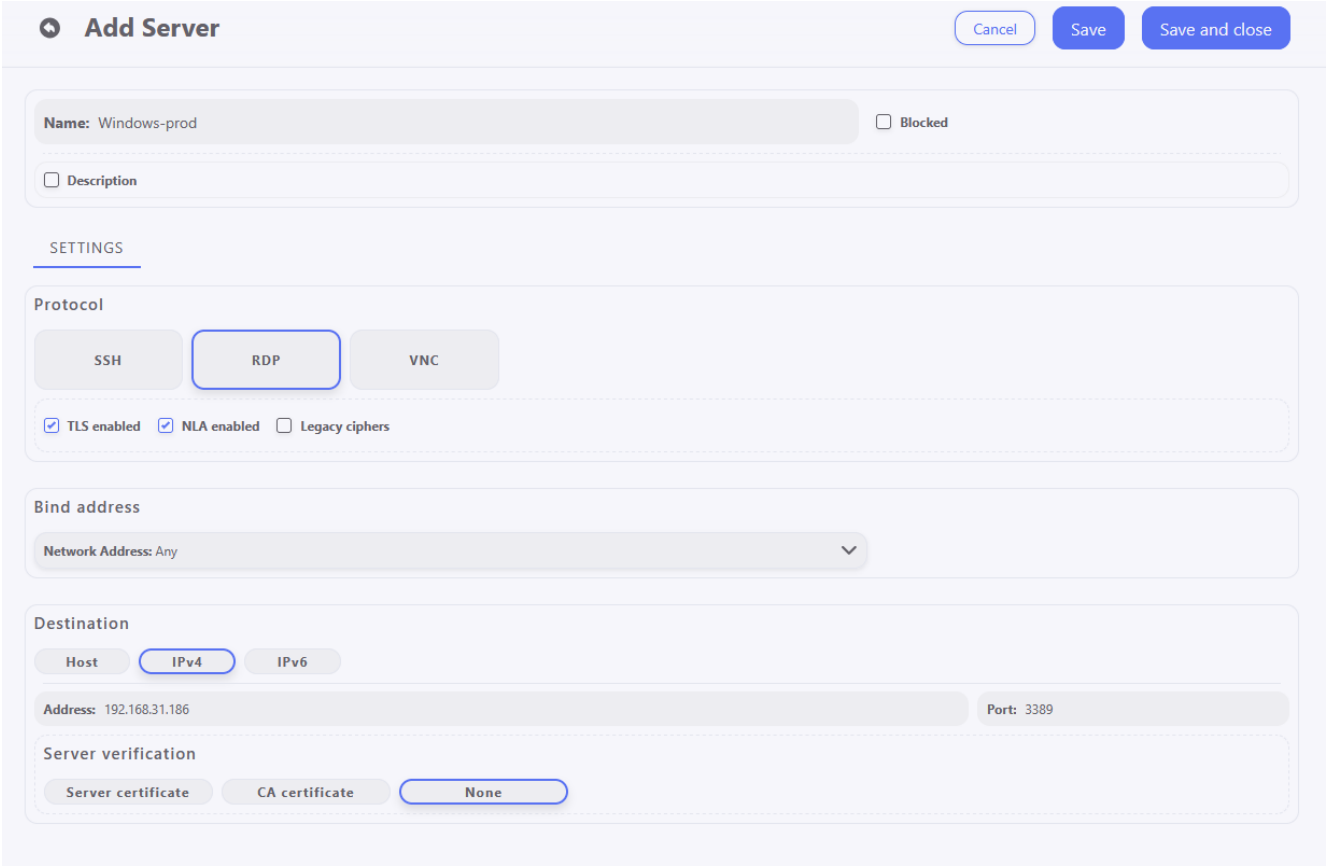

Рис. 3.2.5 Створення RDP серверу

У процесі додавання нового облікового запису було запропоновано вибір між двома типами: *Forward* та *Regular*. У випадку використання режиму *Forward* облікові дані не зберігаються локально в системі Fudo PAM. Натомість, при кожному підключенні користувач вводить логін та пароль вручну, або ж відповідна інформація може бути передана до системи ззовні, наприклад, через інтеграцію з іншими джерелами автентифікації чи з використанням механізмів динамічного підключення. Режим *Regular*, навпаки, передбачає централізоване зберігання облікових даних у захищеному середовищі самої системи PAM. У такій моделі користувач взагалі не має доступу до паролю чи ключів — система Fudo самостійно передає відповідні дані на цільовий сервер у момент встановлення з'єднання, за умови, що користувач має дозвіл на доступ до цього облікового запису згідно визначених політик.

Під час створення облікового запису також визначається зв'язок із одним або декількома серверними вузлами. Це дозволяє чітко регламентувати контекст використання кожного облікового запису — наприклад, конкретний обліковий запис може бути застосований лише до певного сервера, і лише в межах обмеженого протоколу доступу. Така гнучкість сприяє побудові детального

контролю над правами доступу в корпоративній інфраструктурі, з можливістю централізованого моніторингу й подальшої аналітики.

Після додавання користувачів, серверів та відповідних облікових записів наступним кроком стало налаштування об’єктів типу *Safes*, які в архітектурі Fudo PAM виконують роль логічних контейнерів для керування доступом. *Safes* дозволяють визначити, які саме користувачі можуть ініціювати сеанси підключення до певних серверів, за допомогою яких облікових записів, і за яких умов. Таким чином, вони реалізують політику привілейованого доступу на основі контексту та відповідності визначеним правилам.

Інтерфейс конфігурації *Safes* структуровано у вигляді трьох основних сторінок: *General*, *Users* та *Accounts*.

На першій сторінці — *General* — здійснюється конфігурація загальних параметрів доступу, які регламентують поведінку сесій та взаємодію користувача з системою під час ініціалізації підключення. Одним із ключових параметрів є Login Reason, який активує механізм запиту до користувача про необхідність вказати причину підключення до ресурсу. Цей елемент використовується з метою підвищення прозорості дій користувача та формування контексту, що надалі може бути використаний під час аналізу журналів доступу. Такий підхід дозволяє краще ідентифікувати мотивацію дій та виявляти потенційні зловживання доступом.

