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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо захисту інформаційної системи організації від несанкціонованого доступу на основі Fudo Security 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

_____ Віталій ЧАЙКІВСЬКИЙ
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
ЧАЙКІВСЬКИЙ Віталій
(прізвище, ім'я)

Керівник д.ф., МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ВСТУП

Актуальність дослідження. В умовах сьогодення динаміка тенденцій кібербезпеки неупинно змінюється. Наразі складно уявити роботу будь-яких структур, бізнесів тощо без інформаційних технологій. Для підтримки функціонування інформаційних систем та їх компонентів призначаються відповідальні особи, зокрема адміністратори ІС, які наділяються привілейованими правами доступу. Тому привілейовані користувачі відіграють ключову роль у забезпеченні функціонування операційних процесів та сервісів.

Однак зростаюча кількість кібератак, пов’язаних із компрометацією привілейованих облікових записів, робить такі облікові записи однією з основних цілей зловмисників. Несанкціонований доступ до привілейованих облікових записів може спричинити витоки чутливої інформації та перешкоджати штатному функціонуванню інформаційних систем організації.

З метою зменшення кількості інсайдерських атак та контролю діяльності привілейованих користувачів (адміністраторів) організації вдаються до впровадження ряду організаційних та технічних заходів і засобів.

Одним із технічних підходів до захисту привілейованих облікових записів є впровадження механізмів контролю та управління привілейованим доступом. Рішення класу PAM дозволяють контролювати та відслідковувати діяльність привілейованих користувачів, знижуючи ризики, пов’язані з несанкціонованим використанням таких облікових записів.

Для огляду функціональних можливостей вищезгаданої технології пропонується розглянути рішення від Fudo Security, яке забезпечує комплексний підхід до захисту від компрометації облікових записів.

Об’єкт дослідження – захист привілейованих облікових записів в інформаційних системах.

Предмет дослідження – методи та засоби контролю діяльності та захисту привілейованих облікових записів в інформаційних системах з використанням Fudo PAM.

Мета роботи – розробка організаційних та технічних рекомендацій щодо реалізації методів контролю діяльності привілейованих облікових записів та їх захисту.

Завдання бакалаврської роботи:

проаналізувати роль привілейованих облікових записів у забезпеченні функціонування ІС та класифікувати користувачів за рівнем доступу;

дослідити загрози, які застосовні до привілейованих облікових записів, із їх класифікацією;

проаналізувати популярні засоби захисту PAM та порівняти їх функціональні можливості;

розглянути архітектуру та особливості рішення Fudo PAM, як інструменту захисту привілейованих облікових записів;

продемонструвати застосування Fudo PAM для захисту привілейованих облікових записів у корпоративному середовищі;

сформувати практичні рекомендації щодо впровадження PAM у корпоративному середовищі організації.

Методи дослідження – опрацювання літератури та відкритих джерел за вищезгаданою тематикою, аналіз експлуатаційної документації рішення Fudo PAM, міжнародних стандартів та їх порівняння, проведення експерименту.

Практичне значення одержаних результатів: викладені рекомендації щодо захисту інформаційної системи можуть використовуватися у корпоративних інформаційних системах.

1 АНАЛІЗ НЕОБХІДНОСТІ КОНТРОЛЮ ТА ЗАХИСТУ ПРИВІЛЕВОНИХ ОБЛІКОВИХ ЗАПИСІВ

1.1. Аналіз концепції привілеїв та актуальності контролю діяльності привілейованих облікових записів

Сьогоденне інформаційне середовище є сукупністю різних компонентів, зокрема інформаційних систем, інформаційних ресурсів, механізмів захисту, користувачів та їхніх ролей. Організації мають значну цінність не лише в даних, які вони обробляють та володіють, але й у даних, які їм довірили клієнти. Співробітники та сторонні партнери мають потребу переглядати, змінювати та видаляти дані у своїй повсякденній діяльності. Уявімо, що могло б статися, якби кожен мав необмежені привілеї до компонентів ІС та даних, які вони обробляють, але спершу розглянемо питання привілеїв.

Відповідно до термінології національного інституту стандартів і технологій (NIST) привілеями вважаються права, надані особі, програмі або процесу [1]. Тобто, даний термін означає повноваження, які має певна особа (використовуючи обліковий запис), програма або процес на створення або виконання функцій у ІС або мережі. Наприклад, користувачеві потрібен доступ для внесення будь-яких змін, пов'язаних з ІБ, таких як конфігурація мереж/систем.

Хоч і кінцеве призначення привілеїв слугує для важливої операційної мети, яка необхідна для того, щоб користувачі могли виконувати поставлені перед ними задачі, існує ризик для ІБ, коли привілеї можуть бути використані не за призначенням або користувачі зловживають наданими привілеями з метою завдання шкоди організації.

Ситуація, де б кожен мав необмежені привілеї до компонентів ІС та даних створила б суттєві загрози для конфіденційності, цілісності та доступності даних та інформації в цілому. Оскільки відсутність механізмів контролю доступу

призвела б до безконтрольної циркуляції чутливих даних, що могло б мати серйозні юридичні та репутаційні наслідки для організацій.

В дописі блогу Securden фахівець Захіруддін Ахмед зазначає, що організації будь-якого розміру, від малих до великих міжнародних компаній, схильні до витоків даних і кібератак та наводить кілька тривожних статистичних даних:

- 81% зламів пов'язані з використанням скомпрометованих та слабких паролів – Verizon;
- 22% витоків даних спричинені фішинговими атаками – Verizon;
- 8% – середній викуп при атаках програм-вимагачів у 2-му кварталі 2022 року склав $228 125, що на 8% більше порівняно з 1-м кварталом того ж року – Coverware;
- 71% – середній викуп у перші 5 місяців 2022 року зріс до $925 162, що на 71% більше порівняно з 2021 роком – Palo Alto;
- 75% зламів здійснювали зовнішні зловмисники, що означає, що 25% – це внутрішні загрози – Verizon;
- 69% атак на державні установи пов'язані з методами соціальної інженерії – Verizon;
- 74% жертв витоків даних у період травень 2020 – 2021 рік визнали, що їхні мережі були скомпрометовані через надмірні привілеї сторонніх користувачів – Ponemon Institute;
- 7% – у 2021 році ФБР отримало 847 376 звернень щодо кіберзагроз, що на 7% більше, ніж у 2020 році, а загальні втрати перевищили $6,9 млрд;
- Викупи, сплачені при атаках програм-вимагачів, у 2020 році зросли на 171%, а найбільша виплата сягнула $10 млн – Symantec;
- $1,8 млн – середня вартість витоку даних на стільки менша для компаній із впровадженою концепцією Zero Trust, порівняно з тими, хто її не використовує – IBM [2];

Ці статистичні дані ще раз підкреслюють важливість кібербезпеки та демонструють серйозні втрати, яких зазнали світові компанії через кібератаки, а також демонструють необхідність у постійному вдосконаленні технічних та

організаційних засобів й заходів управління доступом, які є важливим аспектом для досягнення кіберстійкості.

Зі стрімким розвитком інформаційних технологій пропорційно постають виклики для інформаційної та кібербезпеки. Зловмисниками використовуються нові підходи, техніки та тактики для реалізації кібератак. Більшість складних та масштабних атак вимагають отримання саме привілейованого доступу. Тому зловмисники концентруються на отриманні доступу до облікових записів, які мають привілейовані права доступу до чутливих ІС. Вважається, що привілейовані облікові записи є одним із важливих компонентів для підтримки сталого функціонуванням будь-якої ІС, оскільки вони дають змогу привілейованих користувачам (адміністраторам) налаштовувати складові ІС, вносити зміни до конфігурацій безпеки та адмініструвати користувацькі облікові записи.

Враховуючи викладене вище можна зробити висновок, що без належного контролю та захисту привілейованих облікових записів організації наражатимуться на ризики, зокрема такі як несанкціонований доступ, зловживання адміністративними правами, компрометація чутливої інформації та інсайдерські атаки.

Відповідно до звіту 2024 року «Insider Threat» від Gurucul 48% організацій повідомили, що інсайдерські атаки стали частішими за останні 12 місяців. Крім того, 51% зазнали шістьох або більше атак за останній рік, при цьому середня вартість усунення наслідків для 29% респондентів перевищила 1 мільйон доларів. Також респондентів попросили оцінити середню вартість усунення наслідків інсайдерської атаки. Деталізація та відсоткові значення продемонстровані на рис. 1. Варто зауважити, 12% вказали, що витрати на відновлення сталого функціонування становлять менше $100 тис., а 8% навіть оцінили їх у понад $2 млн. [3].

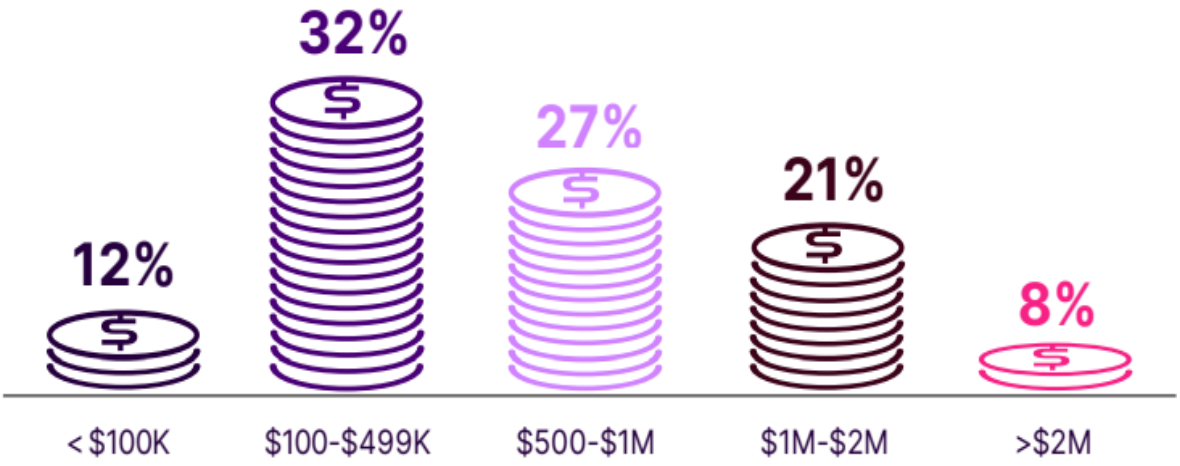

Рис. 1.1. Середня вартість усунення наслідків інсайдерської атаки [3]

Ця статистика демонструє зростаючу кількість інсайдерських атак, які в свою чергу наносять відчутні збитки для грошових ресурсів організацій. Тому з метою зменшення відсотку таких видів атак приймаються рішення щодо реалізації заходів з контролю діяльності привілейованих користувачів впровадження систем класу PAM.

1.2. Дослідження типів облікових записів, їх класифікація та застосовні загрози

Для забезпечення захисту інформації та стійкості ІС необхідно впроваджувати механізми ідентифікації, автентифікації та авторизації користувачів, які дозволяють визначати рівень доступу до інформаційних ресурсів відповідно до посадових обов'язків.

З огляду на те, що в ІС важливу роль відіграють облікові записи, які є основним механізмом контролю доступу та дозволяють не лише ідентифікувати користувача, а й забезпечити контрольоване виконання операцій у ІС. Обліковий запис користувача – це ідентифікатор, створений для особи в ІС. Облікові записи користувачів також можуть створюватися для машинних сутностей, таких як сервісні облікові записи для запуску програм, системні облікові записи для

зберігання системних файлів і процесів, а також root і адміністративні облікові записи для адміністрування ІС та їх компонентів.

Останні дві категорії облікових записів зазвичай є привілейованими обліковими записами, тобто такими, які мають більше привілеїв, ніж звичайні облікові записи користувачів [3].

З огляду на вищезгадане пропонується детальніше розглянути рівень привілеїв за класифікацією користувачів (рис 1.1):

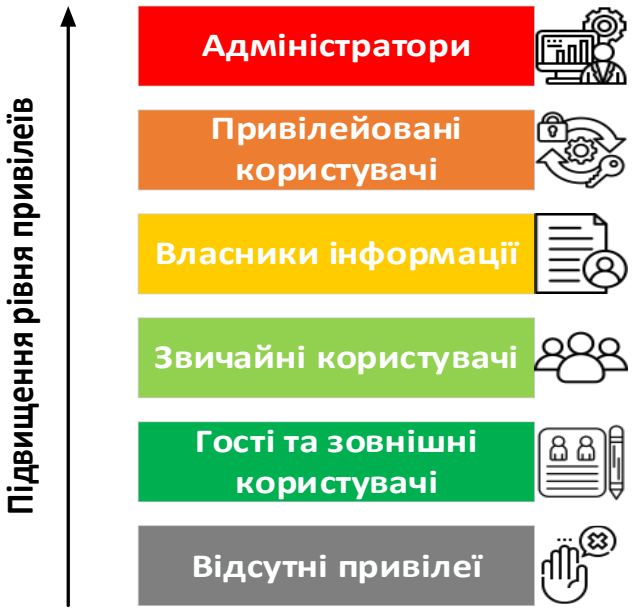

Рис. 1.2. Концептуальна класифікація привілеїв

Адміністратори

Зазвичай дана група облікових записів є ключовою для забезпечення управління та підтримки компонентів інформаційної інфраструктури. Відповідають за налаштування, експлуатацію, оновлення та забезпечення безперебійної роботи серверного, мережевого та програмного забезпечення. Привілеї охоплюють управління обліковими записами користувачів, резервне копіювання даних, налаштування політик доступу, а також виявлення та усунення технічних збоїв. Разом з тим, адміністратори здійснюють контроль за використанням апаратних і програмних ресурсів, забезпечуючи їхню оптимальну продуктивність.

З огляду на високий рівень привілеїв, адміністратори є критичними суб’єктами з погляду ІБ. Недостатній контроль за їх діяльністю або компрометація таких облікових записів можуть призвести до суттєвих наслідків. Тому діяльність адміністраторів має піддаватися посиленому моніторингу, а їхні облікові записи захищені додатковими засобами та заходами автентифікації.

Привілейований користувач

Привілейований користувач має більш розширені права доступу до ІС, порівняно зі стандартними можливостями звичайних користувачів. Це можуть бути менеджери БД, системні аналітики, спеціалісти з обслуговування критично важливих сервісів. Вони мають доступ до чутливої інформації даних та можуть, за необхідності, змінювати налаштування певного ПЗ, керувати критичними процесами та виконувати адміністративні операції, необхідні для коректного функціонування ІС та їх компонентів.

Через збільшений спектр доступу ці користувачі, так само як і адміністратори є потенційною мішенню для зловмисників, тому їхні облікові записи потребують посиленого захисту.

Власник системи

Власником системи є особа або структурний підрозділ організації, який визначає політики доступу, встановлює рівень привілеїв для інших користувачів та ухвалює рішення щодо впровадження змін в архітектурі ІС. Власник системи також несе відповідальність за відповідність її функціонування нормативним вимогам, корпоративним стандартам та політикам безпеки.

Попри те, що власник системи не обов’язково має безпосередній адміністративний доступ, його роль є значною для організації. Оскільки саме він визначає стратегічні напрями розвитку функціонування ІС, приймає рішення щодо її оновлення, оптимізації та інтеграції з іншими сервісами. Разом з тим, власник відповідає за оцінювання ризиків ІБ та впровадження механізмів захисту інформаційних активів.

Звичайний користувач

Основна кількість співробітників та/або уповноважених осіб, які використовують ІС відповідно до своїх посадових обов’язків – звичайні користувачі. Їхній доступ обмежений певними функціональними можливостями, необхідними для виконання повсякденних задач. Як правило, такі користувачі можуть переглядати, вводити та редагувати дані у межах своїх повноважень, але не мають повноважень щодо змін та конфігурування компонентів ІС або здійснення адміністративних дій.

Гості та зовнішні користувачі

Гості та зовнішні користувачі – особи, які отримують тимчасовий або обмежений доступ до ІС. Зокрема підрядники, партнери, аудитори або інші сторонні особи, яким необхідно взаємодіяти з певними ресурсами організації. Їхній доступ зазвичай обмежений у часі та контролюється відповідальними особами, зокрема адміністраторам, а права чітко визначені для запобігання небажаних змін в ІС.

Варто зауважити, що зовнішні користувачі не завжди керуються внутрішнім політикам ІБ, тому їхні облікові записи є потенційно вразливими до атак та зловживань. З метою мінімізації таких ризиків ІБ організаціями застосовуються механізми розмежування доступу, обмеження за часом активності облікового запису та впроваджують системи моніторингу та контролю дій користувачів у системі.

Відсутні привілеї

Категорія користувачів без привілеїв передбачає суб’єктів, які не мають жодного доступу до ІС або їх компонентів. До такої групи можуть відноситися звільнені співробітники, заблоковані користувачі або особи, яким не надано жодних прав доступу відповідно до політики ІБ організації.

Наступним етапом пропонується дослідити загрози, які застосовні до облікових записів, зокрема привілейованих. Пропонується класифікувати загрози за двома ключовими критеріями (рис. 2.2): за джерелом походження (внутрішні чи зовнішні) та за характером дій (цілеспрямовані чи випадкові).

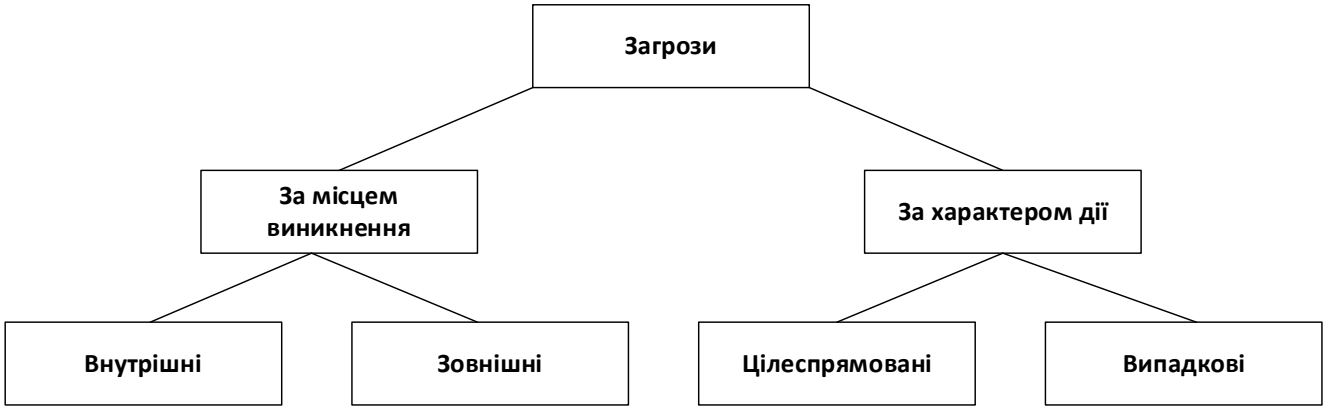

Рис. 1.3. Концептуальна класифікація загроз

Насамперед, увагу слід приділити внутрішнім загрозам, які в сучасних умовах визнаються одними з найскладніших для виявлення. Їхня небезпека зумовлена тим, що зазвичай суб'єкти внутрішніх загроз мають санкціонований доступ до інформаційних систем та ресурсів і можуть як свідомо, так і ненавмисно порушувати встановлені правила та політики ІБ. Такі порушення можуть бути виявлені у разі використання користувачем наданих прав та повноважень для досягнення власних інтересів, а також при несанкціонованих модифікаціях, копіюванні або видаленні чутливих даних.

Водночас внутрішні загрози є лише одним із потенційних векторів атак на ІС. На противагу внутрішнім загрозам стають зовнішні, які спрямовані на компрометацію облікових записів шляхом використання методів соціальної інженерії та експлуатації вразливостей ІС.

