УДК 004.056.53

О.В. Кручінін[1], М.О. Герасимов[1]
[1]Національний технічний університет «Дніпровська політехніка», Дніпро, Україна

СУЧАСНІ ЗАСОБИ АВТЕНТИФІКАЦІЇ В СИСТЕМАХ ІДЕНТИФІКАЦІЇ ТА КОНТРОЛЮ ДОСТУПУ

Анотація. Розглянуто необхідність процесів ідентифікації та автентифікації при побудові систем інформаційної безпеки. Виконано порівняння існуючих засобів ідентифікації та автентифікації в розподілених мережах. Зроблено висновки стосовно доцільності їх використання.

***Ключові слова**: ідентифікація, автентифікація, авторизація, управління ідентифікацією та доступом, розподілені мережі.*

Вступ. Процес ідентифікації та автентифікації є дуже важливим. Без нього неможлива побудова систем інформаційної безпеки. Це та задача, що потребує постійного вдосконалення своєї реалізації.

На сьогодні існує велика кількість методів ідентифікації та автентифікації, які реалізуються багатьма засобами, кожен з яких має свої переваги та недоліки. Тому для прийняття рішення чи підходить той чи інший засіб для вирішення задачі, необхідно виконати їх аналіз та порівняння.

Постановка задачі. Для досягнення поставленої мети в роботі сформовані і вирішені такі завдання:

- викласти принципи ідентифікації та автентифікації в розподілених системах;
- визначити основний, мінімально необхідний фунціонал системи ідентифікації та автентифікації;
- обрати ознаки для класифікації систем ідентифікації та автентифікації;
- виконати аналіз та порівняння існуючих систем;
- зробити висновки щодо доцільності їх використання.

Основний зміст роботи. У загальному розумінні, система управління ідентифікацією та доступом – це система бізнес-процесів для управління ідентифікаційними даними та системами контролю та управління доступом [1]. Така система складається з організаційної політики та спеціальних програмних і/або програмно-апаратних засобів.

Побудова систем ідентифікації та контролю доступу можлива на базі багатьох факторів автентифікації, де автентифікація – процедура перевірки відповідності пред’явленого ідентифікатора об’єкта комп’ютерної системи на предмет належності його цьому об’єкту; встановлення або підтвердження автентичності [2].

Однією з ознак, за якими можна класифікувати системи ідентифікації та контролю доступу, є фактори, на підставі яких виконується автентифікація. У загальному випадку розрізняють такі факторі автентифікації:

- фактор знання – те, що користувач знаєте, може бути будь-якими обліковими даними автентифікації, що складаються з інформації, якою володіє користувач, включаючи персональний ідентифікаційний номер (PIN), ім'я користувача, пароль або відповідь на секретне питання;
- фактор володіння – те, що у користувача є, може бути будь-яким посвідченням, ґрунтується на предметах, якими користувач може володіти і носити з собою, включаючи апаратні пристрої, такі як токен безпеки або мобільний телефон, використовуваний для прийому текстових повідомлень або запуску застосування автентифікації, яке може генерувати одноразовий пароль або PIN-код;
- фактор інгерентності – те, чим користувач є, зазвичай ґрунтується на якій-небудь формі біометричної ідентифікації, включаючи відбитки пальців, розпізнавання особи, сканування сітківки ока або будь-яку іншу форму біометричних даних;
- фактор місцеположення – може бути менш конкретним за попередні, але фактор місцезнаходження іноді використовується як доповнення до інших факторів. Місце розташування можна визначити з достатньою точністю за допомогою пристроїв, оснащених системою глобального позиціонування, або з меншою точністю шляхом перевірки мережевих адрес і маршрутів. Фактор місця розташування зазвичай не може використовуватися для автентифікації сам по собі, але він може доповнювати інші фактори, надаючи можливість виключити деякі запити. Наприклад, він може завадити зловмисникові, що знаходиться у видаленій географічній зоні, видати себе за користувача, який зазвичай входить в систему тільки зі свого дому або офісу в країні розташування організації;
- фактор часу – час автентифікації, сам по собі недостатній, але він може бути додатковим механізмом для відсіювання зловмисників, які намагаються отримати доступ до ресурсу в той час, коли цей ресурс недоступний для авторизованого користувача. Він також може використовуватися разом з місцем розташування. Наприклад, якщо користувач останній раз проходив автентифікацію опівдні в Україні, спроба автентифікації з Китаю через годину буде відхилена на основі поєднання часу і місця розташування.

Крім цього, залежно від кількості факторів та вимог, які використовуються, сучасні системи можуть реалізовувати наступні методи автентифікації:

- однофакторна – автентифікація, що здійснюється з використанням одного фактору (частіше за все – паролю);
- багатофакторна – автентифікація, що здійснюється з використанням двох або більшої кількості факторів;
- строга – автентифікація, під час якої використовується інформація без розкриття цієї інформації. Як правило, реалізується за допомогою асиметричних криптографічних алгоритмів.