Опція Access Request Required Votes реалізує політику попереднього схвалення доступу до ресурсу, що відповідає моделі Just-in-Time (JIT) доступу. За допомогою цього параметра встановлюється кількість голосів адміністраторів, необхідних для надання дозволу на підключення. Таким чином, контроль над доступом набуває багаторівневого характеру, де дозвіл видається лише після ретельної оцінки запиту кількома особами, що значно підвищує рівень захищеності критичних ресурсів.

Параметр Note Access визначає рівень доступу користувачів до робочих приміток, пов’язаних із сесіями. Можливе налаштування режиму лише для перегляду або з правом внесення змін. Ця функціональність використовується для ведення оперативних коментарів під час роботи з ресурсом, а також для документування рішень або дій, що були вжиті у процесі підключення.

Налаштування Session Time Limit дозволяє встановити максимальну тривалість активної сесії у хвилинах. Це забезпечує автоматичне завершення сесії після вичерпання визначеного часу, що сприяє дотриманню принципів мінімізації привілеїв та зниженню ризиків, пов’язаних із занадто тривалим перебуванням у системі з підвищеними правами. Аналогічно, параметр Session Inactivity Limit

дозволяє обмежити тривалість бездіяльності користувача в активній сесії. Якщо протягом заданого часу не фіксується активність, з'єднання автоматично припиняється. Це зменшує імовірність несанкціонованого доступу у випадку, якщо користувач залишив робоче місце без завершення сесії.

Функціональність OTP in Access Gateway передбачає можливість генерації одноразового пароля (OTP) безпосередньо в користувацькому порталі. Такий механізм додає додатковий рівень автентифікації при доступі до цільових серверів.

У свою чергу, опція Web Client активує можливість підключення до цільової сесії через веб-браузер. Це забезпечує гнучкість в умовах віддаленої роботи та сумісність із широким спектром пристроїв, без необхідності встановлення або використання додаткового клієнтського програмного забезпечення.

На другій вкладці — *Users* — виконується прив'язка конкретних користувачів або груп користувачів до відповідного Safe. Цей крок забезпечує реалізацію політики обмеження доступу лише для уповноважених осіб.

Третя сторінка — *Accounts* — відповідає за зіставлення облікових записів, які можуть використовуватися у межах поточного Safe. Адміністратор конфігурує, які саме облікові записи можуть бути застосовані для підключення до серверів, визначених у цьому Safe.

У рамках конфігурації протоколів доступу особливу увагу приділяється налаштуванням, що визначають допустимі або обмежені функції з'єднання. У демонстраційному середовищі, представленому на рисунку 3.2.6, увімкнено лише протокол RDP, що дозволяє проілюструвати можливості тонкого налаштування цього типу підключення в межах системи Fudo PAM.

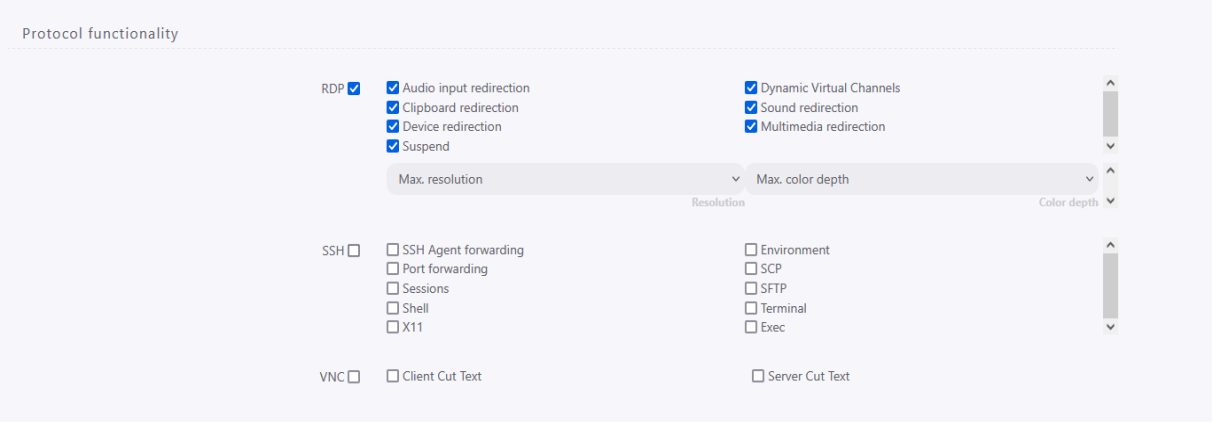

Рис. 3.2.6 Налаштування функціоналу протоколів

Серед доступних параметрів протоколу RDP першим варто розглянути *Audio Input Redirection*, що надає можливість перенаправлення аудіо з мікрофона клієнта до віддаленого серверного середовища. Це є особливо корисним у разі використання голосових інтерфейсів або додатків, що вимагають введення голосом. Налаштування *Clipboard Redirection* дозволяє синхронізувати буфер обміну між клієнтом і віддаленим сервером. Завдяки цьому користувачі можуть здійснювати копіювання й вставлення текстових або графічних об'єктів безпосередньо між двома середовищами, але така можливість може бути не завжди бажаною, особливо на серверах де зберігаються конфіденційні дані. Іншою важливою можливістю є *Device Redirection* — технологія, що дозволяє інтегрувати локальні пристрої користувача (наприклад, принтери, USB-накопичувачі або смарт-картки) безпосередньо в сесію, таким чином забезпечуючи доступ до периферійних пристроїв навіть у віддаленому середовищі. Ще один параметр, *Multimedia Redirection*, відповідає за делегування обробки відео та аудіо контенту з серверного боку на клієнтський пристрій, що знижує навантаження на сервер. Серед функцій, спрямованих на забезпечення збереження стану сесії, важливим є параметр *Suspend*, що дозволяє тимчасово призупинити активну сесію з можливістю її подальшого відновлення без потреби запуску нового підключення.