Цілеспрямовані загрози виникають, коли зловмисник вчиняє дії, спрямовані на порушення конфіденційності, цілісності або доступності інформації, яка циркулює в ІС. Наприклад, одним із поширених методів є компрометація облікових даних шляхом їх викрадення, що дозволяє зловмисникам діяти під легітимним обліковим записом без викриття з боку засобів моніторингу.

На відміну від цілеспрямованих атак, випадкові загрози виникають унаслідок людських помилок, недбалості або недосконалого процесу управління доступом в організації. Найбільш поширеним фактором такої загрози є помилки під час адміністрування ІС. Випадкове та/або некоректне призначення повноважень та

привілеїв призводить до того, що звичайні користувачі можуть отримати доступ до чутливої інформації або критичних функціональних можливостей ІС.

З огляду на викладене вище можна зробити висновок, що для реалізації механізмів захисту від несанкціонованого доступу організації мають враховувати масштаби та потенційні наслідки зазначених загроз. Тому постає необхідність у впровадженні засобів захисту, які дозволять мінімізувати ризики несанкціонованого доступу, здійснювати контроль за активністю привілейованих користувачів та забезпечувати належний рівень ІБ для всіх категорій облікових записів.

1.3. Аналіз засобів захисту та порівняння їх функціональних можливостей.

Відповідно до інформації, яка викладена в попередніх розділах можна зробити висновок, що передбачити інсайдерську атаку досить складно. Тому вендори рішень кібербезпеки пропонують організаціям певною мірою автоматизувати цей процес з використанням засобів захисту, які здійснюють контроль діяльності привілейованих користувачів. Рішення класу PAM дозволяють контролювати та відслідковувати доступ до чутливих інформаційних ресурсів організації, запобігаючи зловживанню наданими правами та привілеями. Ринок рішень кібербезпеки пропонують широкий спектр рішень класу PAM, які відрізняються функціональними можливостями та рівнем автоматизації.

Для кращого розуміння ринку пропонується звернутися до статистики авторитетного джерела, а саме розглянути звіт Gartner Magic Quadrant за 2024 рік. Звіт підтверджує, що зростає усвідомленість організацій щодо інвестування в рішення PAM. У Gartner Magic Quadrant 2024 (рис. 1.4) продемонстровано, що лідируючі позиції на ринку займають компанії BeyondTrust, CyberArk та Delinea.
Аналітики Gartner наголошують, що для протидії актуальним кіберзагрозам системи PAM мають включати основні функції, серед яких управління привілейованими обліковими записами та сесіями (PASM), надання та делегування

привілеїв (PEDM), автоматичне управління паролями, а також поведінковий аналіз користувачів задля виявлення аномалій [4].

Рис. 1.4. Gartner Magic Quadrant 2024 [4]

CyberArk (CyberArk Privileged Access Security)

CyberArk традиційно вважається найбільш функціональним рішенням на ринку PAM. Його перевага полягає у комплексному підході: від управління привілеями до моніторингу, аудиту, інтеграції з SIEM-системами, хмарними середовищами та автоматизації DevOps. CyberArk масштабований, підтримує тисячі облікових записів і є доцільним вибором для великих підприємств та критичних галузей.

Окрім функціонального зазначеного вище, важливою перевагою CyberArk є відповідність міжнародним стандартам ІБ, таки як ISO/IEC 27001, NIST CSF та інші. Це і робить рішення привабливим для впровадження в організаціях, які відносяться до критичного сектору економіки або ж співпрацюють з такими організаціями, зокрема у фінансовому, енергетичному та державному секторах.

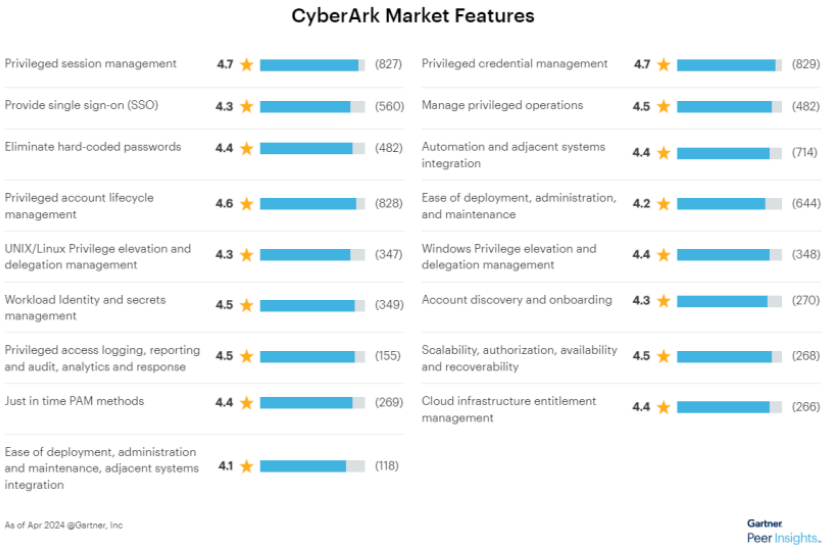

Рис. 1.5. Огляд рейтингів CyberArk Privileged Access Manager [5]

Delinea (Delinea SecretServer)

Рішення від Delinea демонструє високу ефективність у сфері контекстного контролю доступу. Контекстний контроль доступу (context-aware access control) – підхід, коли доступ до ресурсів надається не лише на основі ролі користувача, а й з урахуванням додаткових умов (контексту). Це можу бути час, коли користувач отримує доступ, географічне розташування, тип пристрою тощо. Саме тому Delinea SecretServer пропонує більш адаптивне управління ролями, політиками розмежування доступу до об'єктів інформаційної інфраструктури на основі поведінки користувача. Сильними сторонами Delinea є виявлення аномалій і підтримка аналітики ризиків. Утім, обмежена гнучкість під час реалізації TimeFrame-доступу (механізм, який дозволяє обмежити надані користувачеві права у часі, надаючи привілейований доступ лише на певний період). Розглянемо приклад: адміністратору можна надати доступ до критичної системи лише у вівторок з 10:00 до 12:00 або лише на 30 хвилин для виконання конкретного завдання, саме це і є TimeFrame-доступ. Також рішення Delinea SecretServer має залежність від веб-інтерфейсу, що може обмежувати його застосування у складних гібридних інформаційних середовищах.

Рис. 1.6. Огляд рейтингів Delinea [6]

Wallix (WALLIX Bastion)

З поміж функціональних можливостей WALLIX Bastion варто виділити механізм доступу Just-In-Time, який дозволяє призначати тимчасові облікові записи для виконання конкретних дій у чітко визначений часові терміни. Даний механізм дає змогу не створювати привілейовані облікові записи на постійну основу, а здійснювати активацію таких привілеїв лише на момент операційної потреби. З точки зору ІБ це означає, що після завершення сесії або закінчення санкціонованого часу обліковий запис автоматично ізолюється. Такий підхід дозволяє реалізувати більш гнучке та безпечне управління доступом та сприяє зниженню ризику довготривалого зберігання в ІС неактуальних привілейованих облікових записів.

За своєю логікою Just-In-Time є концептуально подібним до TimeFrame-доступу (Delinea SecretServer), оскільки обидва механізми передбачають надання привілеїв на обмежений період. Проте на відміну від TimeFrame, який зазвичай реалізується у вигляді статичних часових діапазонів доступу (наприклад, з 9:00 до 12:00), Just-In-Time функціонує динамічно, тобто привілеї надаються за запитом у момент фактичної необхідності й автоматично анулюються після виконання операційного завдання.

Окремої уваги заслуговує модульна архітектура рішення, що дозволяє налаштовувати контроль доступу з урахуванням ролей, повноважень та часу використання.

Варто зауважити, що функціональні можливості Wallix надають механізми встановлення політик доступу не лише для груп користувачів, а й на рівні окремих задач або додатків, що дозволяє більш гармонійно здійснювати адміністрування ІС.

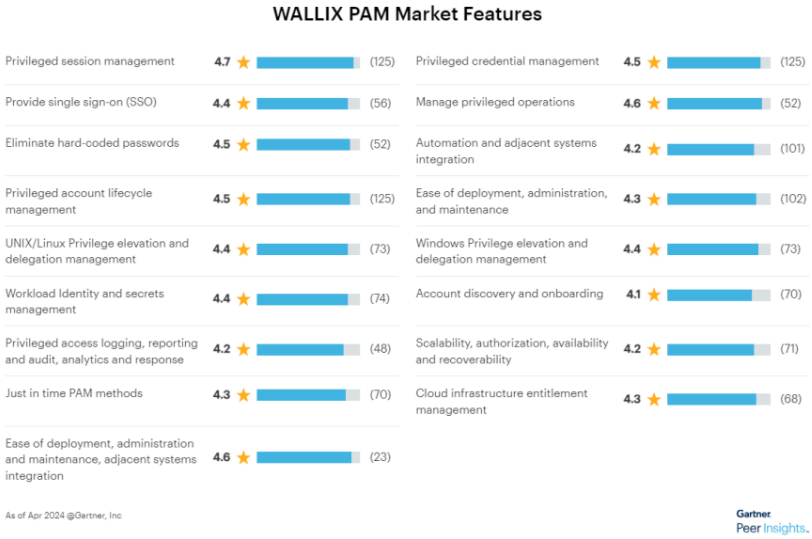

Рис. 1.7. Огляд рейтингів WALLIX PAM [7]

Fudo Security (Fudo PAM)

Рішення Fudo PAM позиціонується на ринку як високопродуктивне рішення, яке фокусується на оперативному моніторингу та записі сесій підключення привілейованих користувачів, поєднуючи простоту інтеграції з дієвими механізмами контролю. На відміну від вищезгаданих популярних рішень, зокрема CyberArk, Fudo вирізняється оперативністю впровадження, спрощеним адмініструванням та незначними вимогами до інформаційної інфраструктури. Саме ці перелічені переваги роблять його більш оптимальним для середніх та малих організацій.

Ключовими функціями є реєстрація, індексація та відтворення дій привілейованих користувачів у сесіях доступу. Ці механізми дозволяються детально відслідковувати хронологію введення команд адміністраторами,

натискання клавіш, рухи мишкою тощо. Завдяки використанню системи поведінкового аналізу, Fudo PAM здатен виявляти аномальні дії у реальному часі та сповіщати про такі дії відповідальних адміністраторів безпеки.

Fudo не є «всеосяжним» рішенням у класичному розумінні Gartner, оскільки не має повної моделі управління привілеями, як-от у Delinea чи CyberArk. Проте, застосування саме цього рішення є доцільним у ситуаціях, де пріоритетом є негайне посилення контролю за адміністративними сесіями з мінімальним впливом на операційні процеси організації. Отже, можна зробити висновок, що Fudo PAM впроваджують організації, які прагнуть оперативних, надійних та доступних за ресурсами методів та способів захисту і контролю привілейованого доступу.

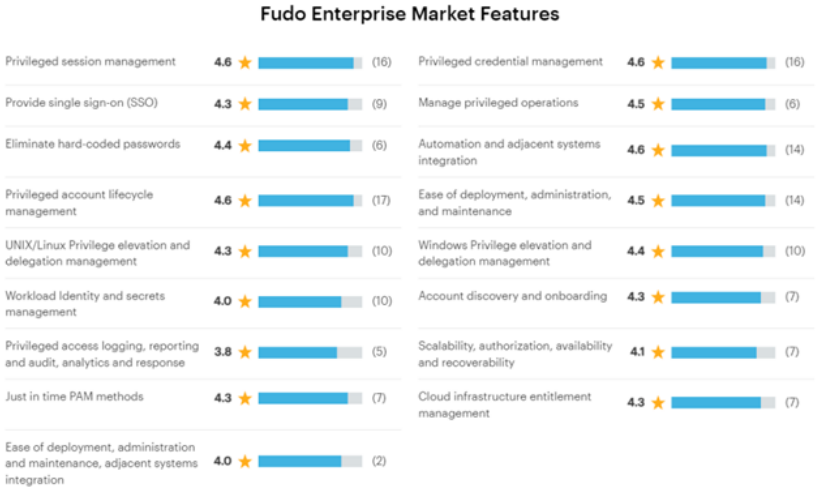

Рис. 1.8. Огляд рейтингів Fudo PAM [8]

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ

2.1. Методи та засоби захисту привілейованих облікових записів

Ознайомившись з попереднім розділом стає зрозуміло, що привілейовані облікові записи відіграють вагому роль в загальній інформаційні інфраструктурі. Саме тому до таких облікових записів можна використовувати аналогію «ключі до королівства», оскільки саме вони є привабливим для зловмисників.

Якщо подивитися на використання привілейованих облікових записів через призму ризик-орієнтованого підходу, то стає явно зрозуміло, що компрометація такого облікового запису відкриває зловмиснику «двері» до багатьох ІС відразу [9]. По-друге, як вже згадувалося, користувачам властиво робити помилки, оскільки повністю людський фактор виключити неможливо, хіба що наділити достатніми повноваженнями штучний інтелект, щоб він здійснював підтримку та адміністрування ІС Організації, але поки про це зарано говорити. Третім аспектом, який варто зазначити – використання статичних паролів, тобто адміністраторами використовуються ідентичні паролі до більшості ІС, що ясна річ не є кращою практикою ІБ. Також яскравою проблематикою є так зване «наростання привілеїв». Даний термін означає, що привілейований обліковий запис з часом набуває тих привілеїв, які не потрібні для забезпечення посадових/функціональних обов’язків. Тобто, порушується основоположне правило – принцип мінімальних привілеїв.

Відповідно до викладеного вище можна зробити висновок, що без реалізації спеціальних заходів контролю організації можуть не помітити несанкціонованих привілейованих облікових записів або нелегітимного використання наявних.

З метою забезпечення належного рівня ІБ створено спеціалізовані організації, які визначають і документують найкращі практики у вигляді міжнародних стандартів. Яскравим прикладом таких організацій є Міжнародна організація зі стандартизації (International Organization for Standardization) та

Міжнародна електротехнічна комісія (International Electrotechnical Commission), які здійснюють гармонізацію практик ІБ, зокрема за рахунок забезпечення сумісності стандартів різних країн та регіонів, що сприяє уніфікації підходів до впровадження процесів ІБ, полегшує міжнародну співпрацю та взаємодію в кіберпросторі. Одним з розроблених стандартів цих організацій є ISO/IEC 27001:2022 [10]. Даний стандарт містить низку вимог щодо впровадження СУІБ, і дозволяє адаптувати реалізацію відповідно до специфіки діяльності організації.

Повертаючись до привілейованих прав доступу, то даний стандарт, а саме його контроль A.5.18 (Управління правами доступу), вимагає строге обмеження та підконтрольне надання привілейованих прав доступу. Необхідно забезпечити, щоб такі права надавалися тільки тим особам, які їх дійсно потребують для виконання службових обов'язків, і лише на необхідний період. Стандарт також наголошує на регулярному перегляді привілейованих прав і відкликанні зайвих повноважень. Разом з тим, контроль A.5.17 (Управління автентифікаційною інформацією) рекомендує обмежувати використання технологічних облікових записів з привілейованими права доступу – їх використання має бути під особливим контролем, адже такі інструменти можуть обходити стандартні механізми ІБ.

Також варто приділити увагу рекомендаціям Національного інституту стандартів і технології (NIST), а саме NIST SP-800-53 Rev.5 [11]. містить ряд вимог, спрямованих на мінімізацію ризиків, пов'язаних з адміністративними обліковими записами. Зокрема, контроль AC-6 (Least Privilege) вимагає реалізації принципу найменших привілеїв: користувачам слід надавати найменший рівень доступу, достатній для службових обов'язків. Підсилення AC-6(5) прямо зазначає, що всі привілейовані облікові записи в ІС повинні бути обмежені визначеним колом осіб або ролей – тобто ніхто не має отримувати привілейовані права «за замовчуванням» або без належного обґрунтування.

Інший важливий аспект – розподіл прав та обов'язків (Separation of Duties, контроль AC-5): адміністративні функції необхідно розподіляти між різними відповідальними особами, щоб уникнути концентрації надмірних повноважень у сутності однієї особи.

Контроль IA-2 (Identification and Authentication) висуває вимогу щодо MFA для отримання доступу до привілейованих облікових записів. Практично це означає, що адміністратори мають проходити додаткову перевірку (зокрема, OTP або сертифікатом) при вході в обліковий запис з розширеними правами.

В продовження огляду вимог та рекомендацій щодо захисту привілейованих облікових записів пропонується розглянути неурядову організацію Center for Internet Security (CIS), яка у своїх рекомендаціях також акцентує на необхідності захисту адміністративних привілеїв. У версії 8.1 CIS Critical Security Controls викладено групу заходів з управління доступом (Control 6: Access Control Management), яка включає й контроль використання привілейованих облікових записів. CIS прямо радить застосовувати MFA для всіх облікових записів з привілейованими правами [12]. Разом з тим, необхідно забезпечити централізоване надання-відкликання привілейованих прав доступу (робиться для того, щоб, наприклад, при звільненні співробітника негайно забрати його адміністративні права) та періодично перевіряти актуальність наданих привілеїв і повноважень.

Одним із ключових принципів CIS Controls є «не надавати адміністративні права для щоденної (операційної) роботи», навіть системні адміністратори повинні працювати під звичайним користувацьким обліковим записом і підвищувати привілеї лише на час виконання конкретних задач. Цей принцип тісно перегукується із зазначеними принципами NIST, обмежуючи час життя привілейованих сесій.

Наступним етапом пропонується зануритися більш детально в методи захисту адміністративних облікових записів. Тому спираючись на згадане організаційне підґрунтя, зокрема стандарти ІБ, вироблені такі базові засоби захисту:

Принцип найменших привілеїв і рольова модель надання доступу.

Кожному обліковому запису надаються тільки ті права, які необхідні для забезпечення його функцій, і не більше. Доступ до критичних ІС сегментується за допомогою ролей та рівнів довіри. Надмірні привілеї відкликаються або не надаються взагалі. Такий підхід обмежує потенційну поверхню атаки, навіть якщо

зловмисник скомпрометує один акаунт, він не отримає доступу до всієї інформаційної інфраструктури одразу.

MFA та надійні паролі.

Впровадження механізмів обов'язкової MFA для адміністраторів значно підвищує ІБ процесу автентифікації. Якщо розглянути самі парольні фрази для привілейованих акаунтів, то вони мають бути довгими, унікальними, складними та регулярно (визначає сама організація або регуляторні вимоги з ІБ, якщо такі розповсюджуються на організацію) змінюватися. Багато організацій реалізують політики примусової зміни паролів не тільки адміністраторів, а й звичайних користувачів, скажімо, кожні 30-90 днів.

Також рекомендується вимикати опцію необмеженого строку дії пароля та не використовувати тривіальні парольні фрази. Деякі стандарти встановлюють конкретний час життя пароль, зокрема PCI DSS 4.0 вимагає, щоб адміністративні паролі змінювалися принаймні кожні 90 днів і одразу після першого використання або компрометації.

Використання сховищ/сейфів паролів.

Сховища паролів, так звані «password vaults», є захищеним місцем для централізованого зберігання привілейованих облікових даних з використанням засобів стійкої криптографії. Доступ до сховищ контролюється, тому коли адміністратор ініціює з'єднання з сервером він отримує динамічний пароль зі сховища/сейфа або взагалі не бачить пароля – система сама заповнює форму автентифікації при встановленні сеансу (рис. 2.1).

Такий підхід усуває проблему, коли один і той самий пароль відомий великій кількість користувачів. Сейф може автоматично генерувати нові паролі та змінювати їх на цільових ІС за розкладом (наприклад, щогодини або щодня). Сучасні системи класу PAM майже завжди включають модуль керування паролями привілейованих облікових записів.