Управління ідентифікацією і доступом (IAM) – це, передусім, визначення і управління ролями і привілеями доступу користувачів. Рішення IAM повинні

мати функціональність для підтримки сховища даних цих користувачів, механізму визначення ролей і авторизації, системи ідентифікації та автентифікації з можливістю єдиного входу, управління паролями, надання/депозиціонування облікових записів і аудиту.

У цій роботі запропонована класифікація систем управління ідентифікацією і доступом за наступними ознаками:

- фактори автентифікації, які використовуються;
- методи автентифікації, які реалізовані;
- наявність можливості використання як хмарного сервісу;
- наявність можливості самостійного встановлення та налаштування;
- наявність телеметрії;
- тип ліцензії.

Було розглянуто та класифіковано наступні IAM системи:

- Okta – це хмарна платформа, що дозволяє користувачам отримувати доступ до усіх програм, використовуючи для цього тільки один логін/пароль [3]. Один логін для доступу, наприклад, до Slack, Zoom, Gmail і Figma. При цьому Okta дозволяє робити це з комп'ютера, планшета або телефону. При цьому адміністратор може віднести користувача до певної групи усередині Okta, щоб надати доступ тільки до потрібного набору програм і сервісів. Має бібліотеку з тисячами готових рішень для інтеграції з різноманітними застосуваннями. Є одним з найпопулярніших продуктів. Використовується такими компаніями, як LinkedIn, Hubpost, T - Mobile і Hewlett Packard. Фактори автентифікації, які використовуються: знання, володіння, інгерентності. Методи автентифікації, які можуть бути реалізовані: однофакторна, багатофакторна;
- OpenIAM – це платформа з відкритим вихідним кодом для управління доступом, дозволами і серверами федерації [4]. Складається з двох основних модулів: Identity Governance та Web Access Manager. Усі модулі платформи мають загальну інфраструктуру, що дозволяє клієнтам бачити єдине рішення для ідентифікації, а не набір розрізнених продуктів. Поширюється як по підписці, так і окремим продуктом для самостійної установки і налаштування. Використовується такими компаніями, як WarnerMedia і Deutsche Bank. Фактори автентифікації, які використовуються: знання, володіння. Методи автентифікації, які можуть бути реалізовані: однофакторна, багатофакторна;
- Auth0 – це перша платформа управління ідентифікацією, спрямована на полегшення для розробників інтеграції платформи із застосуваннями [5]. Є набором окремих API і інструментів для реалізації SSO і управління користувачами. Поставляється в декількох варіантах для різних сценаріїв: B2C (рішення для автентифікації звичайних користувачів за допомогою ідентифікатора і пароля, а також OAuth2), B2B (рішення для автентифікації ділових партнерів за допомогою SAML, LDAP і AD), B2E (рішення для автентифікації співробітників усередині організації). Із закритим вихідним кодом, поширюється по підписці. Є безкоштовні варіанти для невеликих проектів і некомерційних організацій. Популярне рішення, інтегроване в

інфраструктуру таких компаній, як Mazda, AMD і Pfizer. Фактори автентифікації, які використовуються: знання, володіння. Методи автентифікації, які можуть бути реалізовані: однофакторна, багатофакторна;

- Ory Kratos – це хмарна система управління користувачами [6]. Вона забезпечує вхід і реєстрацію користувачів, багатофакторну автентифікацію і зберігання інформації про користувачів за допомогою API. Вона повністю налаштовується, підтримує широкий спектр протоколів, таких як Google Authenticator, і зберігає інформацію про користувачів за допомогою схеми JSON. Ory Kratos реалізує усі необхідні потоки, такі як вхід і вихід з системи, активація облікового запису, багатофакторна автентифікація, управління профілями і сесіями, помилки, з якими стикається користувач, і методи відновлення облікового запису. Поширюється як по платній підписці, так і окремим продуктом для самостійної установки і налаштування. З відкритим вихідним кодом. Відносно молодий продукт. Використовується такими компаніями, як Sainsbury's, Tinkoff Group і Segment. Фактори автентифікації, які використовуються: знання, володіння. Методи автентифікації, які можуть бути реалізовані: однофакторна, багатофакторна;
- Keycloak – це система управління ідентифікацією і доступом з відкритим вихідним кодом для сучасних застосувань і сервісів [7]. Вона дозволяє додати автентифікацію з мінімальними витратами. Продукт з відкритим кодом для реалізації SSO з можливістю управління доступом. Основні функції: User Federation (зв’язування цифрової особстості користувача та її атрибутів, що зберігаються у кількох різних системах управління ідентифікацією), Identity Brokering (створення довірчих відносин із зовнішнім постачальником ідентифікаційних даних), Social Login (схема автентифікації, що дозволяє отримати доступ до різних незалежних сервісів з одними автентифікаційними даними за допомоги соціальних мереж). Поширюється як безкоштовне рішення для самостійної установки і налаштування. Використовується такими компаніями, як Gympass і Backbase. Фактори автентифікації, які використовуються: знання, володіння. Методи автентифікації, які можуть бути реалізовані: однофакторна, багатофакторна.