Для забезпечення відповідності графічного відображення вимогам конкретного середовища, можна задати параметр *Max. Resolution*, який визначає максимальну допустиму роздільну здатність виводу. Це дозволяє не лише контролювати якість зображення, але й оптимізувати мережеве навантаження, особливо при роботі через канали з обмеженою пропускною здатністю.

Для складних випадків або при наявності специфічних технічних вимог передбачено можливість налаштування *Common Configuration*. Цей механізм дозволяє вручну додавати ключі та параметри до конфігураційного файлу RDP, що значно підвищує гнучкість системи та дозволяє її адаптацію до нестандартних вимог.

У контексті реалізації захищених підключень до UNIX-подібних систем важливу роль відіграє протокол SSH, який широко застосовується у корпоративному середовищі для віддаленого керування, передачі файлів та тунелювання трафіку. У системі контролю доступу Fudo PAM надається гнучкий набір параметрів, що дозволяє точно регулювати поведінку SSH-з’єднань, виходячи з вимог безпеки, зручності адміністрування та політик доступу.

Опція **Environment** відповідає за пересилання змінних середовища. У разі її деактивації змінні не передаються через механізм SendEnv, однак усе ще можуть бути визначені локально на сервері. У більшості сценаріїв ця опція застосовується

для забезпечення ізоляції середовищ користувача, уникаючи небажаного впливу на системну поведінку або обхід обмежень через сторонні змінні.

Port Forwarding забезпечує створення захищених тунелів для перенаправлення трафіку через інші порти. Це дозволяє, зокрема, здійснювати доступ до внутрішніх ресурсів, розташованих за NAT або міжмережевим екраном. Використання тунелювання підвищує гнучкість інфраструктури та дозволяє створювати складні схеми маршрутизації трафіку без порушення безпекових політик.

У випадках, коли потрібна безпечна передача файлів, активуються механізми **SCP** або **SFTP**. Обидва ці протоколи функціонують поверх SSH та забезпечують конфіденційність, цілісність і автентичність переданих даних. SCP підходить для швидкої передачі окремих файлів або папок, у той час як SFTP є більш гнучким та дозволяє виконання розширених операцій із файловою системою, таких як навігація по каталогах, зміна прав доступу тощо.

Параметр **Sessions** визначає, чи має користувач змогу ініціювати повноцінні інтерактивні сесії або запускати команди на віддаленому сервері. Якщо ця можливість деактивована, зберігається функціональність тунелювання, SCP або SFTP, однак пряма взаємодія з командним інтерпретатором буде заборонена, що може слугувати елементом обмеженого доступу згідно з політикою найменших привілеїв.

Опція **Shell** регулює доступ до інтерпретатора команд. У випадку її відключення користувач не зможе ініціювати інтерактивну сесію з shell-доступом, проте запуск окремих скриптів або команд за допомогою механізму exec усе ще буде можливим.

Нарешті, параметр **Exec** дозволяє запускати одну команду без необхідності відкривати повноцінну shell-сесію. Це ідеально підходить для автоматизованих завдань, коли необхідно виконати лише одну інструкцію, наприклад, отримати системну інформацію або викликати скрипт.

Окрім SSH і RDP, система Fudo PAM також підтримує протокол **VNC** (Virtual Network Computing), який широко застосовується для організації віддаленого доступу до графічного інтерфейсу систем. Хоча в сучасному корпоративному середовищі VNC частіше виступає як допоміжний механізм або використовується в спеціалізованих сценаріях (наприклад, для взаємодії з системами без RDP/SSH-підтримки), його налаштування в межах платформи контролю доступу не менш важливе для забезпечення безпечної та контрольованої взаємодії.

Одним з основних параметрів є **Client Cut Text**, який дозволяє користувачеві передавати текст із клієнтської машини у віддалене середовище, вставляючи його безпосередньо у вікно VNC-сесії. Ця можливість корисна під час роботи з адміністративними інтерфейсами, що вимагають введення команд або даних, але водночас створює потенційний канал для введення небажаних команд.

Другий ключовий параметр — **Server Cut Text**, який забезпечує можливість копіювання тексту з віддаленого середовища (тобто VNC-серверу) на локальний комп'ютер користувача. Це може бути корисним для збереження виводу команд, повідомлень про помилки або інших фрагментів інформації для подальшого аналізу, проте також супроводжується ризиком несанкціонованого перенесення конфіденційних даних за межі контрольованого середовища.

Налаштування доступу до Linux-серверу через протокол SSH відбувалося за аналогічним підходом, як і для систем на базі Windows, однак з урахуванням специфіки UNIX-подібного середовища. У межах даної конфігурації, окрім основних параметрів, було активовано опцію **"Access request required votes"**, яка є ключовою для реалізації принципу JIT доступу. Цей підхід передбачає, що доступ до критичних ресурсів не є постійним, а надається лише на обмежений час за запитом користувача та після погодження з боку визначеної кількості адміністраторів.

Завдяки цьому механізму суттєво знижується ризик зловживання привілейованим доступом або несанкціонованого проникнення до системи у разі компрометації облікових даних. У межах розгортання було встановлено вимогу підтвердження з боку одного адміністратора перед початком сесії.

Фінальним етапом розгортання системи було налаштування **User Portal**, який забезпечує користувачам централізований веб-інтерфейс для доступу до дозволених їм систем, а також запитів на доступ. Для цього було відкрито розділ Network Configuration. У відповідних полях було вказано IP-адресу 192.168.31.193, яка закріплюється за веб-порталом, та здійснено прив'язку цієї адреси до відповідного інтерфейсу.

У межах користувацького веб-порталу, що був налаштований на попередньому етапі, представлено інтерфейс для взаємодії з ресурсами, доступ до яких регламентується відповідно до раніше створених політик у Safes. Після авторизації у системі користувач має змогу переглянути перелік серверів, доступ до яких йому надано. У даному випадку було представлено два сервери: Linux-prod та Windows-prod, кожен із яких має різні сценарії доступу, що відображають особливості їх налаштувань у системі контролю доступу Fudo PAM.