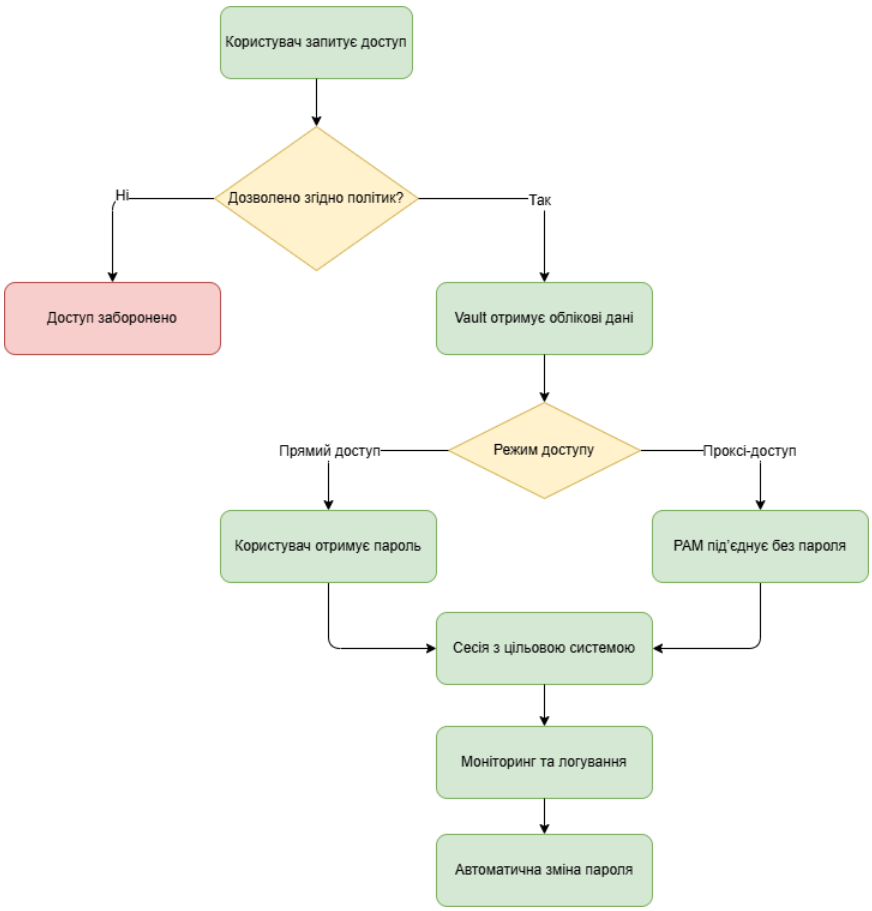

Рис. 2.1. Блок-схема процесу надання доступу до привілейованих облікових записів із використанням сейфів паролів

Моніторинг та логування дій привілейованих користувачів.

Усі дії, які виконуються з привілейованими правами і повноваженнями, мають логуватися: команди, які вводяться, зміни в налаштуваннях, створення нових користувачів тощо. Необхідно зберігати детальні журнали подій, а по можливості – записи сесій (наприклад, відеозапис екрану або текстовий журнал введених команд). Це певною мірою створює додатковий ефект стримування, оскільки адміністратор ІС розуміє, що його дії фіксуються, забезпечуючи доказову базу на випадок розслідування інцидентів ІБ. Кращі практики ІБ передбачають впровадження SIEM-систем для централізованої кореляції подій ІБ не тільки привілейованих користувачів, а й інформаційної інфраструктури в цілому, для аналізу на предмет аномалій. Наприклад, якщо адміністратор раптово починає виконувати нестандартні команди або підключатися в нетиповий час (поза робочим) – цей факт має бути виявлено та перевірено.

Розподіл обов'язків і контроль використання інструментів.

Небезпечним є сценарій, коли одна особа має надто широкі можливості (наприклад, може і створювати користувачів, і затверджувати собі права доступу, і здійснювати конфігурування критичних ІС). З метою уникнення подібних до вищезгаданої ситуації впроваджується принцип «четверо очей». Даний принцип означає залучення різних людей та інструментів протягом усього життєвого циклу операції (зміни). Кожен етап перевірки в процесі затвердження має бути доручений різним співробітникам, щоб підвищити загальний рівень ІБ.

Принцип «четверо очей» відповідає концепції розподілу обов'язків, згідно з якою жоден працівник не повинен мати можливості одночасно здійснювати та приховувати шахрайство або помилки. Кожна важлива дія виконується окремою людиною, щоб зменшити ризик шахрайства та/або обману. Чітке обмеження повноважень співробітників є ключовим фактором для ефективного процесу авторизації [13].

Окремо необхідно контролювати технологічні облікові записи з привілейованими правами та повноваженнями (наприклад, засоби автоматизації прямого редагування БД, відключення журналювання подій тощо) – доступ до них обмежується, щоб навіть адміністратори не могли їх запустити без спеціального дозволу.

Just-In-Time (JIT) доступ та мінімізація «постійних» привілейованих прав.

Новітній підхід – не надавати адміністративні доступи на постійні основі, а видавати їх лише на час виконання конкретного операційного завдання. Тобто, коли інженеру потрібно зробити зміни на сервері, він запитує тимчасове підвищення привілеїв або чек-аути потрібних облікових даних. Після завершення робіт привілейовані права автоматично відкликаються (рис. 2.2). Така модель Zero Standing Privileges (ZSP) запобігає ситуації, коли у великої кількості облікових записів є постійні привілейовані права доступу, якими можна скористатися в будь-який момент. JIT-доступ, як правило, реалізується через централізовану PAM-систему, яка в реальному часі надає дозвіл на доступ і відслідковує, коли треба відкликати доступ.

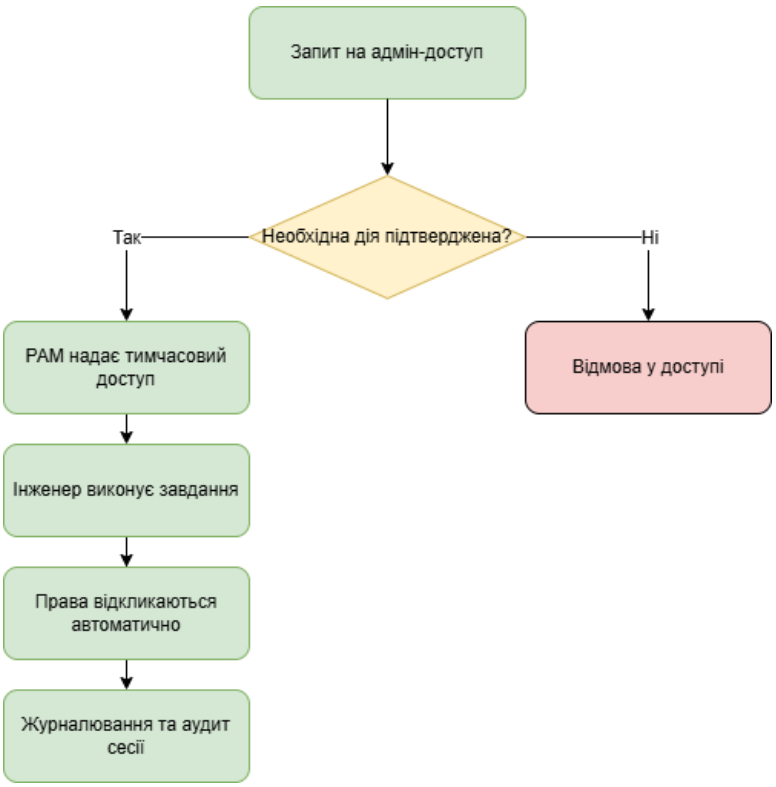

Рис. 2.2. Блок-схема процесу надання JIT доступу через PAM-систему

Обмеження віддаленого доступу та сегментація мережі.

Адміністративні інтерфейси і порти (наприклад, RDP, SSH) рекомендовано ізолювати від загального сегменту користувацької мережі. Для цього можна використовувати бастіон-хости або шлюзи – проміжні сервери, через які проходить весь адміністративний трафік. Такий підхід дозволяє застосувати механізми додаткової автентифікації і здійснювати контроль на точці входу. Міжмережеві екрани налаштовуються у такий спосіб, щоб зовнішні підключення напряму до критичних ІС були неможливими – лише через захищений шлюз. У такий спосіб реалізовується модель Zero Trust Network Access (ZTNA) для привілейованих користувачів, де кожне підключення перевіряється і має бути санкціонованим.

Регулярні перевірки та навчання персоналу.

Ще однією вагомою складовою є регулярне проведення аудиту привілейованих облікових записів, зокрема здійснювати перегляд списку адміністраторів, аналізувати, чи всі вони ще потребують доступу, перевіряти відповідність політикам ІБ (наприклад, відсутність спільних облікових записів, забезпечення достатньої складності паролів тощо). Виявлені порушення потрібно

негайно виправляти – надмірні права доступу відкликаються, а надлишкові облікові записи блокуються.

Разом з тим, необхідно регулярно (рекомендовано щорічно) проводити навчання для усіх користувачів з кібергігієни. Формування культури ІБ серед користувачів є не менш важливим фактором, ніж впровадження та підтримка технічних засобів захисту інформації.

З огляду на комплексність описаних задач, стає очевидним, що автоматизовані рішення класу PAM є доцільними для впровадження, оскільки вручну виконувати вищезгадані заходи в масштабі великої організації складно і дорого, тоді як спеціалізовані системи можуть забезпечити централізований контроль привілейованого доступу. Вже згадані в попередньому розділі рішення PAM (CyberArk, Wallix, Fudo PAM тощо) реалізовуються більшість зазначених механізмів «під одним дахом». Зокрема, вони пропонують керування паролями, моніторинг сесій, модуль надання JIT. Таким чином, сучасна практика захисту привілейованих облікових записів ґрунтується на поєднанні різних методів (рольової моделі надання доступу, принципу найменших привілеїв тощо) та технічних засобів (PAM-рішення), які разом дозволяють суттєво знизити ризик несанкціонованого доступу до критичних інформаційних систем та ресурсів організації.

2.2. Архітектура Fudo Security PAM

Fudo Security пропонує комплексне рішення для керування привілейованим доступом – продукт Fudo PAM (названий у нових версіях Fudo Enterprise). Це програмно-апаратний комплекс «все-в-одному», який може постачатися як фізичний пристрій або віртуальна машина для розгортання у мережі організації. Архітектурно Fudo PAM побудований за принципом бастіон-сервера (proxy), тобто всі підключення привілейованих користувачів проходять через спеціальний шлюз, який виконує роль посередника між користувачем і цільовим сервером. Важливою рисою є «agentless-архітектура», бо Fudo не потребує встановлення жодних

клієнтських чи серверних агентів на робочі станції адміністраторів або на сервери, до яких здійснюється підключення. Такий підхід значно спрощує інтеграцію, оскільки адміністратори можуть підключатися до ІС через Fudo, використовуючи свої звичні засоби (зокрема, RDP-клієнт чи SSH-термінал), просто ініціюючи з'єднання через Fudo. Разом з тим, це дозволяє розгорнути рішення в стислі терміни. (постачальник заявляє про «розгортання за один день» без суттєвих змін інфраструктури) [14].

Внутрішня архітектура Fudo PAM модульна – включає кілька функціональних підсистем, тісно інтегрованих між собою. Відповідно до офіційної документації, Fudo PAM містить наступні функціональні можливості:

- Моніторинг та запис сесій/сеансів – надає адміністраторам безпеки розширені інструменти для моніторингу та управління сесіями в режимі реального часу. Адміністратори безпеки можуть приєднуватися, ділитися, призупиняти або завершувати сеанси привілейованих користувачів, забезпечуючи швидке реагування на потенційно підозрілі дії. Платформа підтримує спільний доступ до ресурсів по більш ніж 10 протоколам, включаючи RDP, SSH і HTTPS, забезпечуючи безпечний доступ до критично важливих ІС. Fudo PAM записує весь мережевий трафік разом з метаданими, що дозволяє точно відтворювати сеанси та здійснювати повнотекстовий пошук контенту. Ця функція забезпечує повний аудиторський журнал для підвищення безпеки та дотримання нормативних вимог.
- Управління секретами (сейф паролів) – як вже згадувалося, Fudo PAM надає безпечну та гнучку систему для управління привілейованими обліковими записами. Облікові дані надійно зберігаються і ніколи не залишають систему, забезпечуючи надійний захист.
- JIT – дана функціональна можливість дозволяє організаціям реалізовувати Zero-Trust підхід. За допомогою JIT адміністратори безпеки можуть визначати і планувати конкретні часові вікна для доступності ресурсів, надаючи доступ тільки тоді, коли це необхідно. Даний факт дозволяє забезпечувати дотримання принципу мінімальних привілеїв, мінімізуючи ризики ІБ шляхом обмеження тривалого доступу до критично важливих ІС.

- SSO – спрощує автентифікацію, автоматично реєструючи користувачів у ІС, підвищуючи зручність та ефективність роботи, зберігаючи при цьому надійні стандарти безпеки.
- Зручний доступ без агентів – гнучкий доступ до інформаційних ресурсів без використання агентів, який дозволяє користувачам обирати зручний для них спосіб підключення. Користувачі можуть продовжувати використовувати свої улюблені нативні клієнти для безперебійної роботи або скористатися перевагами вбудованого веб-клієнта на основі браузера, який надається Fudo PAM. Така гнучкість забезпечує простоту використання як для технічних, так і для нетехнічних користувачів.
- Профілактика на основі штучного інтелекту – використовує можливості штучного інтелекту з метою оптимізації виконання щоденних завдань. Надає рекомендації для підтримки процесів верифікації та моніторингу, спрощуючи обов'язки адміністраторів безпеки. Аналізуючи поведінкові та семантичні шаблони, Fudo PAM виявляє потенційну компрометацію облікових даних і надсилає сповіщення, забезпечуючи швидке реагування на потенційні інциденти ІБ, що зменшує ризики і посилює загальну безпеку ІС.
- Аналізатор продуктивності – відстежує дії користувачів і надає точну інформацію про їхню активність і час простою. Аналіз сесій детально показує продуктивність користувачів за певний період часу. Параметр «Поріг активності» дозволяє визначити сеанси, користувачів, які не перевищують необхідний рівень активності користувачів, а також допомагає встановити граничне значення, досяжне для певної кількості користувачів або сеансів. Також наявний рейтинг активності користувачів, який дозволяє виявити сеанси, які не перевищують необхідний рівень активності користувачів [15].

Отже, такий набір функціональних можливостей та модулів охоплює ключові аспекти керування привілейованим доступом, від спостереження за діями привілейованих користувачів до захисту їх облікових даних. Fudo PAM побудований як єдиний веб-застосунок з двома основними консолями: адміністративна панель (для налаштування політик, керування користувачами,

перегляду журналів подій) та користувацький портал (через який привілейовані користувачі ініціюють свої підключення). Для зберігання даних (записів сесій, журналів подій, конфігурацій) Fudo PAM використовує внутрішнє сховище. Всі критичні дані можуть резервуватися, а для цілісності журналів застосовано механізм довірчого міткування часу (trusted timestamping) – щоб записи не могли бути непомітно змінені.

Також варто зауважити, що Fudo PAM розроблений, щоб допомогти організаціям відповідати широкому спектру нормативних вимог, включаючи PCI-DSS, SOX, HIPAA, NIST, GDPR та ISA/IEC 62443. Надаючи надійні механізми ІБ та аудиту, Fudo PAM забезпечує дотримання галузевих стандартів і нормативних вимог, спрощуючи управління відповідністю для організацій.

Важливою частиною архітектури є модель даних, яка відображає, як Fudo PAM керує об’єктами доступу. В системі визначено п’ять базових типів об’єктів: користувач (user), сервер (server), обліковий запис (account), сейф (safe) та слухач (listener). Пропонується розглянути детальніше кожен з них:

Користувач (user) – суб’єкт (людина або обліковий запис), який має право підключатися до серверів через Fudo PAM у межах контрольованої зони IT-інфраструктури. Детальне визначення суб’єкту (наприклад, унікальна комбінація логіна та домену, повне ім'я, адреса електронної пошти тощо) дозволяє чітко відстежувати дії користувача, коли логін і пароль замінюються на спільні облікові дані для входу в обліковий запис.

Сервер (server) – ресурс IT-інфраструктури, до якого можна отримати доступ за одним із зазначених протоколів. В об’єкті «Server» задається IP-адреса або назва вузла, тип протоколу (SSH, RDP тощо) та інша інформація про цільову ІС.

Обліковий запис (account) – визначає привілейований обліковий запис, який створений на сервері, за яким здійснюється контроль. Об’єкт містить реальні облікові дані для входу, режими автентифікації користувача: анонімний (доступ без автентифікації користувача), звичайний (Fudo підставляє логін і пароль замість користувача) або переадресований (Fudo переадресовує логін і пароль).

Сейф (safe) – центральний об’єкт моделі надання доступу, який безпосередньо регулює доступ користувачів до серверів, які знаходяться під контролем. Даний елемент визначає можливості доступних протоколів, політики та інші деталі, які стосуються взаємовідносин користувачів і серверів. Фактично, сейф визначає, які користувачі можуть підключатися до яких серверів та під якими обліковими записами, і з якими обмеженнями.

Слухач (listener) – об’єкт, який визначає режим з'єднання з сервером через PAM, а також його особливості, зокрема конкретні мережеві налаштування (IP-адресу та порт), які слухає Fudo PAM і куди спрямовує підключення [16].

Наступним кроком пропонується розглянути сценарії розгортання Fudo PAM в інформаційному середовищі організації. Дане рішення підтримує кілька варіанті інтеграції в IT-інфраструктуру, щоб підлаштуватися під конкретні цілі та потреби організації.

Перший варіантом розгортання Fudo PAM є міст (bridge). В такому випадку PAM виступає посередником між користувачами і серверами незалежно від того, чи контролюється трафік (тобто використовується будь-який з підтримуваних протоколів) чи ні (рис. 2.3).

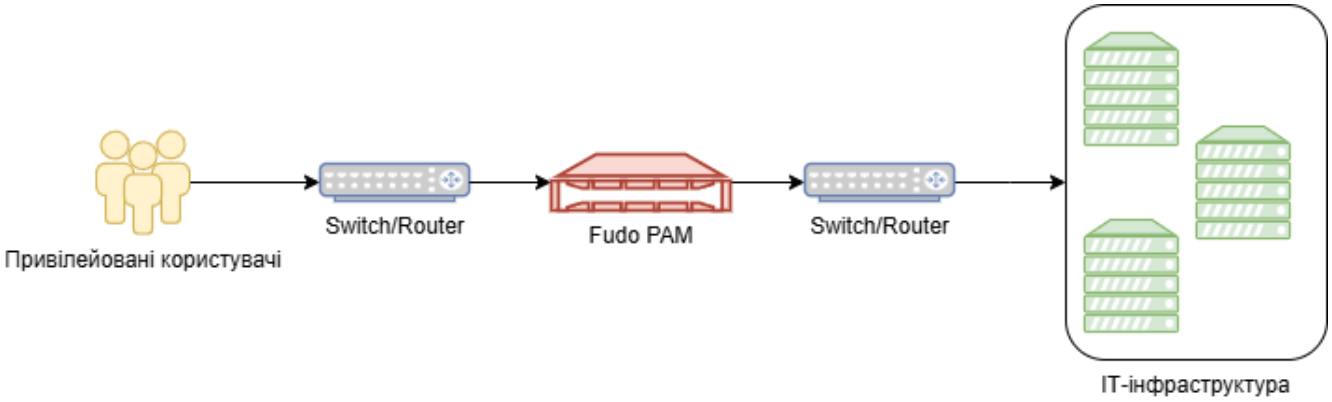

Рис. 2.3. Схема «Міст» розгортання PAM-системи

Іншим прикладом розгортання Fudo PAM є примусова маршрутизація (forced routing). Даний режим вимагає використання правильно налаштованого маршрутизатора. Таке рішення дозволяє контролювати мережевий трафік на третьому (мережевому рівні) моделі OSI, тому тільки привілейовані запити

проходять через PAM, а решта трафіку перенаправляється безпосередньо на цільовий сервер призначення (рис. 2.4).

