УДК 004.72.056.523 **DOI:** 10.31673/2412-9070.2024.014851

М. І. БАКЛИКОВ, студент магістратури;
А. М. ТУШИЧ, доктор філософії (PhD), доцент;
Ю. К. КАГРАМАНОВА, аспірантка,
Державний університет інформаційно-комунікаційних технологій, Київ

ЕФЕКТИВНІСТЬ ЗАСТОСУВАННЯ IAM-СИСТЕМИ НА ПІДПРИЄМСТВІ

Розглянуто проблеми підприємства, де відсутня централізована система обліку ідентифікаційних даних і контролю доступу, та описано переваги, які може надати впровадження IAM-системи. Перелічено основні компоненти та наведено технології, що використовуються у системах IAM. Здійснено аналіз ефективності від використання IAM-системи на підприємстві та перші кроки щодо її впровадження. Запропоновано питання, на які потрібно надати відповіді перед вибором тієї чи іншої системи керування обліковими даними.

Ключові слова: IAM-система; облік ідентифікаційних даних; контроль доступу; автентифікація; авторизація.

Вступ

Постановка проблеми. Уявімо процес організації доступу до IT-ресурсів у компанії без автоматизації. Під час прийняття на роботу відповідальна особа відділу кадрів вносить дані щодо нового працівника в облікову систему. Потім ця інформація потрапляє до IT-відділу. IT-відділ створює обліковий запис у службі каталогів Active Directory, формує для співробітника поштову скриньку. Далі, звернувшись до системного адміністратора, новий працівник отримує доступ до спільних папок, бази даних, інших застосунків. Найчастіше системний адміністратор має узгоджувати надання того чи іншого доступу з керівництвом.

Якщо в невеликій компанії організація доступу вирішується прямими комунікаціями та новачок протягом дня зможе отримати доступ до всього, що потрібно йому для роботи, то в географічно розподіленій компанії зі штатом понад 500 осіб на це можуть знадобитися дні.

За кілька років роботи в компанії співробітник просто-таки «обростає» доступами в різні системи, при цьому він ніколи не просить позбавити його доступу. Якщо в компанії є працівники, що працюють за контрактом, або сезонні робітники, то в разі розторгнення контракту доступ до ресурсів має бути припинено.

У співробітника може змінюватися посада, телефон, прізвище, і ці зміни мають відразу відображатися в усіх інформаційних системах. За відсутності автоматизації ці зміни доведеться вносити до кожної системи вручну. У разі зміни посади слід пам'ятати, яких ресурсів потрібно позбавити, а які надати.

Якщо в компанії кілька інформаційних систем, наприклад, система документообігу, бухгалтерська програма, корпоративна пошта, то постає завдання керування паролями. Паролі в кожній системі створюються окремо, і вони можуть не збігатися. Користувачеві важко запам'ятати кілька паролів, і це призводить до того, що їх зберігають на папері і в такий спосіб компрометують. Якщо користувач забув пароль або його обліковий запис було заблоковано через неправильно введені дані, йому доведеться звертатися до системного адміністратора і чекати на його допомогу, тоді як доступ йому потрібен негайно.

У разі звільнення працівника необхідно заблокувати йому доступ до всіх систем компанії і це зазвичай важливо зробити дуже швидко. Такий процес у масштабах великої організації забирає у IT-відділу багато часу, неминуче призводячи до помилок та, як наслідок, фінансових втрат.

Аналіз останніх досліджень і публікацій. Вибір рішень IAM на ринку досить різноманітний. Є рішення, які можна встановлювати на серверах компанії, та рішення, які можна орендувати у форматі хмарного сервісу (Identity as a Service). Можна також розробити свою IAM-систему на основі open-source рішень або пропрієтарного програмного забезпечення власного розроблення [1].

Переваги систем IAM активно досліджують компанії, які саме і розробляють рішення IAM, такі світові гіганти, як Microsoft [2] та Oracle [3], а також і невеликі локальні українські як GlobalLogic [4]. Але у відкритих даних цих компаній немає практичних кроків і конкретних рекомендацій, яку саме IAM-систему варто вибрати. У цій статті буде зроблено акцент на практичному боці питання.

Мета статті — знайти вирішення, яке дасть змогу усунути зазначені проблеми, а саме: оптимізувати процес обліку співробітників, підвищити безпеку паролів, прискорити процес надання доступу до корпоративних ресурсів.