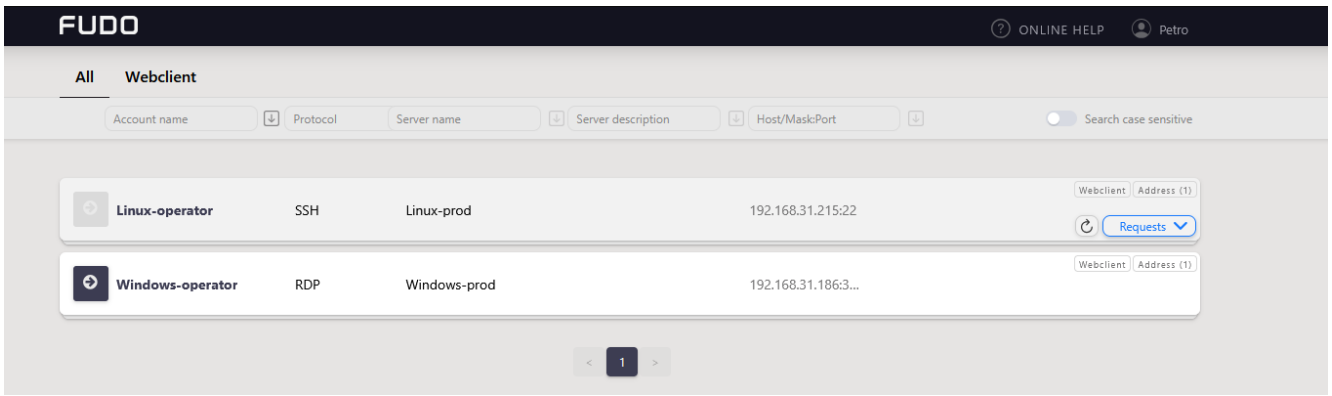

Рис. 3.2.7 Веб-портал користувачів

Сервер Linux-prod є прикладом ресурсу, до якого доступ регулюється за принципом JIT. Це означає, що користувач не може одразу ініціювати підключення, а має спершу подати запит на доступ. Після подання такого запиту, система очікує схвалення з боку одного або кількох адміністраторів, відповідно до конфігурації (зокрема, значення параметру *Access request required votes*). Такий підхід забезпечує динамічне надання прав лише у разі фактичної потреби, мінімізуючи тривалість та обсяг привілейованого доступу до критичних систем.

Механізм JIT-доступу у Fudo PAM реалізований через модуль керування запитами, що інтегрований з політиками безпеки, визначеними у Safes. Через наявні налаштування - для створення сесії користувачу спочатку необхідно подати запит. У діалоговому вікні користувач має вказати тривалість сесії, що запитується (наприклад 60 хвилин або на період кількох днів), а також обґрунтування потреби у доступі. Це може бути конкретне завдання, технічна потреба або відповідь на інцидент. У деяких випадках система може вимагати також вказати пріоритетність або інші метадані, які будуть використані під час оцінювання запиту.

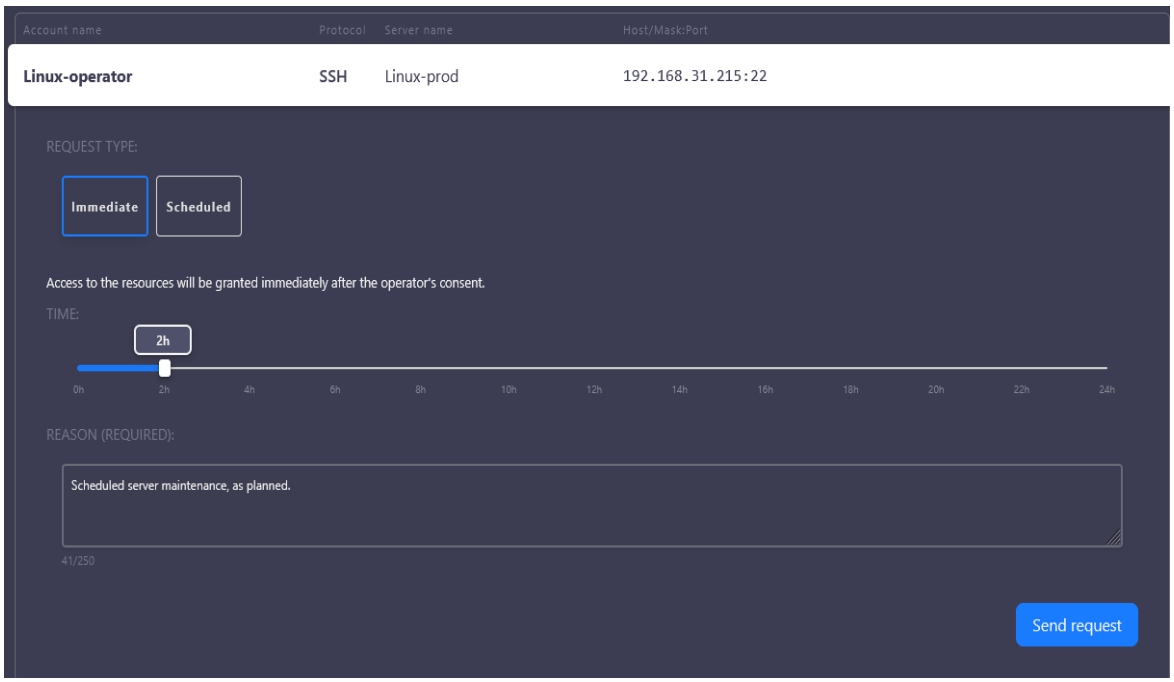

Рис. 3.2.8 Форма запиту доступу в User Portal

Після подання, запит надходить до адміністраторів або інших уповноважених осіб, яких визначено у політиці доступу. Кількість необхідних погоджень визначається параметром Access request required votes. Наприклад, для підвищеної безпеки може бути задано правило, за яким щонайменше двоє адміністраторів мають підтвердити запит, перш ніж буде створено сесію.