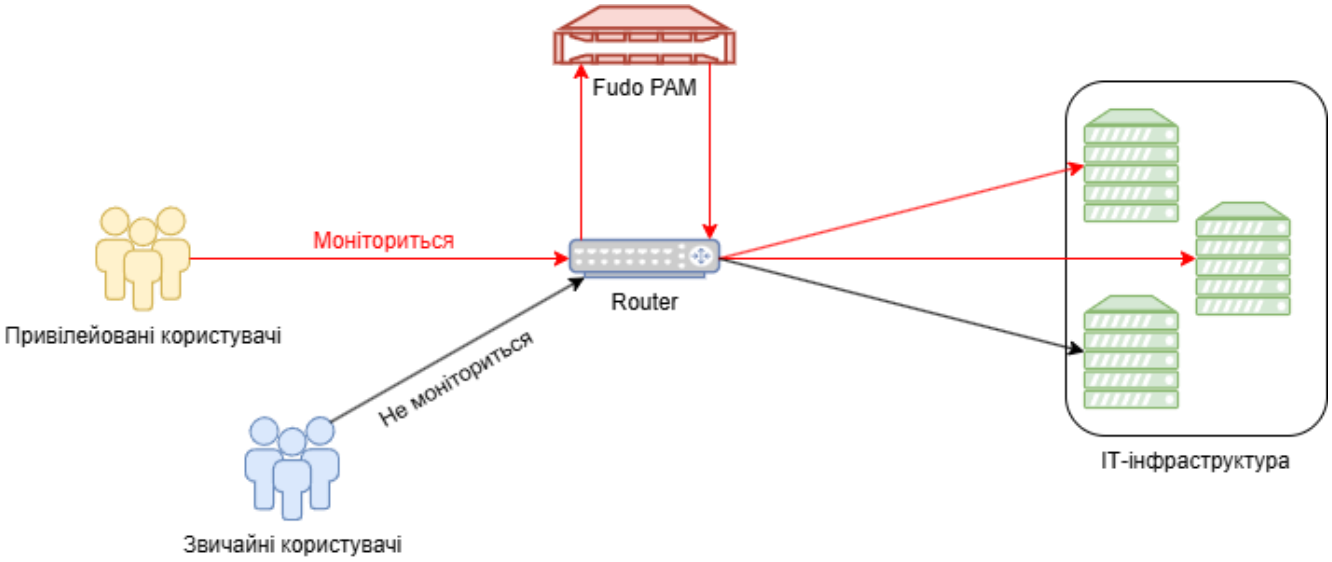

Рис. 2.4. Схема «Примусова маршрутизація» розгортання PAM-системи

Після розгортання Fudo PAM користувачеві необхідно здійснити підключення до кінцевих серверів. Варіанти підключень у свою чергу також поділені на кілька видів, а саме:

Прозорий (transparent)

У прозорому режимі користувачі підключаються до кінцевого сервера призначення, використовуючи задану IP-адресу сервера (рис. 2.5).

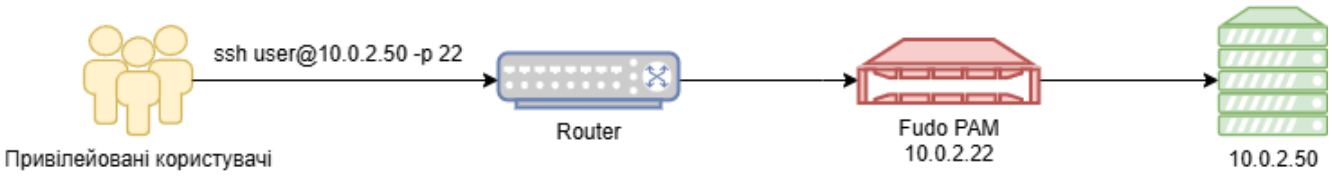

Рис. 2.5. Схема прозорого (transparent) підключення

Шлюз (gateway)

У режимі шлюзу користувачі підключаються до сервера призначення, використовуючи реальну IP-адресу сервера. Fudo PAM виступає посередником при з'єднанні з сервером, використовуючи власну IP-адресу. Це гарантує, що трафік від сервера до користувача проходить через Fudo PAM (рис. 2.6).

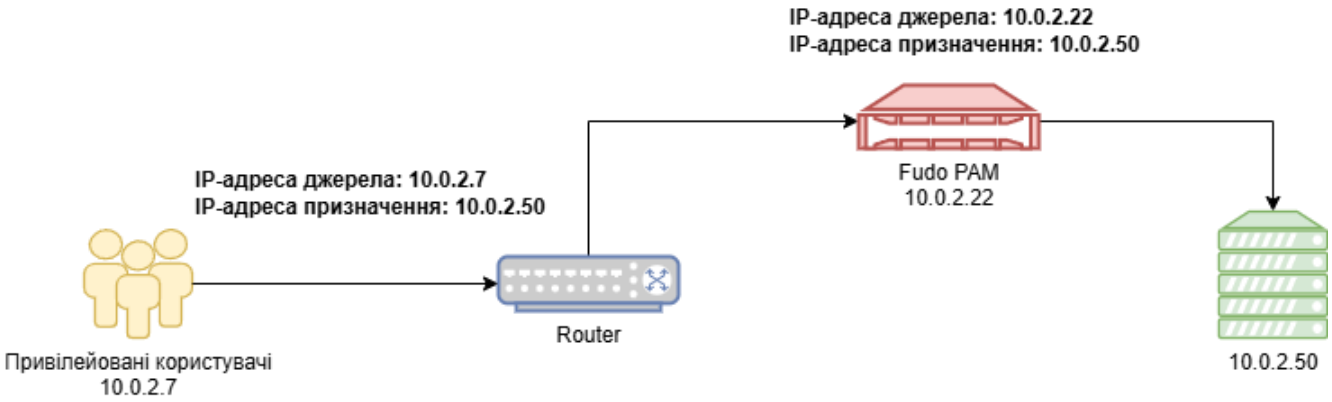

Рис. 2.6. Схема підключення – шлюз (gateway)

Проксі (proxy)

У режимі проксі привілейований користувач з'єднується з сервером призначення, використовуючи комбінацію IP-адреси Fudo PAM та унікального номера порту, призначеного для даного сервера. Унікальність цієї комбінації дозволяє встановити з'єднання з конкретним ресурсом (рис. 2.7). Такий підхід дозволяє приховати реальну IP-адресу і дозволяє налаштувати сервери на прийом запитів тільки від Fudo PAM.

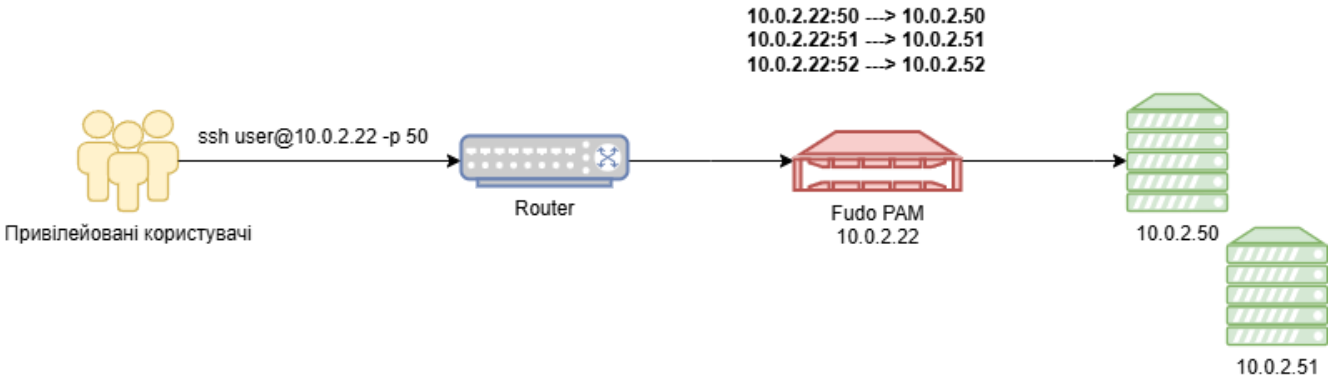

Рис. 2.7. Схема підключення – проксі (proxy)

Бастіон (bastion)

У режимі бастіону цільовий хост вказується в рядку, що ідентифікує користувача і сервер, до якого він намагається підключитися, наприклад, ssh user#root@10.0.2.22. Це дозволяє полегшити доступ до групи серверів, що контролюються, за допомогою однієї і тієї ж комбінації IP-адреси і номера порту (рис. 2.8).

Під час підключення Fudo PAM очікує:

- <ім'я користувача>[@домен][#<логін сервера>#<адреса>[:<порт>]],

де:

- <ім'я користувача>: логін користувача на Fudo PAM,
- [@domain] необов'язковий,
- <serverlogin>: логін користувача на цільовому сервері,
- <адреса>: адреса сервера на цільовому сервері (<порт> можна не вказувати, якщо він є рідним для протоколу).

Режим бастіону підтримується при підключенні за протоколами SSH, RDP, VNC, Telnet, Telnet 3270, Telnet 5250, MS SQL.

Рядок цільового об'єкта перевіряється в наступній послідовності:

1. Точне ім'я користувача – Fudo PAM намагається зіставити рядок з об'єктом, визначеним у локальній БД.
2. Точна адреса сервера – Fudo PAM намагається зіставити рядок з IP-адресою об'єкта сервера, визначеного в локальній БД.
3. IP-адреса, повернута службою DNS – Fudo PAM запитує службу DNS і намагається зіставити повернуту IP-адресу з IP-адресою об'єкта сервера, визначеного в локальній БД.
4. Ім'я хоста, повернуте службою зворотного DNS – Fudo PAM запитує службу зворотного DNS і намагається зіставити повернуте ім'я хоста з об'єктом сервера, визначеним у локальній БД.

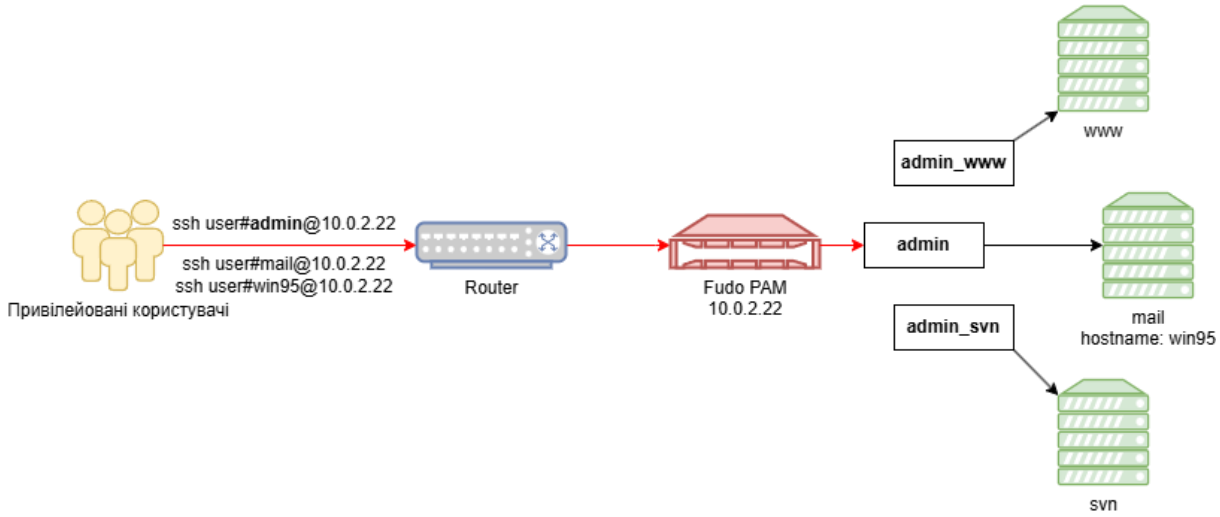

Рис. 2.8. Схема підключення – бастіон (bastion)

Для більш кращого розуміння пропонується розглянути концептуальну мережеву схема роботи Fudo PAM (рис. 2.9). Адміністратор встановлює з’єднання не безпосередньо з цільовим сервером, а з адресою Fudo PAM (крок 1). Fudo PAM автентифікує користувача (може запросити окремий логін/пароль, або інтегрується з Active Directory для Single Sign-On) і визначає, до якого ресурсу той намагається підключитися. Далі Fudo PAM від свого імені відкриває сесію до потрібного сервера, використовуючи облікові дані, що зберігаються у сейфі (крок 2). Після встановлення сеансу, Fudo PAM ретранслює усі дані між користувачем та сервером у режимі реального часу (крок 3), одночасно відстежуючи та записуючи кожну дію (крок 4). Адміністратор працює, як зазвичай, але всі його команди, натискання клавіш, переміщення миші тощо фіксуються. Якщо Fudo PAM виявить порушення політики (наприклад, виконання забороненої команди), він може миттєво розірвати з’єднання (крок 5). Завершена сесія зберігається у вигляді зашифрованого запису для подальшого аналізу (крок 6).

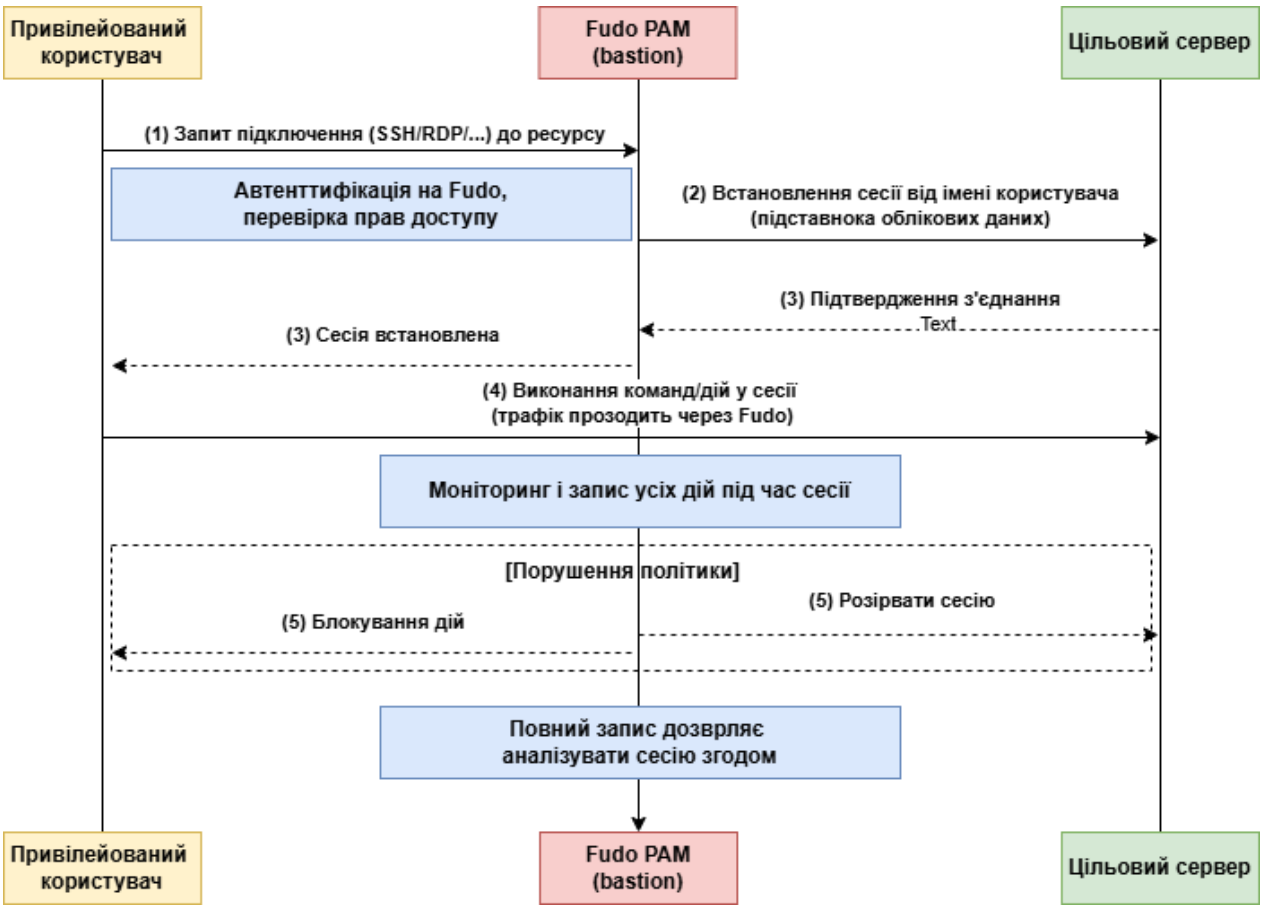

Рис. 2.9. Концептуальна мережева схема роботи Fudo PAM

Fudo PAM виступає посередником між адміністратором і сервером, контролюючи автентифікацію, командний потік і дозволи. Всі дії протоколюються і при виявленні порушень або загрози Fudo PAM може миттєво втрутитися (розірвати або призупинити сесію).

Отже, архітектура Fudo PAM спроектована з акцентом на безперервний контроль та зручність впровадження. Завдяки відсутності агентарного підходу (agentless) і режиму підключення «бастіон», Fudo PAM можна впровадити без кардинальної перебудови інформаційної інфраструктури, отримавши при цьому повний контроль над діяльністю привілейованих користувачів та їх сесій підключення до критичних серверів. Модульність та масштабованість рішення дозволяє його адаптувати під різні вимоги – від невеликого IT підрозділу до розподіленої корпоративної мережі з тисячами користувачів.

2.3. Призначення та функції Fudo PAM для захисту привілейованих користувачів

Основною метою впровадження Fudo PAM є забезпечення централізованого захисту та контролю діяльності привілейованих користувачів, тим самим мінімізуючи ризики несанкціонованого доступу. PAM діє як щит між привілейованим користувачем і критичними ресурсами, контролюючи кожен сеанс. По суті, Fudo PAM реалізовує концепцію Zero Trust для привілейованих користувачів, тобто кожен доступ має бути дозволений політиками та підлягає моніторингу. Таким чином, призначення Fudo PAM – унеможливити несанкціонований або неконтрольований доступ привілейованих осіб до критичних ІС організації. Для цього рішення Fudo реалізує цілий набір функцій, що охоплюють всі стадії життєвого циклу привілейованого доступу: від керування обліковими даними до моніторингу сесій у реальному часі та подальшого аналізу. Розглянемо ключові функціональні можливості Fudo PAM та їх значення для ІБ:

Моніторинг, контроль і запис привілейованих сесій.

Базова функція Fudo PAM, яка відрізняє його від звичайних засобів управління доступом. Кожне підключення привілейованого користувача через PAM автоматично потрапляє під спостереження. Fudo PAM здійснює повний запис сеансу, для CLI сесій (SSH, Telnet тощо) зберігається журнал команд і вихідних даних, а для графічних сесій (RDP, VNC, X11, веб-браузер) – відеозапис екрану, синхронізований з подіями (рухами миші, натисканнями клавіш). При цьому підтримується запис навіть протоколів БД (наприклад, запити SQL) і веб-запитів HTTP/HTTPS. Fudo діє як «чорний ящик», тому усі дії адміністратора фіксуються з точністю до мілісекунд і зберігаються у зашифрованому вигляді (з мітками часу) на пристрої. Записи захищені від редагування і можуть слугувати доказом у разі інциденту ІБ (формат збереження завірений, наявний контроль цілісності).