Основна частина

Сьогодні існує безліч систем, що розв'язують описані раніше проблеми. Найчастіше ми зустрічаємо термін *Identity Management* **(IdM)**, що означає керування обліковими записами або електронними уявленнями користувачів. Але здебільшого

від IdM-системи вимагається керувати не лише обліковими записами, а й доступом до систем. Тому зазвичай, якщо говорять про IdM, то йдеться про *Identity and Access Management* **(IAM)**.

Але для початку дамо визначення IAM і опишемо більш докладно, що являє собою IAM-система.

Під Identity and Access Management розуміють набір технологій та програмних продуктів, що відповідають задачам керування життєвим циклом облікових записів та керування доступом до різних систем у компанії [5]. Система ідентифікації та керування доступом — це рішення, яке виконує роль ядра, що об'єднує всі дані про співробітника в організації: не тільки ПІБ та унікальний ідентифікатор, а й коли він влаштувався, яку посаду обіймає, які права має, і, відповідно, до яких систем повинен мати доступ.

Далі розглянемо, який вигляд має процес формування користувачів на підприємстві із системою IAM.

З появою нового співробітника інформація про нього заноситься лише до однієї облікової системи, а саме — до списку користувачів IAM. Немає потреби вносити ці дані повторно до інших систем та баз даних. Інформація про цього користувача буде автоматично поширена всіма під'єднаними керованими системами.

Потім на основі атрибутів користувача (посада, відділ) IAM-системою буде надано доступ цьому співробітнику тільки до тих систем та в тому обсязі, які йому необхідно мати згідно з посадою (тобто потрібні для виконання своїх функціональних обов'язків). IAM-система може перевіряти значення атрибутів на відповідність правилам та забороняти створення некоректних записів, наприклад із незаповненою посадою. Це унеможливить появу співробітників із неконтрольованим доступом.

Тепер за будь-яких змін достатньо внести дані в одному місці, і вони автоматично будуть відображені в усіх під'єднаних системах. Так, наприклад, користувач, змінюючи свій пароль, автоматично отримує такий самий пароль у всіх системах. У разі переведення чи звільнення працівника система відбирає доступ до всіх керованих систем майже миттєво.

Що є основними компонентами IAM? Існує безліч стандартів та протоколів IAM, але Identity Management Institute розбиває IAM на три складові, які дістали назву модель AAA. Три A — це автентифікація (authentication), авторизація (authorization) та облік (accounting). Ці три протоколи разом становлять повноцінну IAM-систему [6]. Розглянемо ці компоненти докладніше.

Автентифікація. Інструменти автентифікації гарантують, що людина, яка входить до системи, є саме тою, ким вона себе називає. Існує три основні типи автентифікації:

1) інформація, відома користувачеві, наприклад пароль або відповідь на секретне запитання;

2) об'єкт, яким володіє користувач, наприклад токен або смарт-картка;

3) унікальна біометрія, наприклад відбиток пальця.

Інструменти автентифікації IAM можуть вмикати двофакторну *2-factor authentication* (2FA) або багатофакторну *multi-factor authentication* (MFA) автентифікацію, яка використовує комбінацію зазначених раніше категорій для посилення безпеки – наприклад, ваш пароль та ваш смартфон. Інструменти IAM також можуть застосовувати служби єдиного входу *Single Sign-On* (SSO), які дають змогу користувачеві отримувати доступ до всіх програм через один централізований вхід.

Авторизація. Авторизація полягає в керуванні обліковими даними; системні адміністратори керують правами доступу користувачів, а система IAM гарантує, що користувачі отримують доступ тільки до тих даних, які абсолютно необхідні для виконання посадових обов'язків. У надійній системі IAM доступ до даних визначається наданою співробітнику роллю, яка налаштована в такий спосіб, що задовольняє всі його робочі потреби.

Облік. Облік передбачає ведення логів: запис у журнал дій користувачів і неперервний їх моніторинг для виявлення аномальної поведінки, що вказує на потенційні спроби зламати систему. Облік дає можливість IT-адміністраторам оперативно реагувати та запроваджувати додаткові заходи щодо контролю в разі виявлення вразливості.