В адміністративній панелі Fudo PAM, ми можемо переглянути запити на доступ, які надходять від користувачів. Інтерфейс запитів побудований таким чином, щоб забезпечити швидке прийняття обґрунтованих рішень на основі наданої інформації. При відкритті конкретного запиту адміністратор бачить детальну інформацію, зокрема ідентифікатор користувача, цільовий ресурс, обраний протокол з'єднання, дату та час запиту, а також запитувану тривалість сесії. Окреме поле виводить коментар, залишений користувачем, де він пояснює причину звернення — це може бути опис задачі, службова потреба або інше обґрунтування, яке підлягає оцінці.

Адміністратор має два основні варіанти дій: погодити запит або відхилити його. У разі відмови система дозволяє додати коментар з поясненням причини, що фіксується в журналі подій і може бути використане у подальшому аналізі або внутрішньому розслідуванні. Якщо запит схвалено, система автоматично активує доступ на визначений у запиті період, після чого доступ анулюється. Всі такі дії виконуються без потреби ручного втручання у конфігурацію доступу до ресурсу.

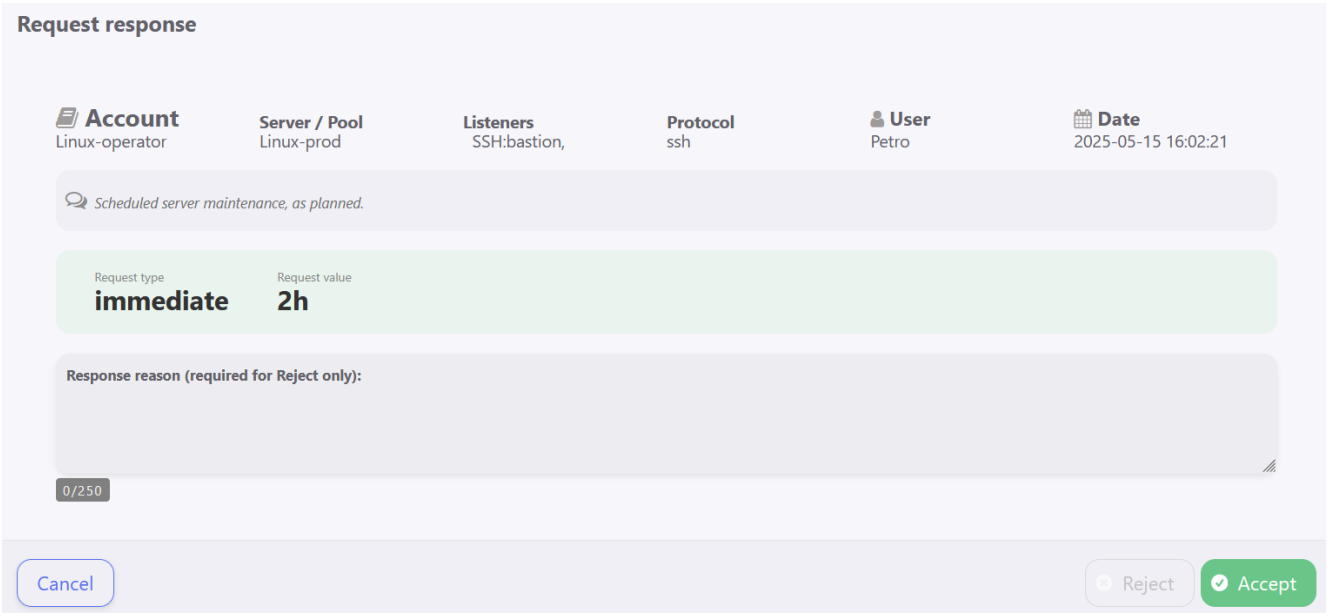

Рис. 3.1.9 Заповнена форма запиту доступу в Administrative Portal

На сторінці **Active Accesses** адміністратор має змогу бачити всі поточні дозволи, які перебувають у стані активної сесії або мають тимчасове вікно доступу. Кожен дозвіл відображається з інформацією про користувача, ресурс, тип доступу, тривалість та інші ключові параметри. Це дозволяє оперативно реагувати на незвичну активність або вручну завершити сесію у разі підозрілої поведінки.

По завершенню терміну доступу або після ручного відкликання сесії, всі записи переміщуються до архівної частини системи, де зберігаються у вигляді журналів із повною хронологією подій.

Однією з ключових функцій є наскрізний пошук по сесіях, який дозволяє здійснювати пошук за ключовими словами або командами, введеними під час сесії. Цей механізм реалізовано шляхом індексації введених користувачами даних у режимі реального часу, що дає змогу адміністраторам швидко виявити потенційно небезпечні дії, спроби виконання заборонених команд або відхилення від стандартних процедур.

Функція моніторингу сесій доступна як у режимі реального часу, так і в режимі перегляду архіву. У режимі реального часу адміністратор може приєднатися до активної сесії, не порушуючи її перебіг. Інтерфейс надає змогу бачити дії користувача поетапно, з точним часовим штампом для кожного натискання клавіші. У випадках, коли сесія була завершена, усі дії зберігаються у вигляді деталізованого журналу, де можна не лише переглядати відеозапис або журнал комунікації, а й фільтрувати його за певними параметрами, включно з командами, файлами, або конкретними ключовими словами.

З адміністративної панелі керування сесіями доступні функції призупинення, примусового завершення або вступу в сесію з правом активної участі. Така участь дає змогу адміністратору втрутитися у процес виконання дій, наприклад, у разі потреби надати технічну допомогу, проконтролювати критичні операції або запобігти порушенням політик доступу.