Більше того, Fudo PAM дозволяє не лише пасивно записувати, а й активно контролювати сесії в реальному часі. Адміністратор безпеки або інша відповідальна особа може через веб-інтерфейс Fudo переглядати наживо все, що відбувається на екрані привілейованого користувача. Якщо фіксується підозріла активність, система надає можливість негайно втрутитись, а саме призупинити сесію, завершити її або навіть під’єднатися у сесію привілейованого користувача та працювати в ній у режимі спільної роботи. Функція «join live session» (спільний сеанс) дає змогу другому адміністратору безпеки приєднатися до поточної сесії привілейованого користувача – при цьому дії кожного позначаються окремо, а підключеного адміністратора безпеки можна обмежити тільки режимом спостерігача або надати можливість керувати курсором/вводом. Такий режим корисний для навчання або супроводу зовнішніх підрядників. Наприклад, більш досвідчений інженер контролює дії підрядника, або два адміністратори разом вирішують проблему на сервері.

Важливо, що Fudo PAM може автоматично реагувати на певні події ІБ у сесії без участі людини. Завдяки функціям політик безпеки, адміністратори Fudo задають тригери. Зокрема, якщо в SSH-сесії вводиться заборонена команда («sudo su» чи «useradd»), або якщо в RDP виявлено спробу скопіювати файли, – PAM одразу блокує сеанс. Вбудований механізм застосування політик може як

попередити адміністратора безпеки, але дозволити користувачеві продовжити роботу (Policy Alert), так і повністю розірвати з'єднання (Policy Terminate). Таким чином, Fudo не тільки збирає дані для пост-фактум аналізу, а й активно запобігає порушенням в момент їх вчинення. Такі функціональні можливості надзвичайно важливі для запобігання випадковим або навмисним руйнівним діям. Наприклад, якщо привілейований користувач помилково ініціює видалення критичних файлів критичні файли – Fudo PAM зможе його зупинити.

Для чого усе це? По-перше, безперервний моніторинг дисциплінує привілейованих користувачів, оскільки усвідомлення тощо, що всі дії записуються та фіксуються – суттєво знижує вірогідність зловживань. По-друге, у разі інциденту ІБ безцінним стає ретроспективний аналіз. Саме із записів, які сформовані PAM-системою можна точно відтворити, що саме робив привілейований користувач в ІС, які команди вводив, які додатки відкривав. Цей функціонал значно спрощує розслідування інцидентів ІБ та пошук їх першопричин. В записах реалізовано пошук по подіях і тексту: Fudo PAM використовує OCR (оптичне розпізнавання символів) для відеозаписів екрану, тому навіть текст на скріншотах RDP-сесії стає доступним для пошуку. Адміністратор безпеки може за ключовим словом знайти всі згадки в архівах (наприклад, який користувач вводив команду «shutdown» або коли на екрані з'являлася помилка з певним кодом). Тому можна зробити висновок, що це значно ефективніше, ніж перегляд «сирих» log-файлів серверів або системних журналів. Власне, девізом таких систем є «контролюй та записуй дії користувачів, уникаючи необхідності кропіткої перевірки log-файлів», що Fudo PAM і реалізує на практиці.

Окремо варто зазначити вигоду для самих привілейованих користувачів. Наявність повного запису їхньої роботи може захистити цих користувачів від необґрунтованих звинувачень. У випадку, якщо виникла підозра, що привілейований користувач щось неправильно налаштував чи перевищив повноваження, запис сесії дозволяє об'єктивно перевірити, чи це так. Тому чесний співробітник завжди зможе довести коректність своїх дій, посилаючись на журнали подій PAM.

Керування паролями та обліковими даними (секретами).

Fudo PAM виконує роль централізованого менеджера привілейованих облікових записів, зберігаючи їхній «ключ» – паролі або ключі доступу, у захищеному сховищі. У термінології Fudo є функція «Прихований адміністратор» (Hidden Admin) – саме так маркетингово названо модуль керування паролями. Його суть полягає в тому, що всі паролі для кінцевих серверів зберігаються всередині PAM у зашифрованому вигляді (з використанням стійкої криптографії), і користувачі не мають прямого доступу до цих паролів. Коли привілейований користувач ініціює підключення до цільового сервера, він фактично отримує не сам пароль, а можливість встановити сесію через Fudo (як було вже згадано – Fudo PAM підставляє пароль самостійно) [17].

PAM дозволяє задати політики паролів для кожного облікового ззапису: мінімальна довжина, складність (вимоги до символів), строк дії тощо. Система сама може перевіряти відповідність пароля політикам та навіть визначати, чи пароль достатньо надійний (зокрема, перевірками з використанням БД із відомими зламаними паролями). У разі невідповідності – генерується новий або вимагається зміна. Досить важливою функцією є автоматизована ротація паролів (Password Rotation): PAM може з певним інтервалом змінювати пароль привілейованого облікового запису на сервері на новий, синхронізуючи цю діяльність зі своїм сейфом. Зокрема, можна налаштувати, щоб паролі локального адміністратора на серверах Windows змінювалися щодня о 00:00. Сама процедура зміни виконується через сценарії (password changers) – Fudo PAM підтримує як Unix-подібні системи, Windows, БД MySQL тощо для автоматичного оновлення паролів. Зазначені функціональні можливості дозволять вирішити проблему «застарілих» паролів, які роками не змінюються і можуть бути відомі великій кількості користувачів. З Fudo PAM після завершення кожної привілейованої сесії можна відразу змінити пароль, тож навіть, якщо хтось його дізнався під час сесії – він більше не буде дійсний.

Додатково «Hidden Admin» веде історію паролів і зберігає попередні значення для можливості екстреного відновлення доступу. Наприклад, якщо з якоїсь причини новий згенерований пароль не спрацював, адміністратор безпеки з

відповідними повноваженнями зможе дізнатися попередній і увійти. Це важливо для забезпечення умов відмовостійкості. Також Fudo PAM відстежує несанкціоновані зміни паролів поза системою, а саме якщо хтось вручну змінив пароль на самому сервері, PAM-система це виявить (та не дозволить увійти наступного разу) і помітить такий випадок для проведення розслідування. Таким чином, будь-яка маніпуляція з обліковими даними привілейованих облікових записів знаходиться під контролем PAM.

У підсумку ця функціональність дозволяє реалізувати рекомендації та вимоги міжнародних стандартів в рамках керування обліковими даними, які детальніше описані в розділі 2.1, з використанням автоматизації.

Також, варто зауважити, що Fudo PAM дозволяє керувати не тільки паролями для інтерактивних входів, а й обліковими даними, які використовуються системами автоматично (Application Accounts). Модуль AAPM (Application to Application Password Manager) надає API/плагіни, через які інші програми можуть запитувати секрети (облікові дані) з сейфа Fudo PAM або зберігати їх туди. Такий чином усувається потреба в зберіганні паролів до БД чи сервісів у відкритому вигляді у конфігураціях, скриптах чи коді. Наприклад, веб-додаток може динамічно отримувати пароль до БД з менеджеру секретів Fudo при старті, а функціональні можливості PAM можуть регулярно змінювати/оновлювати цей пароль, не перериваючи роботу додатку.

Тимчасове підвищення привілеїв та керування доступом (Just-In-Time, Approval Workflow).

Fudo PAM підтримує концепцію JIT доступу і гнучкі механізм надання дозволів. Адміністратор безпеки може налаштувати, що деякі особливо критичні ресурси вимагають додаткового попереднього схвалення перед кожним підключенням. Вбудована система workflow-запитів дозволяє привілейованим користувачам запитати доступ до певного сейфу або сервера, а відповідальній особі – схвалити чи відхилити цей запит. Наприклад, зовнішній підрядник хоче підключитися до ІС – він надсилає запит через веб-інтерфейс Fudo, адміністратор безпеки бачить і підтверджує підключення (або відхиляє) через адміністраторський

інтерфейс. Тільки після затвердження користувач зможе розпочати сесію. Такий процес забезпечує принцип «четверо очей», особливо для операцій з високим рівнем ризику. Запити можуть бути як одноразовими, так і на певний час або за розкладом. Fudo PAM дозволяє автоматизувати деякі запити, наприклад, користувач з групи «DBAdmins» може автоматично отримувати доступ до серверів БД у робочий час, але потребувати схвалення у неробочий. Ефективність роботи при цьому не сильно страждає, оскільки інтерфейс зроблено зручним: користувачі самі можуть ініціювати JIT-доступ через портал, а адміністратор безпеки навіть має спеціальний мобільний додаток Fudo Officer 2.0 для швидкого підтвердження запитів на ходу.

Застосування JIT-доступу та тимчасових прав у Fudo PAM означає, що організація може сміливо забирати постійні привілейовані права та повноваження у більшості користувачів (зведення Zero Standing Privileges (ZSP) до мінімуму). Всі необхідні підвищення привілеїв будуть відбуватися централізовано під наглядом. Якщо у звичайній ситуації десятки людей постійно мають доступ до паролів від критичних ІС (і в будь-який момент компрометації одного з них стає достатньо для інциденту ІБ), то з Fudo PAM – ніхто не знає паролів (їх знає тільки сейф), а щоб встановити сесію, треба отримати явний дозвіл. При цьому PAM забезпечує, щоб такий дозвіл легко запитувався і був операційно прийнятним для організації (швидко надавався).

Виявлення аномалій та захист від компрометації облікових даних.

Сучасні версії Fudo PAM включають елементи штучного інтелекту та машинного навчання для профілювання поведінки користувачів. Модуль під назвою User Behavior Analytics (інтегрований в Efficiency Analyzer) постійно аналізує дії привілейованих користувачів у сесіях і будує поведінкові моделі для кожного профілю. Наприклад, один адміністратор зазвичай працює з певним набором серверів і виконує обмежений перелік команд, тоді як інший діє абсолютно інакше. Система PAM, навчившись на історичних даних, може з високою точністю помічати відхилення від типового поведінкового патерну. Якщо облікові дані адміністратора раптом використовує інша особа (зловмисник) – її дії,

найімовірніше, будуть некоректні з точки зору звичного профілю (зокрема, вхід та автентифікація у позаробочий час, спроби доступу до нових ІС, масове виконання нетипових команд). Fudo PAM в реальному часі відстежує такі аномалії і може налаштовувати автоматичні сповіщення або реакції на них.

Навіть якщо зловмисник якимось чином обійшов попередні бар'єри (наприклад, отримав доступ через вкрадений токен і ввійшов у Fudo PAM), його підозрілу поведінку буде оперативно виявлено. Система PAM може одразу сповістити команду адміністраторів безпеки та, за наявності необхідних налаштувань, заблокувати сесію при виявленні аномалій. За рахунок цього Fudo PAM забезпечує проактивний захист від компрометації привілейованих акаунтів. Фактично впроваджується аналог IDS/IPS, але на рівні привілейованих сесій – коли дії виходять за рамки норми, спрацьовує «тривожна кнопка».

Крім безпеки, модуль Efficiency Analyzer виконує і утилітарну задачу – облік продуктивності привілейованих користувачів. Зібрані дані про активність (тривалість сеансів, час простою, виконані дії) агрегуються і можуть використовуватись для бізнес-аналітики. Керівники структурних підрозділів організації можуть отримати звіти, скільки часу витрачається на ті чи інші задачі, як ефективно працюють підрядники тощо. Хоча це вже більше стосується оптимізації процесів, а не безпосередньо ІБ, на практиці такий аналіз теж корисний, бо він дозволяє виявити, зокрема підозріло низьку активність (чи не покинув хтось сесію відкритою?) або неефективне використання ресурсів.

Централізований портал доступу та зручність для користувачів.

Усі перераховані функції безпеки були б марними, якби рішення було надто громіздким та незручним у використанні для самих привілейованих користувачів. Розробники Fudo приділили достатню увагу і цьому аспекту. PAM-система надає – єдину точку, де привілейований користувач бачить перелік доступних йому ресурсів (серверів, пристроїв, додатків). Користувачу не потрібно пам'ятати десятки IP-адрес і облікові дані від різних ІС, бо це все скомпоновано у Fudo PAM (авторизувавшись один раз, можливо з SSO) і далі просто обрати потрібний ресурс у відповідному переліку. Під капотом Fudo PAM запустить потрібний клієнтський

застосунок (наприклад, RDP-клієнт прямо у браузері через HTML5, або SSH-консоль) і встановить з’єднання.

Використання такого веб-інтерфейсу суттєво спрощує роботу привілейованих користувачів, оскільки вони витрачають менше часу на здійснення підключень. До того ж портал гарантує, що привілейовані користувачі підключаються саме за допомогою Fudo PAM (не оминаючи його), тобто політики ІБ не будуть випадково обійдені. Важливо зауважити, що підтримуються і нативні клієнти. Зокрема, якщо адміністраторові зручніше працювати через термінал чи Remote Desktop застосунок, то він може використовувати їх, просто вказавши в якості хоста PAM (а далі, після входу, вибрати цільовий сервер). У такий спосіб звички користувачів майже не змінюються, що полегшує впровадження рішення.

На основі аналізу можливостей Fudo PAM можна зробити висновок, що дане рішення покриває практично весь спектр заходів, необхідних для надійного захисту привілейованих облікових записів в організації. Воно є прикладом реалізації принципів, описаних в підрозділі 2.1, на практиці з використанням сучасних технологій. Впровадження Fudo PAM дозволяє виробити чіткі підходи до захисту ІС від несанкціонованого доступу, які ґрунтуються на Zero Trust підходах, мінімізації привілеїв та постійному моніторингу.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ НА ОСНОВІ FUDO SECURITY

3.1. Розгортання та налаштування Fudo One для захисту привілейованих користувачів

Для демонстрації пропонується використовувати безкоштовний варіант PAM від Fudo Security, а саме рішення Fudo One. Дане рішення доступне, як віртуальна машина (образ у форматі OVA/OVF) для швидкого розгортання. Компанія Fudo Security надає Fudo One у моделі freemium – з безкоштовною ліцензією на обмежену кількість об’єктів (до 3 активних користувачів та 3 об’єктів інформаційної інфраструктури), що зручно для малих організацій або тестування, як у даному випадку [18].

З метою моделювання компонентів інформаційної інфраструктури організації необхідно розгорнути тестові ІС, зокрема:

- Сервер Fudo One – віртуальна машина з встановленим рішенням Fudo One для контролю сесій привілейованих користувачів. Ресурси віртуальної машини: 4 віртуальні ядра процесора, 8 ГБ оперативної пам’яті, 50 ГБ диску.
- Цільовий сервер – сервер під керуванням ОС Linux з увімкненим SSH-доступом. На якому наявний привілейований обліковий запис – root.
- Адміністративна робоча станція – робоча станція адміністратора під керування ОС Kali Linux, з якого здійснюється SSH-доступ до цільового сервера.

Мережева схема представлена на рис. 2.7. Компоненти інформаційної інфраструктури розгорнуто в рамках однієї віртуальної мережі з використанням функціональних можливостей гіпервізора Oracle VirtualBox. Fudo One виконує роль проксі-сервера для сесій привілейованих користувачів.

Процедура розгортання Fudo One у VirtualBox подібна до розгортання інших віртуальних машин. Після встановлення OVA-файлу його необхідно обрати у

діалоговому вікні VirtualBox. Після запуску віртуальної машини пропонується обрати регіон (рис. 3.1.).

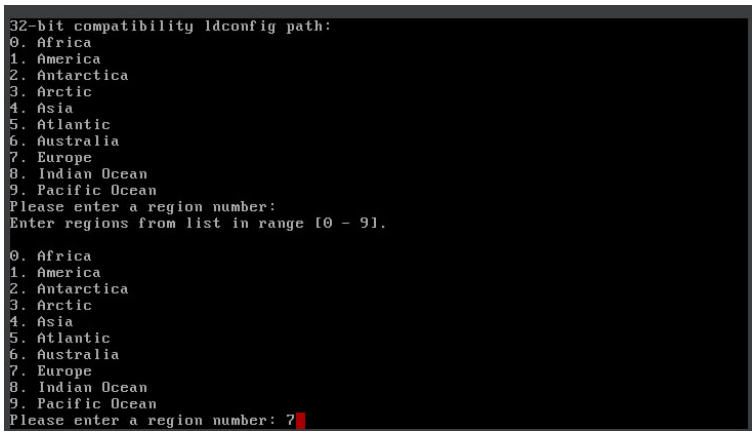

Рис. 3.1. Перелік регіонів для вибору

Після вибору регіону та країни необхідно присвоїти унікальний ідентифікатор у мережі (рис. 3.2), який буде використовуватися адміністратором у веб-браузері, щоб отримати доступ до веб-інтерфейсу адміністративної панелі для здійснення подальших налаштувань.

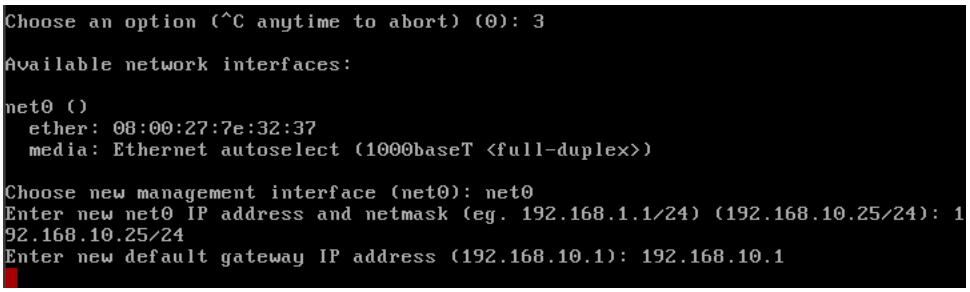

Рис. 3.2. Присвоєння унікальної IP-адреси

У разі успішного конфігурування віртуальної при введенні IP-адреси, вказаної в попередньому кроці, в адресний рядок веб-браузера – адміністратор отримує доступ до панелі Fudo One. Увійшовши, використовуючи облікові дані адміністратора за замовчуванням потрібно перейти до налаштувань, зокрема конфігурування мережі та перевірити IP-адресу шлюзу доступу, встановлену під час розгортання. На рисунку нижче продемонстровано присвоєння IP-адреси

шлюзу доступу, за допомогою якого привілейовані користувачі будуть отримувати доступ до цільових серверів.

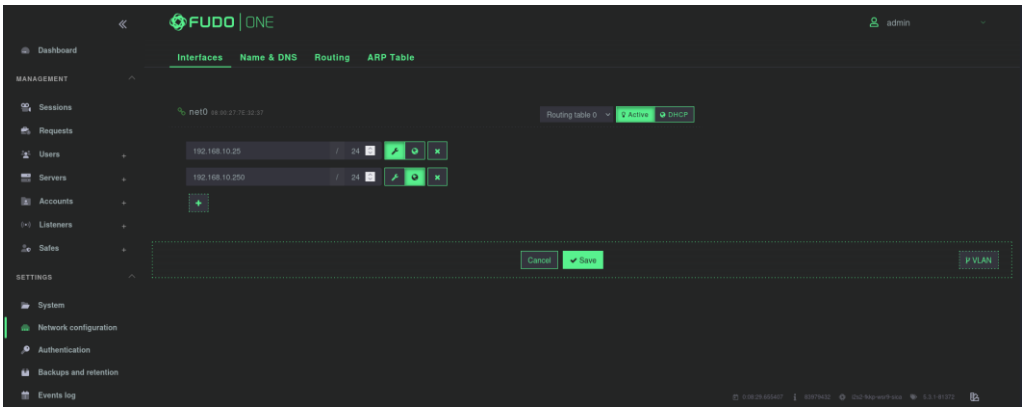

Рис. 3.3. Присвоєння унікальної IP-адреси шлюзу доступу

Наступним кроком потрібно створити сутність цільового серверу, до якого будуть підключати привілейовані користувачі. Як уже зазначалося, це буде сервер під керування ОС Linux, який знаходиться у цій самій мережі та має адресу 192.168.10.11/24. Підключення привілейованих користувачів буде обмежене по SSH не напряму до сервера, а до вузла Fudo One, який перенаправляє з’єднання на цільовий сервер, здійснюючи моніторинг та запис сеансу. Така архітектура відповідає режиму проксі, при якому всі привілейовані доступи йдуть через єдину точку контролю.