Порівняння IAM систем наведено в табл. 1.

Майже кожний з представлених продуктів поставляється як хмарний сервіс, тоді як програмних засобів для самостійного встановлення/налаштування значно менше. Використання архітектури хмарного сервісу прискорює інтеграцію з кінцевими точками системи, що призначені для взаємодії з користувачем, проте виникає залежність від інфраструктури сторонньої компанії та її захищеності, завдяки чому виникають ризики, пов’язані з конфіденційністю і доступністю. Також більшість програмних засобів мають закритий вихідний код, що підвищує їх кінцеву вартість, а відсутність стороннього аудиту кодової бази може стати причиною появи додаткових вразливостей. А ті продукти, що доступні безоплатно та мають відкритий код, є складними в конфігурації, ресурсномісткими, мають багато надлишкового функціоналу, та збирають телеметрію.

Таблиця 1

Порівняльна характеристика IAM систем

Характеристика	Система				
	Okta	OpenIAM	Auth0	Ory Kratos	Keycloak
Фактор знання	+	+	+	+	+
Фактор володіння	+	+	+	+	+
Фактор інгерентності	+	-	-	-	-
Фактор місцеположення	-	-	-	-	-
Фактор часу	-	-	-	-	-
Однофакторна автентифікація	+	+	+	+	+
Багатофакторна автентифікація	+	+	+	+	+
Строга автентифікація	-	-	-	-	-
Хмарний сервіс	+	+	+	+	-
Можливість самостійного встановлення та налаштування	-	+	-	+	+
Телеметрія	+	+	+	+	+
Тип ліцензії	Пропріє тарний	GNU GPL v3 (продукт з відкритим кодом)	Пропріє тарний	Apache 2.0 (продукт з відкритим кодом)	Apache 2.0 (продукт з відкритим кодом)

Наукова новизна розробки складається в запропонованому класифікаторі систем ідентифікації та контролю доступу.

Висновки. На практиці, при реалізації IAM у багатьох випадках необхідне рішення, яке можна інтегрувати в інформаційно-телекомунікаційну систему малого бізнесу з мінімальними зусиллями й витратами, та за найкоротший термін. Деякі існуючі продукти надають готові конфігурації,

проте вони є лише наочним прикладом роботи програмного засобу, а не готовим та безпечним рішенням для роботи в реальних умовах. Таким чином, існує необхідність у рішенні, яке б поєднувало в собі простоту інтеграції SaaS продуктів і доступність open-source програмного забезпечення.

ПЕРЕЛІК ПОСИЛАНЬ

1. What is identity and access management? Guide to IAM [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system.
2. НД ТЗІ 1.1-003-99 [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.ua/assets/files/1.1_003_99.pdf.
3. What is Okta? [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://support.okta.com/help/s/article/What-is-Okta?language=en_US#:~:text=Okta%20features%20include%20Provisioning%2C%20Single,for%20organization%20security%20and%20control..
4. What is OpenIAM? [Електронний ресурс] – Режим доступу до ресурсу: https://docs.openiam.com/docs-4.2.0.8/getting-started/1-what_is_openiam.
5. Understand How You Can Use Auth0 [Електронний ресурс] – Режим доступу до ресурсу: https://auth0.com/docs/get-started/auth0-overview.
6. Ory Kratos Introduction [Електронний ресурс] – Режим доступу до ресурсу: https://www.ory.sh/kratos/docs/#:~:text=Ory%20Kratos%20is%20an%20API,application%20needs%20to%20deal%20with%3A&text=Admin%20APIs%3A%20Import%2C%20update%2C%20delete%20identities.
7. Keycloak - About [Електронний ресурс] – Режим доступу до ресурсу: https://www.keycloak.org/about#:~:text=Keycloak%20is%20an%20open%20source,with%20little%20to%20no%20code.&text=Trying%20Keycloak%20is%20quick%20and%20easy.

УДК [004.942+005.5]: 614.84

О.М. Шопський[1], О.В. Придатко[1], І.О. Малець[1]
[1]Львівський державний університет безпеки життєдіяльності ДСНС України, Львів

АНАЛІТИКА ВЕЛИКИХ МАСИВІВ ДАНИХ ДЛЯ ПРОГНОЗУВАННЯ РИЗИКОВИХ СИТУАЦІЙ

Анотація. Описано процес узагальнення масиву даних для аналітики прогнозування ризикових ситуацій.

Ключові слова. *Система оперативно-диспетчерського управління, СОДУ, геоінформаційна система.*

Вступ. Техногенне навантаження та зміни клімату стимулюють до частого виникнення різного роду ризикових ситуацій: пожеж, ДТП, паводків тощо. Кожна подія супроводжується значними матеріальними збитками, а не