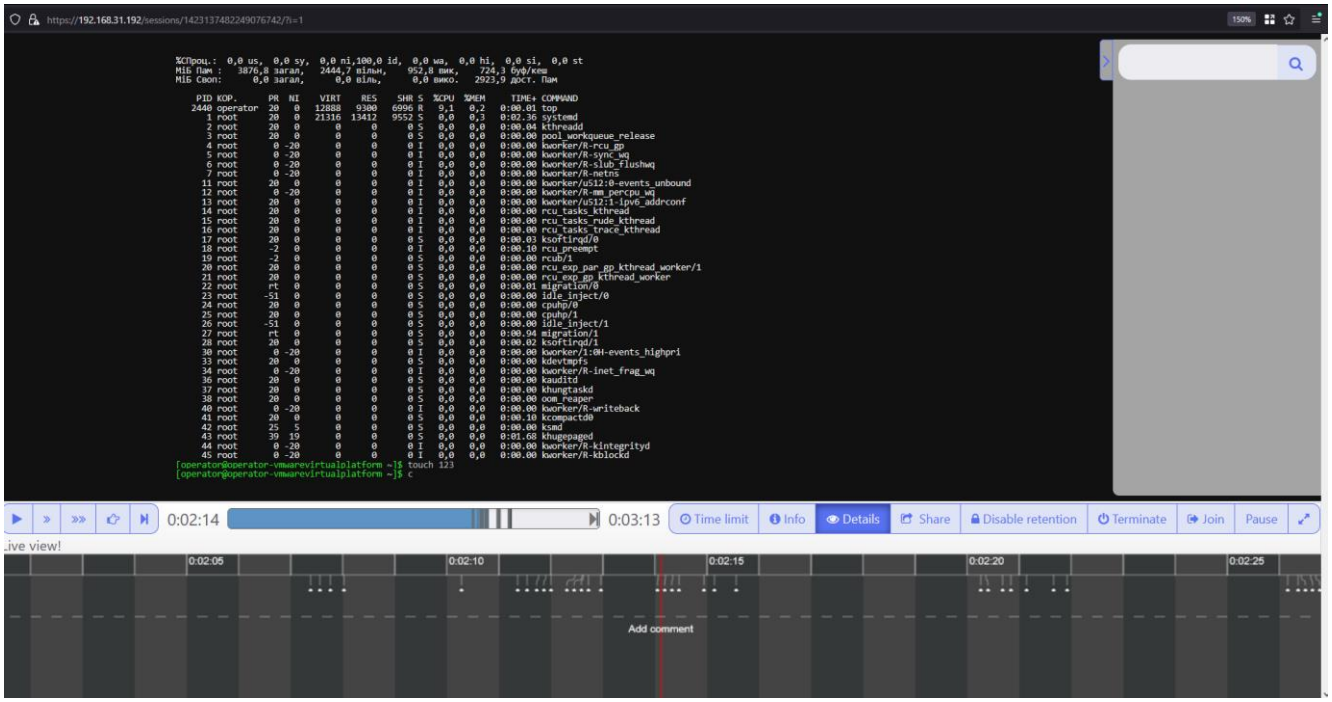

Рис. 3.1.10 Перегляд активної сесії

3.3 Рекомендації щодо застосування методів та засобів контролю доступу в корпоративних системах

На основі проведеного аналізу сучасних загроз, моделей контролю доступу та можливостей рішень PAM, можна сформулювати низку рекомендацій, які дозволять організаціям ефективно побудувати систему керування доступом до критичних ресурсів і зменшити ризики, пов’язані з привілейованими обліковими записами.

Одним із ключових принципів забезпечення інформаційної безпеки в корпоративних системах є **принцип найменших привілеїв** [2], згідно з яким користувачам, процесам або службам мають надаватися лише ті права доступу, що є необхідними для виконання конкретних задач у чітко визначений проміжок часу. Такий підхід значно зменшує площу атаки компанії, знижує ризики зловживання повноваженнями та унеможливлює несанкціоновану ескалацію привілеїв.

У сучасних умовах, коли більшість кібератак ґрунтується на компрометації облікових записів з розширеними правами, критично важливо уникати практики постійного надання адміністративного доступу. Замість цього доцільно впроваджувати динамічні моделі керування доступом, зокрема механізми JIT доступу, що передбачають надання привілеїв лише на час виконання конкретної задачі, після чого доступ автоматично відкликається [20].

Реалізація JIT-доступу може здійснюватися як через попередньо затверджені точки доступу, так і через процедури запиту й затвердження (approval workflows) [13]. Такий підхід дозволяє не лише дотримуватись принципу Zero Standing Privileges, а й забезпечує можливість перевірки та контролю адміністративних дій.

Для забезпечення надійного контролю над критичними ресурсами доцільно уніфікувати керування привілеями, впроваджувати JIT-механізми, а також забезпечити технічну можливість відкликання прав доступу.

Наступним пріоритетом є **централізований контроль та моніторинг сесій**. Ефективне керування привілейованими сесіями передбачає не лише регулювання доступу, а й постійний контроль за діями користувачів у процесі роботи з критичними ресурсами. У межах рішень класу PAM це завдання вирішується шляхом впровадження посередницької архітектури (brokered access), що передбачає направлення всіх привілейованих сесій через єдину точку доступу — PAM.

Централізоване маршрутизування сесій через такий шлюз дозволяє здійснювати повноцінний моніторинг, запис та аудит дій користувачів [21] у режимі реального часу. Застосування даного підходу дозволяє реалізацію детальних політик контролю: обмеження за IP-адресами, фільтрацію команд, часові межі активності, обмеження доступу тощо. Крім того, записи сесій, що зберігаються в зашифрованому вигляді, можуть бути використані для аналізу інцидентів, навчання персоналу, або забезпечення відповідності зовнішнім вимогам.

Важливою перевагою такого підходу є ізоляція користувачів від безпосереднього доступу до цільових систем. Усі підключення реалізуються через контрольоване середовище, що зменшує ризики компрометації інфраструктури, дозволяє уніфікувати контроль над різнорідними системами, а також значно ускладнює можливість обходу засобів контролю.

Крім того, централізація контролю сесій дозволяє інтегрувати PAM-системи з іншими рішеннями кібербезпеки. Така інтеграція дозволяє не лише записувати дії користувачів, але й виявляти поведінкові аномалії у сесіях привілейованих користувачів, що є допоможе у виявлення внутрішніх загрозам.

Таким чином, впровадження архітектури-посередника у системах PAM забезпечує реалізацію принципів контролю та відповідальності при роботі з привілейованими обліковими записами, сприяє зниженню операційних і безпекових ризиків, а також дозволяє ефективно масштабувати [22] політики доступу в корпоративному середовищі.