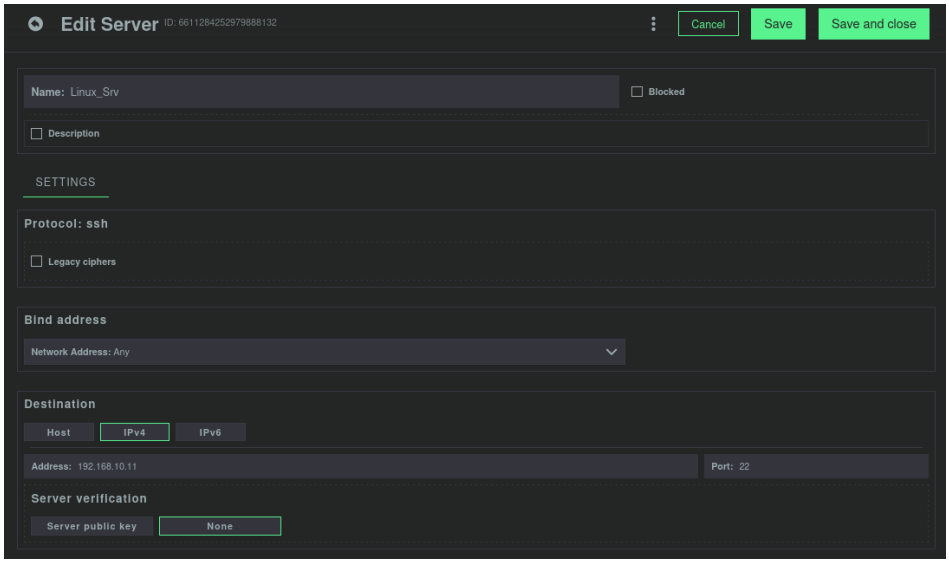

Рис. 3.4. Створення сутності цільового серверу на Fudo One

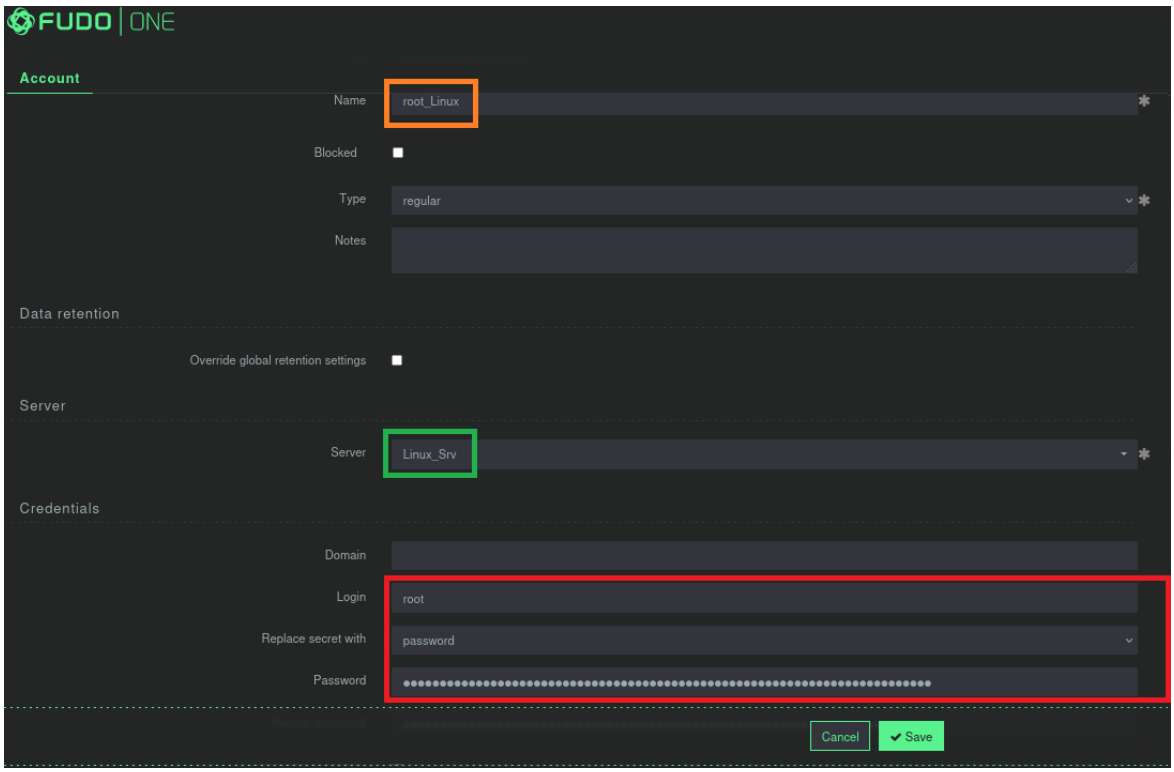

Рис. 3.5. Створення облікового запису на шлюзі доступу для цільового серверу

На рисунку вище зображено процедуру створення облікового запису в Fudo One, який буде використаний для ініціювання сесії з використанням шлюзу доступу. Для кращої деталізації окремі аспекти виділені кольорами:

- Помаранчевим кольором – назву облікового запису в самому Fudo One для підключення до сесії;
- Зеленим кольором – обраний цільовий сервер, який створений у попередніх етапах (рис. 3.4);
- Червоним кольором – облікові дані користувача, який створений безпосередньо на цільовому Linux сервері.

Далі потрібно обрати слухач – об’єкт, який відповідає за мережевий порт, на якому Fudo One очікуватиме підключення для певного протоколу. У Fudo One можна створювати слухачі для протоколів SSH, RDP або VNC. За замовчуванням після встановлення PAM-сервер має активний слухача SSH (рис. 3.6). У нашому випадку він і буде використовуватися на інтерфейсі шлюзу доступу. Після цього PAM-сервер починає приймати SSH-з’єднання на свою адресу 192.168.10.25:22 (шлюзову).

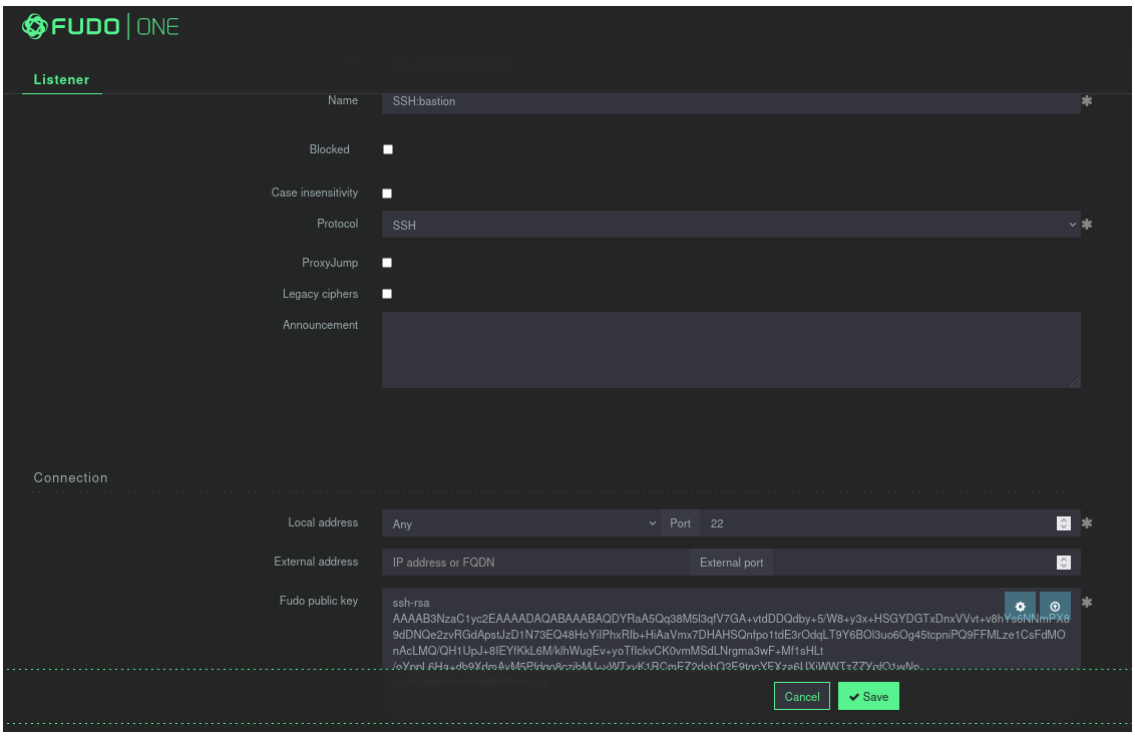

Рис. 3.6. Перегляд налаштувань слухача

Користувач – сутність, яка представляє адміністратора (людину, якій надано привілейований доступ). Створено користувача Adm. Для нього налаштовано парольний метод автентифікації (рис. 3.7).

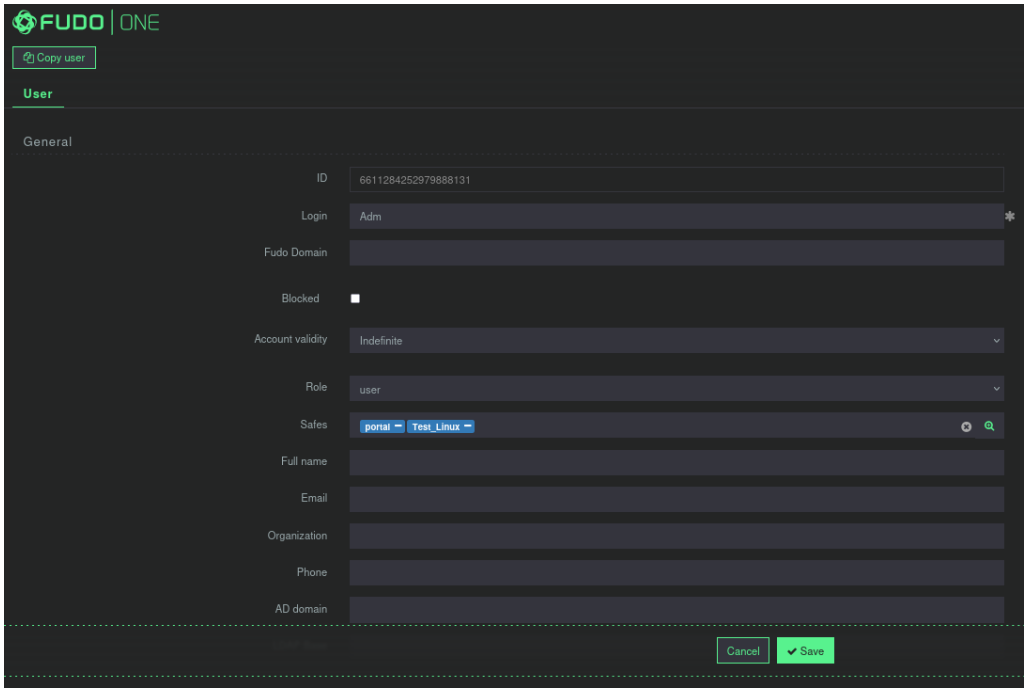

Рис. 3.7. Створення користувача Adm

Фінальним компонентом є «сейф» – логічна група, яка об’єднує облікові записи та користувачів, і визначає політику доступу. Створено сейф Test_Linux, до якого призначено створені Account root_Linux та User Adm. Фактично, це означає, що користувачу Adm дозволено доступ до облікового запису root на сервері Linux_Srv. Також для сейфу увімкнено опцію Access request required votes – вимога запиту доступу із зазначенням кількості голосуючих адміністраторів. Ми встановили, що потрібен 1 голос адміністратора для підтвердження запиту на доступ (тобто достатньо одноосібного дозволу від будь-якого адміністратора PAM-системи).

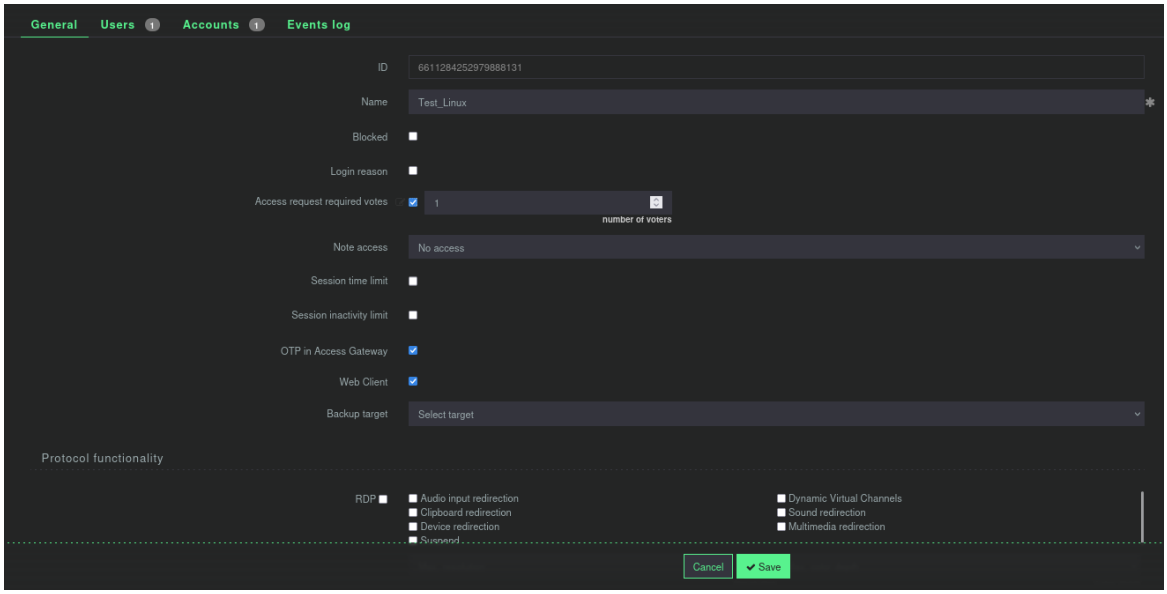

Рис. 3.8. Компонування створених об’єктів у сейф

Завершивши налаштування цих об’єктів, отримуємо наступну картину: адміністратор Adm зареєстрований у Fudo One та прив’язаний до акаунту root сервера Linux_Srv через сейф Test_Linux. Будь-яка спроба Adm підключитися до Linux_Srv тепер повинна проходити через Fudo One, і причому тільки за умови схвалення запиту доступу (вимога політики JIT). У наступному підрозділі пропонується до розгляду, як саме відбувається цей процес на практиці, та які можливості контролю надає Fudo One.

3.2. Результати експерименту захисту привілейованих користувачів за допомогою Fudo One

У цьому прикладі демонструється, як Fudo One захищає SSH-доступ привілейованого користувача до критично важливого цільового сервера. Розглянемо ситуацію, коли системний адміністратор потребує підключитися до сервера по протоколу SSH для виконання регламентних робіт. Без використання системи класу PAM це означало б вхід безпосередньо під обліковим записом root, що несе потенційні ризики ІБ (можливої компрометації паролю, відсутності контролю дій привілейованого користувача, неможливість аудиту тощо). Впровадження Fudo One змінює порядок доступу, оскільки тепер кожен привілейований сеанс вимагає явного підтвердження і повністю протоколюється для подальшого аналізу. На рис. 3.9 схематично зображено послідовність дій при встановленні захищеного сеансу SSH адміністратором через Fudo One (режим JIT):

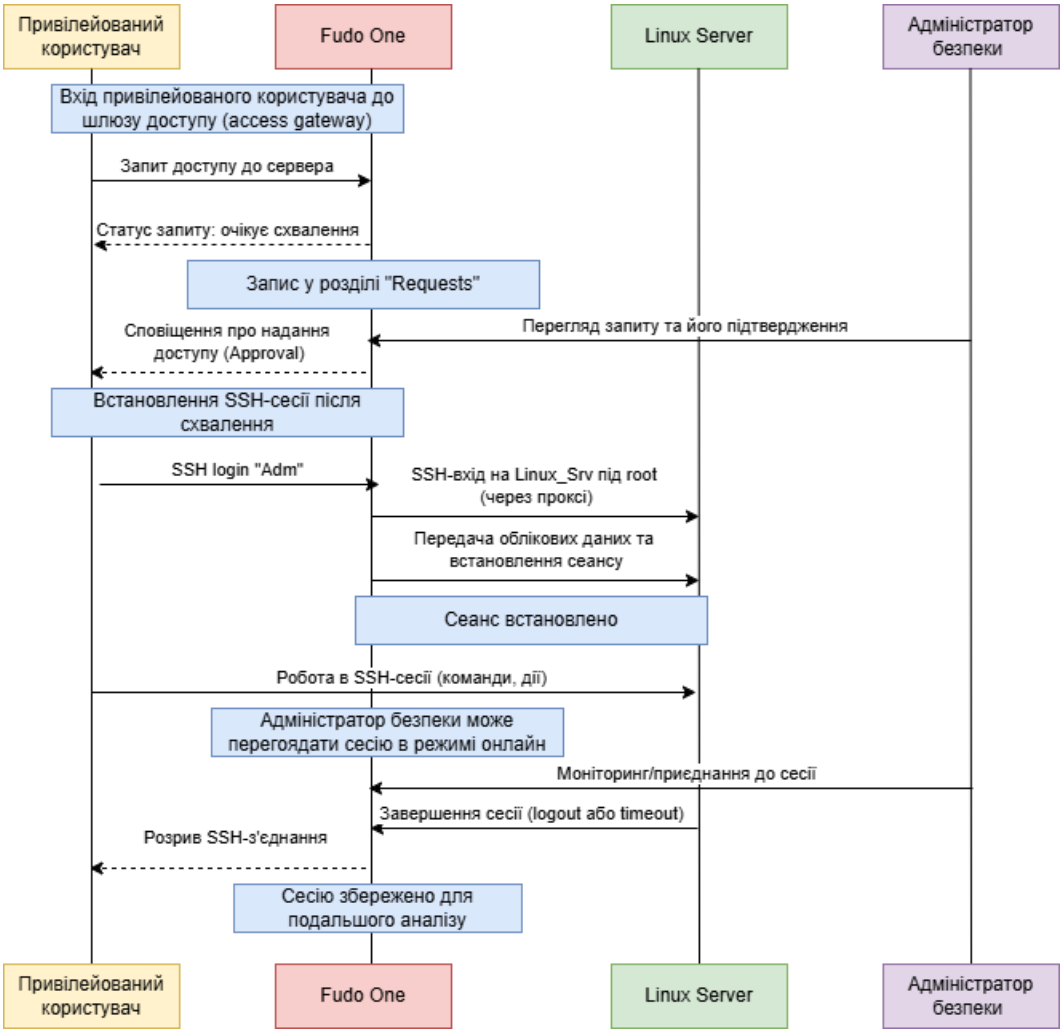

Рис. 3.9. Послідовність дій при встановленні SSH-сесії

Як видно з діаграми, процес складається з двох основних фаз: запит доступу (до встановлення сеансу) та моніторинг сеансу (під час роботи адміністратора на сервері):

Запит доступу (Access Request). Привілейований користувач Adm спочатку авторизується в системі Fudo One (через шлюз доступу). Дана процедура можлива двома способами: через веб-інтерфейс або безпосередньо через SSH. У даному прикладі використано веб-портал (рис. 3.10), де привілейований користувач заходить на веб-сторінку шлюзу (https://192.168.10.250) під своїми обліковими даними (логін Adm + пароль).

