Давидов Петро

# Порівняльний аналіз двох публікацій з теми корпоративного управління ідентичністю та безпекою облікових записів

## Вступ

Порівнюються дві наукові публікації, присвячені захисту облікових записів у корпоративному середовищі:

**«Self-Sovereign Identity-Based IAM in Enterprises»** - міжнародне дослідження, що аналізує можливості впровадження парадигми SSI (Self-Sovereign Identity) в системи управління ідентичністю та доступом (IAM) підприємств. Автори застосовують методологію Design Science Research, створюють прототип SSI-рішення та оцінюють його ефективність через експертні інтерв'ю.

**«Забезпечення безпеки облікових записів корпоративних користувачів»** - публікація Івана Ярославовича Тишика, доцента кафедри захисту інформації НУ «Львівська політехніка». Робота присвячена практичному захисту облікових записів у середовищі Windows Server та Active Directory, з акцентом на утиліти моніторингу, налаштування політик безпеки та протидію типовим атакам.

Обидві статті мають спільну мету - підвищити рівень безпеки облікових записів у корпоративних IT-системах. Проте вони підходять до проблеми з різних сторін: перша - через інноваційний підхід SSI, друга - через оптимізацію традиційних засобів Windows Server.

## Методологія

*Self-Sovereign Identity-Based IAM in Enterprises*

**Методологія**: Design Science Research (DSR)

**Етапи**:

- Систематичний огляд літератури (SLR)

- Кодування вимог (280 кодів, 24 категорії, 4 кластери)
- Напівструктуровані інтерв'ю з 12 експертами
- Створення прототипу SSI-рішення на базі Hyperledger Aries Cloud Agent (ACA-Py)
- Оцінка прототипу через експертні інтерв'ю

**Інструменти**:

- Hyperledger Indy (блокчейн)
- Verifiable Credentials (VC), Verifiable Presentations (VP)
- Мобільні гаманці (esatus, Trinsic, Lissi)

*Забезпечення безпеки облікових записів корпоративних користувачів (Windows Server IAM)*

**Методологія**: Прикладне моделювання та тестування

**Етапи**:

- Аналіз статистики вразливостей Windows Server
- Моделювання атак (наприклад, mimikatz)
- Впровадження утиліт моніторингу (Netwrix Auditor, Semperis DSP, Account Lockout Examiner)
- Налаштування політик безпеки AD
- Тестування функціоналу групи Protected Users

**Інструменти:**

- Windows Server 2012 R2+
- Active Directory
- Утиліти: Netwrix Auditor, Semperis DSP, SolarWinds Permissions Analyzer, Sticky Password

**Результати**

*Self-Sovereign Identity-Based IAM in Enterprises*

*Визначено 4 кластери IAM-вимог:*

1. Security & Compliance
2. Operability
3. Technology
4. User

*Прототип SSI-системи:*

- Видача VC через HR-агента
- Використання VP для входу в інтранет
- Відкликання VC через блокчейн-реєстр
- Захист через selective disclosure та ZKP

*Експертна оцінка:*

- SSI добре інтегрується з OIDC/OAuth
- Підтримує ABAC
- Підвищує прозорість, контроль, безпеку
- Виявлено проблеми з юзабіліті, відсутністю credential chaining

*Забезпечення безпеки облікових записів корпоративних користувачів (Windows Server IAM)*

*Визначено базові правила безпеки:*

- Мінімізація привілеїв
- Персоніфікація акаунтів
- Заборона cached credentials для критичних користувачів
- Строга політика паролів

*Впроваджено комплекс утиліт:*

- Semperis DSP - виявлення змін навіть без журналювання
- Netwrix Auditor - фіксація несанкціонованих змін
- Account Lockout Examiner - аналіз спроб входу

*Моделювання атаки mimikatz:*

- Виявлення через Semperis DSP
- Відновлення прав доступу через інтерфейс

*Впроваджено групу Protected Users:*

- Автентифікація лише через Kerberos
- Відсутність кешування
- Вимога AES-шифрування

**Ключові інсайти**

1. SSI дозволяє реалізувати принцип найменшого привілею без централізованих IAM-систем

Завдяки selective disclosure та атестаціям, користувачі отримують лише ті права, які необхідні. Це знижує ризики надмірного доступу. Це може бути основою для побудови ABAC-моделей у мультиорганізаційних середовищах.

2. Semperis DSP здатен виявляти зміни навіть при вимкненому журналюванні

Це унікальна функція, яка дозволяє виявляти атаки, що обходять стандартні механізми логування. Тобто, можна використовувати цей інструмент для побудови системи реагування на інциденти в критичних середовищах.

3. Група Protected Users - ефективний механізм захисту привілейованих облікових записів.

Обмеження на автентифікацію, кешування та шифрування значно знижують ризик компрометації. Можна враховувати це для сегментації ролей у політиках доступу.

4. SSI підтримує passwordless автентифікацію з вбудованим 2FA

Це знижує залежність від паролів і покращує користувацький досвід. Можна це використовувати як метод контролю security fatigue («втоми від безпеки») у майбутній роботі.

5. Windows Server дозволяє налаштовувати політики паролів через AD

Можна встановити довжину, складність, термін дії, унікальність паролів. Це практичний інструмент для захисту від атак типу Kerberoasting.

6. SSI дозволяє інтегруватися з існуючими IAM-рішеннями через OIDC/OAuth

Це забезпечує поступовий перехід без втрати інвестицій. Застосовується для гібридної інтеграції SSI з системами доступу.

7. Використання мобільних додатків для зберігання паролів - баланс між безпекою і зручністю

Sticky Password - приклад рішення, яке дозволяє використовувати складні паролі без втрати юзабіліті. Це важливо для підтримки password hygiene у великих командах.

8. SSI-гаманці забезпечують прозорість і контроль над розкриттям даних

Користувач бачить, хто запитував його атестації, і може відкликати доступ. Це критично для відповідності GDPR та побудови довіри в системах доступу.

9. Моделювання атак (наприклад, mimikatz) дозволяє перевірити ефективність захисту

Практичне тестування виявляє слабкі місця в реальному середовищі. Моделювання атак допомагають підготувати систему для роботи.

10. SSI відкриває перспективу credential chaining - але технічно обмежену

Як варіант це може дозволити створювати складні зв’язки між атестаціями. Можливо великі організації будуть впроваджувати цю функцію після її вдосконалення.

**Висновок**

Обидві публікації роблять вагомий внесок у галузь корпоративної безпеки облікових записів, але з різних позицій:

Стаття про SSI - інноваційна, стратегічна, орієнтована на майбутнє. Вона демонструє, як децентралізовані технології можуть змінити підхід до IAM, зробити його гнучким, прозорим і масштабованим.

Стаття про Windows Server IAM - глибоко практична, орієнтована на оптимізацію існуючих рішень. Вона демонструє, як правильно налаштовані політики, утиліти та архітектура можуть забезпечити високий рівень захисту в реальному корпоративному середовищі.

Обидва підходи доповнюють один одного. SSI - стратегічний напрямок розвитку IAM, Windows Server - як перевірена платформа для реалізації політик безпеки тут і зараз.

**Перспективи подальших досліджень:**

*Інтеграція SSI з Active Directory через гібридні моделі*

- Порівняння ефективності моніторингу між Semperis DSP та SSI-гаманцями
- Вивчення поведінки користувачів при переході до passwordless моделей
- Розробка сценаріїв credential chaining у SSI для корпоративного середовища

Обидві роботи після їх аналізу виглядають як карта переходу: від оптимізованої централізованої моделі до децентралізованої, гнучкої та прозорої системи управління ідентичністю.