У межах сучасних систем керування привілейованим доступом іншим пріоритетом має бути **мінімізація участі кінцевого користувача в обробці облікових даних**. Один із найбільш ефективних підходів для цього — впровадження механізму Credential Injection, що забезпечує автоматизовану підстановку облікових даних під час ініціації сесії без надання користувачу прямого доступу до логіна чи пароля. Це дозволяє усунути ризики, пов’язані з розголошенням, несанкціонованим копіюванням чи використанням облікових даних у неналежний спосіб.

Credential Injection зазвичай функціонує у зв’язці з захищеним сховищем облікових записів (vault), що також забезпечує їх безпечне зберігання, з якого PAM-рішення отримує автентифікації дані для підключення до цільової системи. У момент створення сесії ці дані підставляються автоматично, після чого користувач має змогу працювати з ресурсом, не володіючи жодною критичною

інформацією. Такий підхід не лише знижує ризик компрометації привілейованих облікових даних, але й дозволяє ведення детального журналу доступу.

Паралельно з підстановкою облікових даних, сучасні PAM-системи забезпечують автоматизоване надання привілейованих облікових записів на основі профільних атрибутів користувача, таких як посада, приналежність до зовнішнього підрядника або рівень доступу. Один із ключових операційних ефектів такої моделі полягає у можливості створення тимчасових або одноразових привілейованих облікових записів згідно з політиками авторизації або правилами надання доступу за ролями, без необхідності ручного втручання адміністратора [23] [24]. Це дозволяє зменшити адміністративне навантаження, уникнути людських помилок під час конфігурації прав доступу, а також зберігати повну відповідність внутрішнім політикам безпеки.

У дослідженні [23] показано, що впровадження механізмів автоматичного надання доступу та Credential Injection дозволяє значно підвищити ефективність управління доступом у великих організаціях, забезпечуючи динамічну адаптацію рівня привілеїв до поточного контексту користувача. На додаток це також мінімізує ризики надлишкових прав доступу [24], які можуть виникати при класичному моделюванні прав вручну.

Таким чином, поєднання Credential Injection та автоматизованого доступу до привілейованих облікових записів на основі атрибутів користувача є важливою частиною для побудови масштабованої, захищеної та контрольованої моделі керування доступом у корпоративних середовищах.

Останнім, що варто зазначити, є **впровадження MFA для привілейованих користувачів**. Це забезпечує додаткову гарантію ідентичності, мінімізує ризик компрометації облікових записів і формує передумови для реалізації принципів адаптивного контролю доступу основаного на контексті.

Суть полягає у використанні двох або більше незалежних факторів перевірки особи: знання (наприклад, пароль), володіння (фізичний токен або пристрій) і притаманна ознака (біометрія). В контексті привілейованого доступу використання лише пароля є недостатнім, оскільки він може бути скомпрометований через фішинг, шкідливе програмне забезпечення або витік даних.

Інтеграція MFA у процес автентифікації привілейованих користувачів дозволяє значно зменшити ризики несанкціонованого доступу, навіть у випадках, коли облікові дані вже стали відомі третім сторонам. Важливою перевагою цього підходу є додатковий рівень верифікації, що активується до встановлення сесії або

в момент спроби виконати критичні дії, такі як підключення до серверів, зміна конфігурацій або отримання доступу до сховищ облікових даних.

З технічної точки зору, MFA може бути реалізована за допомогою різних механізмів: генераторів одноразових кодів, апаратних токенів, push-повідомлень або біометричних сканерів. Доцільним є застосування контекстно-залежної автентифікації, за якої система оцінює ризик сесії (місце підключення, пристрій, час доби) та вимагає додатковий фактор лише за наявності ознак відхилення від типової поведінки.

На основі розглянутих рекомендацій можна зробити висновок, що ефективне управління доступом у корпоративних інформаційних системах вимагає комплексного підходу, який поєднує як організаційні принципи, так і технічні механізми реалізації. Застосування принципу найменших привілеїв у поєднанні з моделлю тимчасового доступу дозволяє зменшити ризики зловживання правами та обмежити наслідки потенційної компрометації облікового запису. Централізація керування сесіями через посередницьку архітектуру забезпечує запис дій користувачів і створює передумови для ефективного аудиту, а Credential Injection усуває необхідність розповсюдження облікових даних серед персоналу, тим самим зменшуючи шанс потенційної компрометації.

Впровадження сегментації доступу на основі ролей і категорій ресурсів сприяє структуризації прав доступу відповідно до функціонального призначення активів та обов’язків користувачів, забезпечуючи ізоляцію внутрішніх систем.

Багатофакторна автентифікація виступає як додатковий захисний бар’єр на етапі ідентифікації, підвищуючи стійкість систем до атак, що базуються на викрадених облікових даних. У сукупності ці підходи формують основу для побудови комплексної системи контролю доступу, орієнтованої на зниження ризиків, відповідність принципам нульової довіри, а також підвищення ефективності безпекових процесів.

Таким чином, впровадження розглянутих практик дозволяє не лише підвищити рівень захищеності інфраструктури компанії. але й забезпечити оперативне реагування на інциденти.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи проведено комплексне дослідження проблематики контролю доступу в корпоративному середовищі. Проаналізовано найчастіші виклики, пов’язані з привілейованими обліковими записами, вразливостями, що виникають унаслідок недостатньо контрольованого або надмірного доступу до критичних IT-систем.

На основі аналізу актуальних загроз та стандартів інформаційної безпеки (зокрема NIST SP 800-53, CIS Controls) було визначено ключові вимоги до побудови ефективної системи контролю доступу. Було детально розглянуто підходи least privilege, just-in-time access, та багатофакторної автентифікації (MFA), що є критично важливими для захисту сучасної IT-інфраструктури.