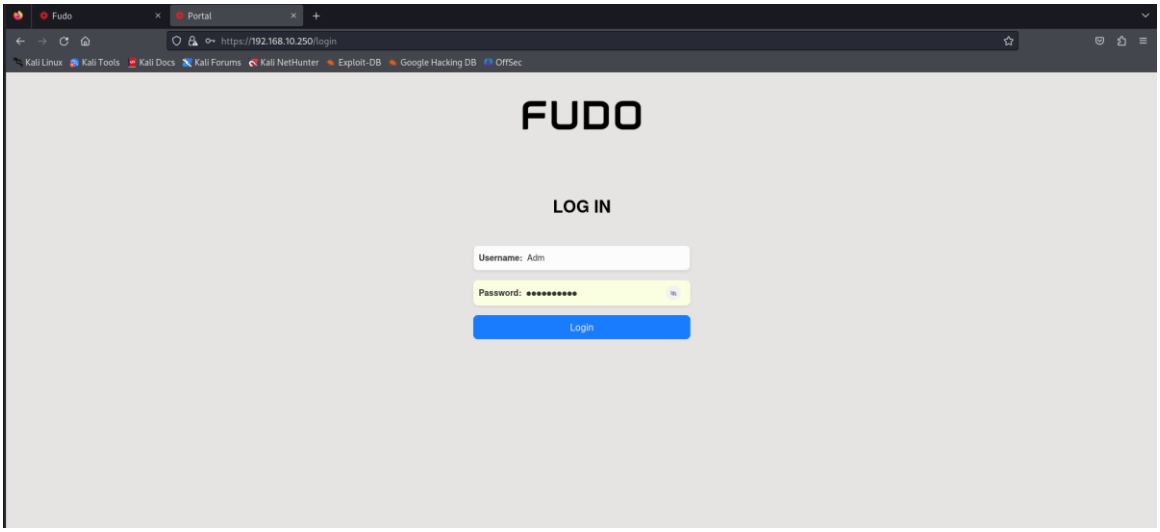

Рис. 3.10. Інтерфейс шлюзу доступу

На порталі привілейований користувач бачить перелік доступних йому ресурсів (в даному випадку сервер Linux_Srv). Тому він ініціює запит на доступ до цього сервера, вказавши бажаний час початку та тривалість сеансу. За політикою JIT, доступ можна запросити негайно або на запланований час. У цьому випадку обрано негайний доступ тривалістю 1 година (рис. 3.11).

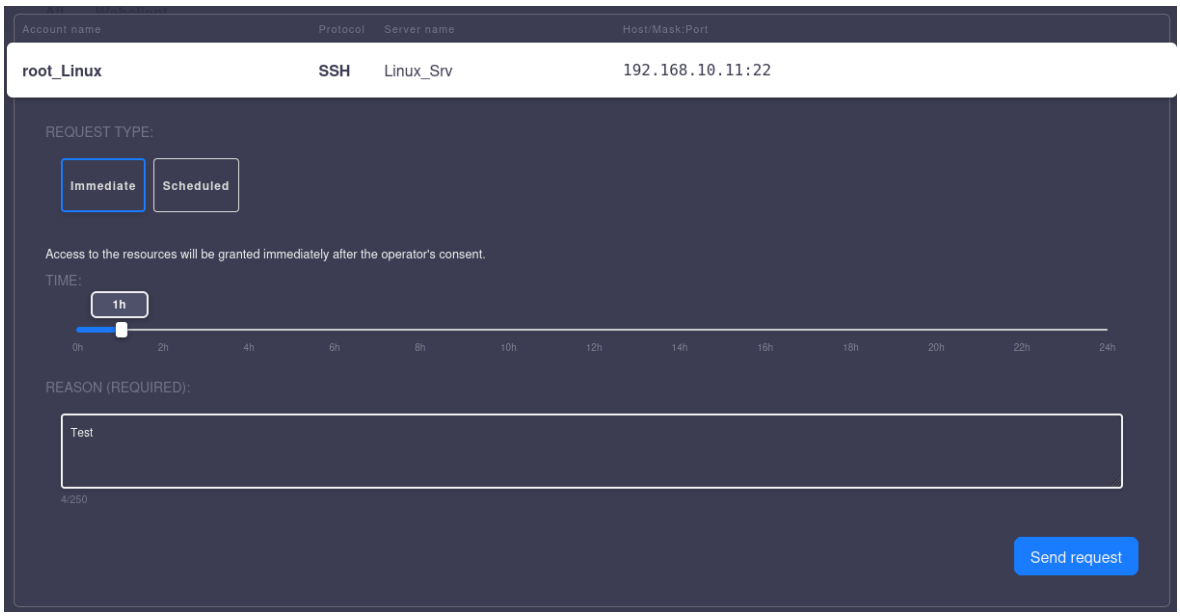

Рис. 3.11. Діалогове вікно встановлення часового проміжку для отримання доступу

Зроблений запит потрапляє до PAM-сервера Fudo і відображається у розділі «Management» → «Requests» панелі адміністрування («Admin Panel»). Статус запиту – «Awaiting» (очікує рішення). Всі адміністратори PAM із роллю «Admin» отримують можливість проголосувати за нього (рис. 3.12). Відповідно до попередньо встановлених налаштувань потрібен один голос, тому будь-який адміністратор безпеки PAM може схвалити або відхилити запит. Припустимо, адміністратор безпеки отримує сповіщення (через електронну пошту або в самій адміністративній консолі) і заходить у розділ «Requests». Там він бачить запит від Adm на сервер Linux_Srv з зазначеною тривалістю доступу. Для прийняття рішення адміністратор безпеки відкриває запит і натискає «Accept», додавши за потреби коментар (причина надання доступу). Статус запиту змінюється на «Accepted», а привілейованому користувачу Adm на порталі шлюзу доступу відображається, що доступ надано.

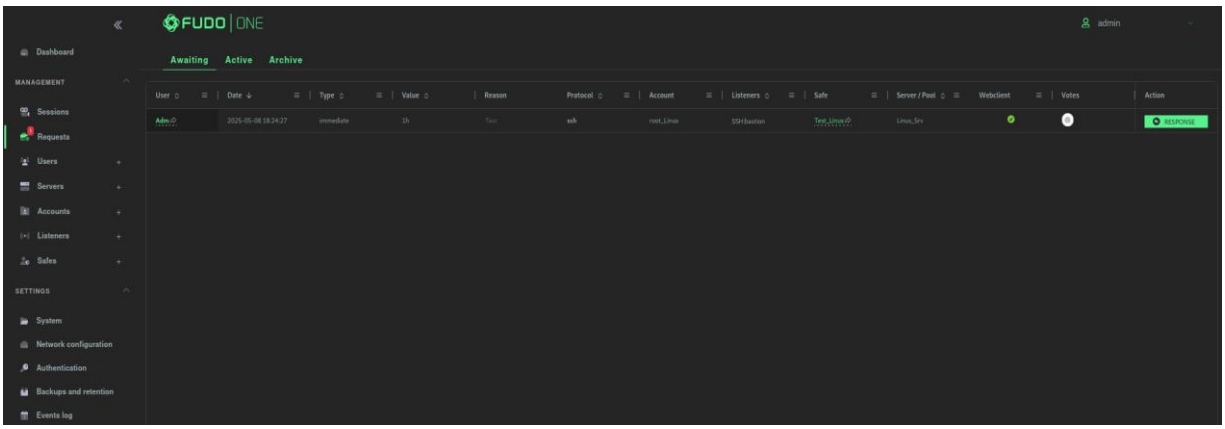

Рис. 3.12. Отримання запиту на схвалення доступу

Примітка: якби адміністратор безпеки відхилив запит («Reject»), привілейований користувач отримав би відмову в доступі. Система вимагає вказати причину відмови, щоб забезпечити прозорість. У разі необхідності схвалення декількома адміністраторами безпеки, якщо хоча б один проголосує проти, запит автоматично відхиляється.

Після схвалення запиту привілейований користувач Adm має тимчасове вікно (до 24 годин), щоб розпочати сесію. Підключення здійснюються через товстий клієнт SSH (наприклад, з терміналу) з використанням IP-адреси Fudo One, а не напряму до сервера або. Інший спосіб підключення через веб-клієнт у браузері (рис. 3.13).

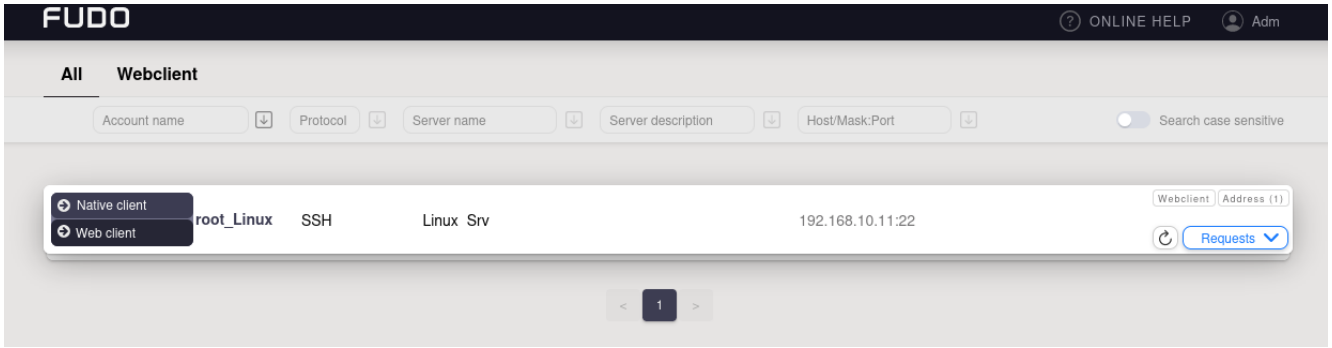

Рис. 3.13. Варіанти підключення до цільового серверу

Після вибору клієнта Fudo One ініціює внутрішнє SSH-з’єднання до цільового сервера Linux_Srv. Він виступає проксі: від імені користувача Adm відкриває сесію для root@Linux_Srv. Цільовий сервер не запитує в привілейованого

користувача автентифікацію (пароль або ключ), оскільки в налаштуваннях Fudo One для облікового запису root_Linux було збережено пароль, тому PAM автоматично передає його (рис. 3.5).

Тепер Adm працює у консолі сервера Linux_Srv, але вся його взаємодія проходить через PAM-сервер (рис. 3.14). Fudo One починає записувати сесію в режимі реального часу. Для SSH-протоколу фіксуються всі процедури вводу-виводу текстового терміналу, а також метадані (час команд, використаний трафік, тривалість сеансу тощо). Привілейований користувач Adm продовжує виконувати свою роботу (наприклад, переглядати конфігурації, змінювати налаштування на сервері).

З точки зору сервера, сесія ініційована від Fudo One (оскільки саме він підключений як клієнт). Таким чином, без доступу до PAM неможливо обійти моніторинг – навіть якщо привілейований користувач мав би прямий доступ до цільового серверу, облікові дані root йому не відомі поза межами PAM-системи. Усі дії привілейованого користувача прозорі для адміністраторів безпеки (контролюючих осіб).

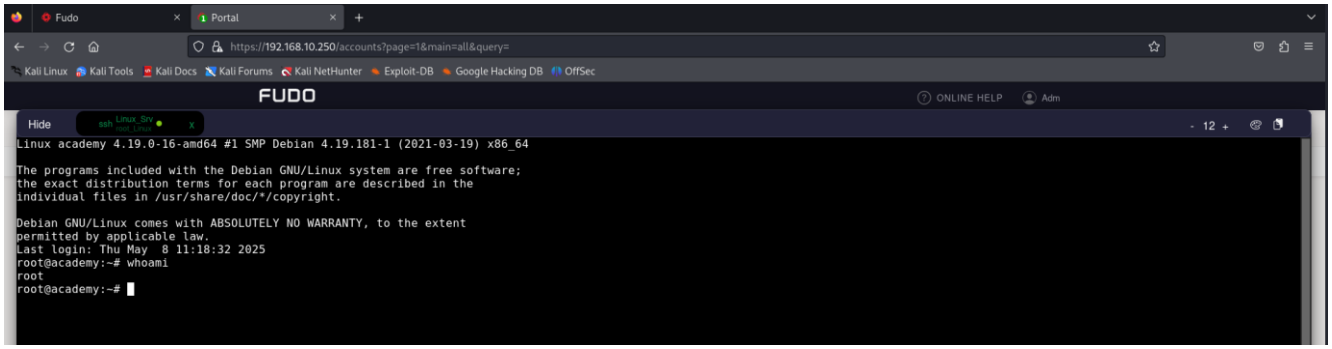

Рис. 3.14. Сесія успішно встановлена та контрольована

Після встановлення сесії адміністратор безпеки має можливість відслідковувати у реальному часу діяльність привілейованого користувача. В адміністративній консолі Fudo One у розділі «Sessions» з’являється запис про активну сесію користувача Adm (вказано, хто, куди і під яким логіном

підключений). Натиснувши на відповідну сесію, адміністратор PAM може вибрати опції (рис. 3.15):

Приєднатися до сесії – відкрити сеанс поточної сесії привілейованого користувача та мати можливість також вводити команди. Простий перегляд сесії в реальному часі дозволяє забезпечити принцип «чотирьох очей».

Призупинити або завершити сесію – примусово зупинити сеанс у разі виявлення несанкціонованих дій. Fudo One дозволяє поставити на паузу сеанс або повністю його розірвати, причому з можливістю заблокувати обліковий запис користувача.

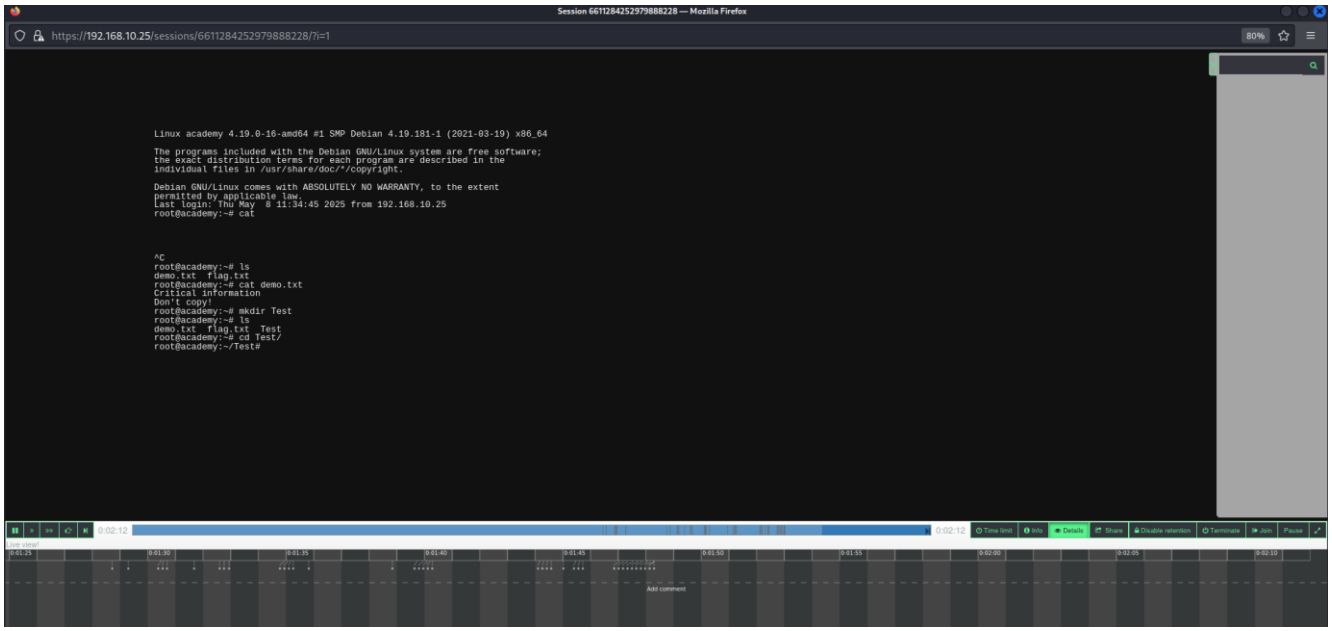

Рис. 3.15. Перегляд сесії в реальному режимі адміністратором безпеки

Враховуючи викладене вище, можна зробити висновок, що протягом всього часу сеанс був під повним наглядом. Fudo One автоматично контролював і інші параметри: ліміт часу сеансу (за запитом був 1 година – PAM відраховує цей час) та ліміт неактивності (якщо б користувач не проявляв активності визначений період, з'єднання могло б бути закрито автоматично, дані опції доступні в налаштуваннях політик сеансу).

Після того як привілейований користувач виконав необхідні роботи, він виходить із сервера (logout). SSH-сесія завершується, і Fudo One фіксує час

завершення. Якщо користувач не вийде сам, то після спливання запитаного часу доступу PAM автоматично розірве з'єднання. В обох випадках результати сесії зберігаються:

- Fudo One зберігає сесію у вигляді відео-запису терміналу. Дані запису компактні: 1 година SSH-сеансу займає близько 30 МБ сховища (для порівняння, година RDP приблизно займає 300 МБ). Запис зберігається у внутрішній базі PAM.
- Метадані сесії. Збережені такі дані, як: хто (користувач Adm), під яким обліковим записом на сервері (root), куди (сервер Linux_Srv), коли (час початку/завершення), тривалість, обсяг переданих даних, IP-адреса клієнта тощо (рис. 3.16).

Рис. 3.16. Перелік збережених сесій, які можна в подальшому аналізувати

Слід зауважити, що продемонстровані функції – саме ті, що входять до Fudo One. Вони охоплюють всі основні потреби контролю привілейованих користувачів, зокрема управління обліковими записами й користувачами, JIT-доступ (механізм запитів доступу), моніторинг та запис сесій (SSH, RDP, VNC тощо), онлайн відслідковування сесії та її примусове переривання. В більш розширеній версії Fudo Enterprise доступні додаткові можливості, які у Fudo One або відсутні, або обмежені. Зокрема, Enterprise-версія підтримує ширший перелік протоколів (HTTP(S), бази даних – MySQL, MSSQL/TDS, Telnet 3270/5250 тощо), вбудоване сховище паролів (Secret Manager) з ротацією паролів, аналіз на основі ШІ (AI-powered Breach Prevention) для виявлення аномалій, розширені мережеві конфігурації (кластери, балансування, резервування) тощо.

Далі пропонується розглянути ситуацію, коли привілейований користувач здійснює шкідливі дії, які призводять до інцидентів ІБ. Під час сесії користувач з

обліковим записом root@academy виконав команду перегляду вмісту файлу demo.txt, у якому містилась чутлива інформація. Далі було зафіксовано спробу передачі системного файлу /etc/passwd на зовнішній хост з IP-адресою 192.168.10.7 за допомогою утиліти scp. Передача пройшла успішно, що підтверджується повідомленням про завершення копіювання файлу зі швидкістю (рис. 3.17).

Продемонстроване свідчить про порушення політики ІБ, зокрема, щодо обмеження несанкціонованої передачі чутливих даних. Сеанс було збережено в архіві Fudo One для подальшого аудиту та аналізу. Результати інциденту ІБ використовуються як приклад для вдосконалення правил доступу та налаштувань сейфів у PAM-системі.

Рис. 3.17. Привілейований користувач копіює чутливий файл

Знімок екрана, який продемонстрований на рисунку 3.18 підтверджує успішне копіювання системного файлу /etc/passwd на зовнішній хост з IP-адресою 192.168.10.7.

На рисунку показано, що користувач, перебуваючи у директорії /tmp на машині під управлінням Kali Linux, виявив наявність файлу passwd, який раніше було передано через SCP. Команда head passwd демонструє вміст початкових рядків системного файлу, зокрема облікові записи root, daemon, bin тощо. Це свідчить про порушення конфіденційності даних, які були передані з привілейованого сервера на сторонній пристрій під керуванням Kali Linux. Інцидент ІБ є наочним прикладом наслідків недостатньої жорсткості політик PAM-системи і демонструє необхідність застосування обмежень на передачу файлів у привілейованих сесіях.

Рис. 3.18. Чутливий файл успішно передано на сторонній хост

З метою аналізу інциденту ІБ адміністратор безпеки виконав пошук за ключовим словом scp, щоб ідентифікувати сесії, у яких використовувалась команда передачі файлів. Результатом є знайдений SSH-сеанс користувача Adm, підключеного до хосту з IP-адресою 192.168.10.11:22 під обліковим записом root_Linux, що належить до сейфу Test_Linux (рис. 3.19).

Пошук дозволив оперативно виявити підозрілу сесію тривалістю 7 хвилин 25 секунд, у якій фіксувався високий рівень активності, а саме 81%. Функціонал повнотекстового пошуку у Fudo One є достатнім засобом для виявлення порушень політик доступу та подальшого аудиту діяльності привілейованих користувачів.

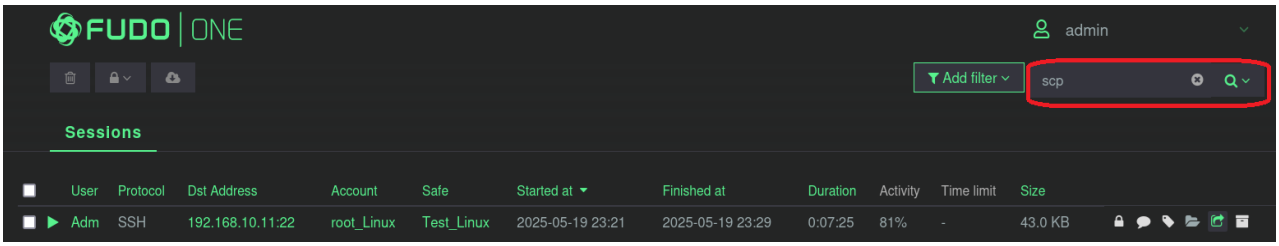

Рис. 3.19. Пошук у Fudo One за допомогою ключової фрази (команди)

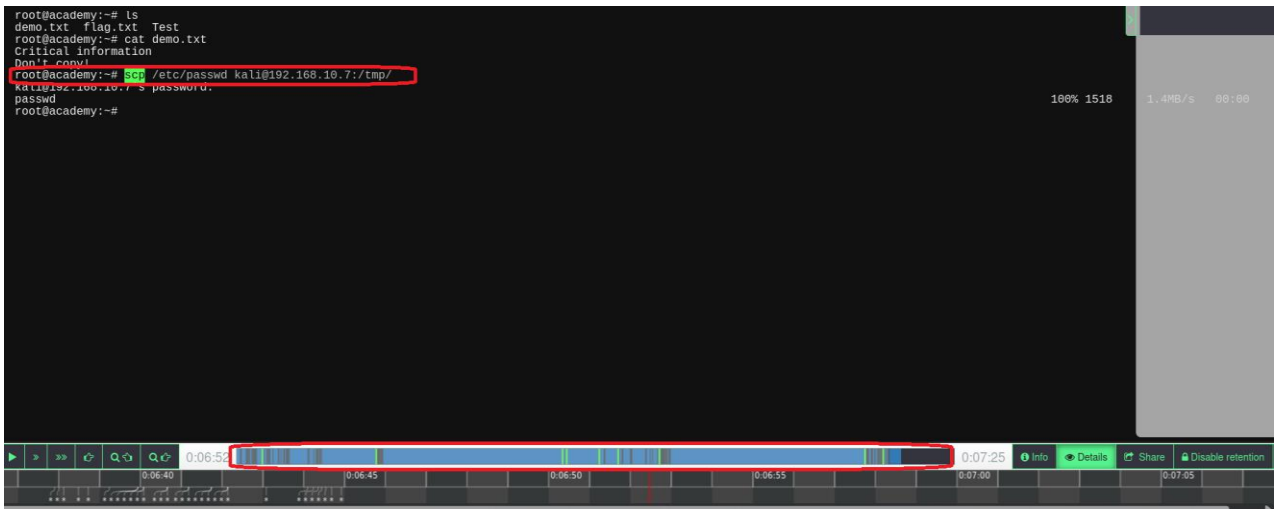

Рис. 3.20. Виявлення скоєного порушення

У режимі перегляду адміністратор безпеки ідентифікував момент виконання команди: scp /etc/passwd kali@192.168.10.7:/tmp/, яка свідчить про спробу передати або завершену передачу файлу з чутливими даними на зовнішній хост. На нижній панелі таймлайну відображено високу активність користувача у відповідному часовому сегменті сесії (6:45 – 7:05), що дозволяє швидко перейти до потрібного моменту.

Такий механізм аудиту у Fudo One забезпечує оперативний аналіз привілейованих дій, дозволяючи виявляти потенційно небезпечну поведінку в інтерактивному інтерфейсі, переглядати ключові команди, а також супроводжувати інцидент службовими коментарями та тегами.

Контекст даного експерименту-демонстрації зосереджений лише на функціях Fudo One, оскільки їх цілком достатньо для потреб невеликої організації.

У підсумку, практичний експеримент продемонстрував, що впровадження Fudo One дозволяє суттєво підвищити контроль над привілейованими сесіями. Всі дії привілейованого користувача відслідковуються та, деякі, потребують підтвердження від адміністратора безпеки. Разом з тим, кожна дія фіксується в журналі аудиту подій. Такий функціонал зменшує ризик зловживань та спрощує розслідування інцидентів ІБ.

3.3. Рекомендації щодо застосування технології захисту привілейованих користувачів на основі Fudo PAM

На основі проведеного експерименту та тестування Fudo One сформульовано низку рекомендацій, дотримання яких дозволить максимально якісно реалізувати механізми контролю привілейованих користувачів та захистити ІС організації від несанкціонованого доступу. Рекомендації поділено на дві частини: кращі практики розгортання і експлуатації та типові ризики/помилки та способи їх уникнення.

Рекомендації з розгортання та використання Fudo One.

Перед впровадження системи класу PAM необхідно попередньо оцінити навантаження на інформаційні інфраструктуру, зокрема заплановану кількість одночасних сесій та, які протоколи будуть використовуватися (SSH, RDP тощо), орієнтовний обсяг записів. Також варто забезпечити достатньо швидкий диск (понад 1000 IOPS) для запису сесій, особливо якщо плануються відеопотоки RDP. Обсяг дискового простору необхідно планувати з урахуванням оцінки приблизно 300 МБ на годину RDP та приблизно 30 МБ на годину SSH-запис плюс резерв на журнали [19].

Рекомендується розгортати Fudo One у такій мережевій зоні, через яку проходитимуть усі привілейовані з’єднання. Оптимальним варіантом є виділений сегмент з контрольованою маршрутизацією, у якому доступ до цільових серверів дозволено виключно з боку PAM-сервера, а підключення привілейованих користувачів здійснюється лише до самого PAM. Таким чином, пряме SSH чи RDP підключення з робочих станцій до серверів блокується міжмережевим екраном, який гарантує неможливість обходу механізмів контролю доступу.

Як зазначалося у попередніх розділах PAM-система підтримує декілька способів впровадження. Рекомендованими способами до впровадження є проксі та бастіон. Альтернативні варіанти, зокрема прозорий режим, можуть вимагати додаткових технічних підходів, таких як конфігурація SPAN-портів або ARP-переадресації, тому їх доцільно розглядати лише за наявності відповідного досвіду та потреби.

Після розгортання PAM обов’язково необхідно змінити стандартні облікові дані (обліковий запис admin). Налаштувати двофакторну автентифікацію для доступу адміністраторів до адміністративної консолі – Fudo One підтримує TOTP (Google Authenticator) або інтеграцію з зовнішніми системами (RADIUS, Duo, SMS, сертифікати тощо). Також варто подбати про розмежування ролей, визначити облікові записи, які можуть лише моніторити сесії, і окремі, які керують налаштуваннями. Такий підхід суттєво зменшить можливість зловживань. Разом з цим, рекомендується регулярно встановлювати оновлення від виробника, які виправляються як помилки, так і потенційні вразливості.

Для зручності управління варто інтегрувати PAM-систему з корпоративним LDAP/Active Directory, якщо така система наявна в інформаційній інфраструктурі. Fudo дозволяє імпортувати користувачів і групи з AD та здійснювати синхронізацію, яка полегшить призначення привілейованих користувачів у PAM (наприклад, група «Адміністратори серверів» може автоматично мати акаунти у Fudo). Водночас, не всіх користувачів з AD слід робити користувачами PAM – необхідно дотримуватися принципу найменших привілеїв, тобто надавати доступ до критичних ІС тільки тим особам, які його реально потребують.

На основі ризик-орієнтованого підходу рекомендованого визначити, для яких інформаційних систем необхідне явне підтвердження доступу. Рекомендується застосовувати JIT для всіх привілейованих облікових записів на критично важливих ІС. Наприклад, доступ до продуктивних БД, фінансових ІС тощо повинен надаватися тільки за запитом із схваленням відповідальною особою. Використання JIT скорочує вікно можливостей для зловмисника у разі компрометації облікових даних, адже навіть знаючи пароль, без явного підтвердження від відповідальної особи – він не отримає доступ. Для менш критичних ІС можна налаштувати автоматичний доступ без запиту, але все одно з повним записом – залежно від визначеної політики ІБ організації. Важливо також визначити осіб, які схвалюватимуть запити. За замовчуванням це адміністратори PAM-системи, але слід призначити конкретних відповідальних осіб за кожен сейф/набір інформаційних ресурсів.

В рамках процесу контролю привілейованих користувачів організація повинна призначити відповідальних осіб, які будуть здійснювати моніторинг та відслідковуватимуть активні сесії, зазвичай це фахівці підрозділу ІБ (так звані адміністратори безпеки). Fudo One дозволяє відкрити сторінку моніторингу, де відображаються всі поточні привілейовані підключення. В ідеалі, фахівці підрозділу ІБ або інші відповідальні особи мають переглядати командний журнал у реальному часі для ключових сесій. Така діяльність дасть змогу миттєво виявити аномалії та негайно припинити сеанс, якщо помічено підозрілу дію. В попередньому підрозділі було продемонстровано, що при перегляді сесії адміністратор може завершити сесію привілейованого користувача (рис. 3.15).

У разі ж неможливості реалізувати перегляд сесій у реальному часі варто впровадити процес періодичного перегляду записаних сесій (наприклад, раз на тиждень). Особливо тих, які стосуються критичних ІС. Аналіз сесій дозволяє виявити порушення політик безпеки, зокрема використання команд, які не мали б виконуватися. Fudo One спрощує цей процес завдяки пошуку по ключових словах, тому можна зосередитися на пошуку спроб змінити конфігурацію без дозволу, запуску небезпечних утиліт тощо.

Також обов’язково перед впровадженням системи класу PAM необхідно провести навчання, як для привілейованих користувачів, чиї сесії будуть контролюватися, так і адміністраторам безпеки, які будуть підтримувати PAM-систему. Привілейованим користувачам варто пояснити новий порядок доступу (через Fudo One), навчити створювати запити на доступ та використовувати другий фактор автентифікації (у разі його наявності та налаштування).

Впровадження PAM має бути підкріплене внутрішніми розпорядчими документами, які регламентуватимуть процес надання контрольованого привілейованого доступу. Необхідно розробити, затвердити та впровадити політику привілейованого доступу, яка описує підходи щодо контролю привілейованих користувачів. Варто зауважити, що розробка внутрішньої розпорядчої документації дозволяє уніфікувати процеси ІБ та забезпечити чітке визначення ролей, відповідальності й порядку взаємодії між учасниками процесу.

Можливі ризики, проблеми та помилки при роботі з PAM і як їх уникнути.

PAM-сервер стає єдиною точкою входу до критичних ІС, що робить його єдиною точкою відмови. Тобто, якщо система класу PAM вийде з ладу, привілейовані користувачі можуть втратити доступ до цільових серверів. Щоб знизити даний ризик – потрібно передбачити резервний сценарій, зокрема, окремий аварійний обліковий запис на критичних ІС, який зберігається в опечатаному конверті і може бути використаний, якщо PAM-система недоступна. Такий підхід прийнято називати «Break Glass» (укр. «Розбити Скло»). Розбити скло – спосіб обійти систему безпеки, яка зазвичай захищає ІС або послугу. Сам термін означає, що хтось розбиває скляну пробку, щоб увімкнути пожежну сигналізацію. У деяких ситуаціях користувач може бути не в змозі отримати санкціонований доступ у звичайний спосіб [20]. Резервні облікові записи повинні мати унікальні складні паролі та використовуватися лише в надзвичайних ситуаціях. В довгостроковій перспективі – рекомендується розглянути розгортання резервного PAM-сервера або перейти на кластер (доступно в Enterprise версії).

Однією з типових помилок при впровадженні PAM є залишити «шпарину», коли привілейований користувач все ще має прямий доступ без підключення через PAM-систему. Наприклад, користувачу лишають прямий VPN-канал до сервера. Необхідно унеможливити обходи PAM, а саме закрити всі альтернативні шляхи підключення, відкликати старі паролі (після впровадження PAM змінити всі паролі, щоб ними володіла тільки PAM-система), відстежувати появу нових облікових записів поза PAM. Для цього добре налаштувати регулярний аудит – Fudo Enterprise, наприклад, має Auto-Discovery облікових записів, але у випадку Fudo One цю перевірку треба робити вручну.

Також, поширеною помилкою є впровадження PAM, але не використання даних, які він збирає. Якщо організація не переглядає журнали і записи, ефективність контролю падає. Зловмисник, знаючи що ніхто не здійснює моніторинг, може все одно нашкодити, хоч і під наглядом – але якщо запис ніхто не переглядатиме, це не завадить інциденту ІБ. Отже, слід виділити ресурси на аналіз журналів подій і відео-записів. Як вже зазначалося, необхідно призначити

відповідальних осіб за вибірковий перегляд записів раз на тиждень. Також варто налаштуйте автоматичні сповіщення: Fudo One може відправляти сповіщення при певних подіях (наприклад, початок сесії, відхилений запит тощо – через email або Syslog).

Підсумовуючи, варто зауважити, що слідування наведеним рекомендаціям дозволить збільшити ефективність впровадження рішення Fudo One в інформаційній інфраструктурі. Як показує досвід організацій, правильне впровадження та використання PAM суттєво підвищує загальний рівень ІБ, особливо в умовах воєнного стану, оскільки загроза інсайдерських атак лише збільшується. Впровадження PAM-системи дозволяє зменшити поверхню атаки шляхом мінімізації постійних привілеїв та сприяє відповідності вимогам міжнародних стандартів ІБ та локальних регуляторних вимог. Водночас, слід пам’ятати, що технологія PAM не є панацеєю – її ефективність залежить від зрілості процесів в організації та підтримки керівництва. Рекомендації вище спрямовані на те, щоб максимально інтегрувати PAM у існуючу систему управління доступом та отримати від нього повну користь.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було здійснено комплексне дослідження проблеми захисту привілейованих облікових записів в ІС організацій. Актуальність цієї проблематики зумовлена тим, що саме привілейовані користувачі мають доступ до чутливих ресурсів, а їх компрометація може спричинити серйозні наслідки, зокрема, витік конфіденційної інформації, порушення цілісності даних, втрату керованості інформаційною системою або повне блокування її функціонування.

У процесі дослідження було проаналізовано сучасні технології управління привілейованим доступом, а також здійснено практичне розгортання та налаштування рішення Fudo One, як прикладу інструменту контролю дій привілейованих користувачів. Особливу увагу приділено демонстрації ключових функціональних можливостей цього продукту, зокрема проксі-доступу до серверів, запису та моніторингу сесій, схеми підключень, а також аудиту дій користувачів. Всі демонстрації реалізовано у тестовому середовищі, змодельованому на базі трьох віртуальних машин, що дозволило в повному обсязі проілюструвати можливості Fudo One в реальному сценарії.

На основі проведеного аналізу було розроблено практичні рекомендації щодо впровадження Fudo One в інформаційне середовище. Запропоновано оптимальну мережеву архітектуру, визначено етапи налаштування правил доступу, розглянуто принципи обліку, реєстрації та погодження сесій адміністраторів.

Результати кваліфікаційної роботи підтвердили доцільність використання Fudo One як ефективного інструменту захисту привілейованих облікових записів. Його впровадження дозволяє підвищити прозорість адміністративних дій, зменшити ризики несанкціонованого доступу, забезпечити контроль відповідності вимогам безпеки та створити умови для подальшої автоматизації процесів управління доступом у відповідності до міжнародних стандартів у сфері інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. National Institute of Standards and Technology. Privilege – Glossary. URL: https://csrc.nist.gov/glossary/term/privilege (дата звернення: 14.05.2025).

2. Securden. Cyber Attack Stats and Privileged Access Strategy Required. URL: https://www.securden.com/blog/cyber-attack-stats-and-privileged-access-strategy-required.html (дата звернення: 14.05.2025).

3. Gurucul. 2024 Insider Threat Report. URL: https://go1.gurucul.com/2024-insider-threat-report (дата звернення: 14.05.2025).

4. BeyondTrust. PAM Comparison – Gartner Magic Quadrant. URL: https://www.beyondtrust.com/blog/entry/gartner-pam-magic-quadrant (дата звернення: 14.05.2025).

5. Gartner. CyberArk Privileged Access Manager – Reviews. URL: https://www.gartner.com/reviews/market/privileged-access-management/vendor/cyberark/product/cyberark-privileged-access-manager (дата звернення: 14.05.2025).

6. Gartner. Delinea Secret Server – Reviews. URL: https://www.gartner.com/reviews/market/privileged-access-management/vendor/delinea/product/secret-server (дата звернення: 14.05.2025).

7. Gartner. Wallix PAM – Reviews. URL: https://www.gartner.com/reviews/market/privileged-access-management/vendor/wallix/product/wallix-pam (дата звернення: 14.05.2025).

8. Gartner. Fudo Enterprise – Reviews. URL: https://www.gartner.com/reviews/market/privileged-access-management/vendor/fudo-security/product/fudo-enterprise (дата звернення: 14.05.2025).

9. Scytale. Privileged Access Management and Compliance ISO 27001. URL: https://scytale.ai/resources/privileged-access-management-and-compliance-iso-27001/ (дата звернення: 14.05.2025).

10. ISO. ISO/IEC 27001 – Information Security Management. URL: https://www.iso.org/ru/standard/27001 (дата звернення: 14.05.2025).

11. NIST. Special Publication 800-53 Revision 5. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (дата звернення: 14.05.2025).

12. CIS. CIS Controls v8.1. URL: https://learn.cisecurity.org/control-download-v8-1 (дата звернення: 14.05.2025).

13. Trustpair. Is the 4-Eyes Principle the Most Effective Way to Block Fraud?. URL: https://trustpair.com/blog/is-the-4-eyes-principle-the-most-effective-way-to-block-fraud/ (дата звернення: 14.05.2025).

14. Cybersecurity Excellence Awards. Fudo Security Presents the Best PAM Solution. URL: https://cybersecurity-excellence-awards.com/candidates/fudo-security-presents-the-best-pam-solution-for-the-most-demanding-environments-fudo-enterprise/ (дата звернення: 14.05.2025).

15. Fudo Security. Fudo Documentation v5.5 – Overview. URL: https://download.fudosecurity.com/documentation/fudo/5_5/online_help/en/intro/en/overview.html (дата звернення: 14.05.2025).

16. Fudo Security. Fudo Documentation – Data Model. URL: https://download.fudosecurity.com/documentation/fudo/latest/online_help/en/intro/en/data_model.html (дата звернення: 14.05.2025).

17. Oberig IT. Fudo Privileged Access Management. URL: https://oberig-it.com/solution/fudo-privileged-access-management/ (дата звернення: 14.05.2025).

18. Fudo One. Licensing. URL: https://fudoone.readme.io/docs/fudo-one-licensing-1 (дата звернення: 14.05.2025).

19. Fudo One. System Requirements. URL: https://fudoone.readme.io/docs/requirements (дата звернення: 14.05.2025).

20. StrongDM. Break Glass in PAM. URL: https://www.strongdm.com/blog/break-glass (дата звернення: 14.05.2025).