Досліджено функціональні можливості системи Fudo PAM, яка належить до класу Privileged Access Management (PAM). Проведений аналіз архітектури, механізмів доступу, інструментів моніторингу, запису сесій, а також поведінкової аналітики продемонстрував, що Fudo PAM забезпечує надійний контроль за адміністративними діями. Окрім цього, окремо розглянуто технічні особливості розгортання системи, підтримку різних сценаріїв доступу а також налаштування з’єднань за протоколами RDP та SSH

В рамках роботи було запропоновано варіант впровадження Fudo PAM. Розроблено рекомендації щодо побудови політик доступу, сегментації ресурсів, інтеграції з існуючими системами ідентифікації та заходів з моніторингу активності користувачів. Визначено доцільність використання таких функцій, як credential injection, MFA, audit trail, session recording та behavior analytics.

Загалом, дослідження підтвердило, що ефективна система керування привілейованим доступом є критично важливою складовою кібербезпеки підприємства. Впровадження рішення Fudo PAM дозволяє не лише мінімізувати ризики несанкціонованого доступу та зловживання правами, але й створити контрольований доступ до критичних систем. Це, у свою чергу, сприяє дотриманню вимог регуляторів, та підвищити рівень захищеності IT-інфраструктури компанії.

Разом з тим, важливо пам’ятати, що контроль доступу — це не разове справа, а постійний процес, що потребує адаптації до нових загроз, перегляду політик доступу, оновлення інструментів та регулярного аудиту ефективності прийнятих заходів.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO 27001 Information security, cybersecurity and privacy protection – Information security management systems. 2023. URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf (date of access: 18.04.2025).

2. NIST SP 800-53 rev. 5: security and privacy controls for information systems and organizations. Independently Published, 2022. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (date of access: 24.04.2025).

3. Verizion DBIR. *Verizion*. No. 2023. P. 4–20. URL: https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf (date of access: 23.04.2025).

4. CIS controls. 8th ed. URL: https://kr-labs.com.ua/books/CIS_Controls_v8_Guide.pdf (date of access: 17.04.2025).

5. Craig S. Wright. The IT Regulatory and Standards Compliance Handbook: How to Survive an Information Systems Audit and Assesments. Syngress Publishing, Inc. URL: https://books.google.com.ua/books?id=RizmpbOHvf4C&printsec=copyright&redir_esc=y#v=onepage&q&f=false (date of access: 10.05.2025).

6. Mandatory access control. URL: https://www.researchgate.net/figure/view-of-mandatory-access-control-MAC_fig4_358430862 (date of access: 08.05.2025).

7. Role-Based Access Control (RBAC): Features and Motivation. National Institute of Standards and Technology. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=916537 (date of access: 09.05.2025).

8. NIST SP 800-162 | Guide to Attribute Based Access Control (ABAC) Definition and Considerations. URL: https://doi.org/10.6028/NIST.SP.800-162 (date of access: 09.05.2025).

9. NIST SP 1800-18 Privileged Account Management for the Financial Services Sector. URL: https://www.nccoe.nist.gov/sites/default/files/legacy-files/fs-pam-nist-sp1800-18-draft.pdf (date of access: 15.05.2025).

10. NIST SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf (date of access: 16.05.2025).

11. Cybersecurity of Medical Data Based on Big Data and Privacy Protection Method Journal Article | IGI Global Scientific Publishing. URL: https://www.igi-global.com/gateway/article/full-text-pdf/325222 (date of access: 17.05.2025).

12. The History and Evolution of Privileged Access Management (PAM): Securing Your Infrastructure | Adaptive. URL: https://adaptive.live/blog/the-history-and-evolution-of-privileged-access-management-pam-securing-your-infrastructure (date of access: 17.05.2025).

13. Request and Approval Workflows. URL: https://help.xtontech.com/content/administrators-and-power-users/workflow/request-and-approval-workflows.htm (date of access: 18.05.2025).

14. Zero Standing Privileges. BeyondTrust. URL: https://www.beyondtrust.com/resources/glossary/zero-standing-privileges (date of access: 18.05.2025).

15. What is Privileged Access Management (PAM)?. WALLIX. URL: https://www.wallix.com/blogpost/what-is-privileged-access-management-pam/ (date of access: 16.05.2025).

16. The CyberArk Digital Vault: Built for Security. URL: https://www.cyberark.com/resources/product-datasheets/the-cyberark-digital-vault-built-for-security (date of access: 17.05.2025).

17. What is Just-in-Time Access (JIT)?. Delinea. URL: https://delinea.com/what-is/just-in-time-access#:~:text=Just-in-Time%20(JIT,on%20an%20as-needed%20basis. (date of access: 18.05.2025).

18. Williamson J., Curran K. Best Practice in Multi-factor Authentication. Semiconductor Science and Information Devices. 2021. Vol. 3, no. 1. URL: https://doi.org/10.30564/ssid.v3i1.3152 (date of access: 18.05.2025).

19. Fudo Enterprise 5.5 documentation. URL: https://download.fudosecurity.com/documentation/fudo/latest/online_help/en/index.html (date of access: 15.05.2025).

20. Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations. URL: https://www.semanticscholar.org/reader/80098a4a913f02cdf8168958d1dd5267fbf7e9d6 (date of access: 23.05.2025).

21. M. THAMPI S. Introduction to Distributed Systems. URL: https://arxiv.org/ftp/arxiv/papers/0911/0911.4395.pdf (date of access: 21.06.2025).

22. H. DENG R., YANG Y. A study of content authentication in proxy-enabled multimedia delivery systems: Model, techniques, and applications. URL: https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?params=/context/sis_research/article/1780/&path_info=Content_Authentication_2009_afv.pdf (date of access: 24.05.2025).

23. Integration of Identity Governance and Management Framework within Universities for Privileged Users. URL: https://thesai.org/Downloads/Volume12No6/Paper_64-Integration_of_Identity_Governance_and_Management_Framework.pdf (date of access: 22.05.2025).

24. Hammoud Alruwies M., Mishra S., Abdul Rahman AlShehri M. Identity Governance Framework for Privileged Users. Computer Systems Science and Engineering. 2022. Vol. 40, no. 3. P. 995–1005. URL: https://doi.org/10.32604/csse.2022.019355 (date of access: 12.06.2025).