В IAM виокремлюють два різні технологічні підходи:

- технологія корпоративного єдиного входу — Enterprise Single Sign-On (ESSO або просто SSO);
- технологія постачальника ідентифікації — Web SSO, Identity Provider (IdP).

У першому підході в процесі впровадження технології на кожен персональний пристрій установлюють програму-агент ESSO. Коли пристрій вмикають, ESSO пропонує користувачу пройти ідентифікацію та автентифікацію з використанням комбінації методів — перевірки пароля, смарт-картки, біометрії.

Після цього користувач може запустити потрібну йому програму. Водночас програма нічого не знає про використання ESSO і під час запуску спробує показати користувачеві екран запиту логіна та пароля. Але агент ESSO перехоплює екран входу і сам підставляє замість користувача його логін і пароль.

Отже, користувач отримує надійну ідентифікацію/автентифікацію на етапі входження в пристрій, а також зручний автоматичний вхід до всіх інформаційних систем компанії. Але такий підхід зумовлений так званим обманом застосунків.

Вхід до них за допомогою логіна/пароля в обхід запущеного агента ESSO як і раніше можливий, а отже, зберігається багато загроз, властивих парольній автентифікації, що є, безумовно, недоліком.

Ще один важливий момент у використанні ESSO — це обмеженість пристроїв, на яких можливе встановлення агента. Також імовірне виникнення проблем із підтриманням Linux, MacOS, iOS чи Android.

Другий технологічний підхід — упровадження IdP. Цей підхід позбавлений недоліків ESSO. Користувач має змогу використовувати будь-які пристрої, а для роботи достатньо веббраузера. Як пристрої можуть застосовуватися не тільки ПК та смартфони, а й голосові станції, ігрові приставки і навіть Smart TV.

Розплатою за таку гнучкість стає потреба в підтриманні з боку програм можливості підімкнення до IdP. Інакше кажучи, застосунок має підтримувати будь-який стандарт взаємодії з IdP. Але більшість популярних застосунків та хмарних сервісів уже вміють це робити, тому недоліком це не є.

У процесі використання IdP користувач звертається до програми, а вона замість відображення свого екрана входу надсилає серверу запит на ідентифікацію. Якщо IdP уже знає користувача, то відбувається перевірка дозволу на вхід до програми та реєстрація факту відвідування. Після цього дані про користувача, отримані з каталогу облікових записів компанії, повертаються до застосунку. Якщо ж IdP не знає користувача, то запропонує йому спочатку пройти ідентифікацію та автентифікацію. Замість звичайної перевірки логіна/пароля IdP може застосовувати додаткові методи автентифікації залежно від контексту входу та політики доступу. Наприклад, під час входу до програми з робочої мережі користувач може бути автоматично ідентифікований за результатами перевірки в домені (технологія Kerberos SSO). Якщо ж користувач хоче зайти в якусь дуже важливу програму або, наприклад, здійснює вхід із мережі «Інтернет» з незнайомого пристрою, то IdP може запросити додаткове підтвердження — запропонувати ввести разовий пароль, надісланий по SMS або згенерований мобільним застосунком разових паролів.

Упровадження IAM. Зрештою, щоб розробити найкращу архітектуру IAM для своїх конкретних варіантів використання, організації знадобиться виконати певну роботу [10]. Насамперед потрібно відповісти на наведені далі запитання.

1. Чого організація сподівається досягти внаслідок упровадження IAM?

2. Кого IAM буде автентифікувати і чому?

3. Якими сервісами чи застосунками користуються в організації?

4. Де перебувають користувачі?

Під час відповіді на ці питання треба звернути особливу увагу на такі елементи:

• наявність програм Software as a Service (SaaS), розміщених за межами корпоративного середовища;

• випадки, коли потрібно використовувати ідентичність, що не належить організації.

Процес підготовки можна розбити на три кроки.

Крок 1. Адміністратори підприємства мають скласти каталог застосунків, сервісів та інших елементів, з якими, на їхню думку, взаємодіятимуть користувачі. Створення такого переліку допоможе з'ясувати спільно з іншими учасниками процесу його повноту та коректність. Цей список також можна використати як вихідні дані на етапі вибору того чи іншого рішення, коли настане час оцінити, чи забезпечують механізми IAM необхідні можливості.

Крок 2. Потрібно заздалегідь продумати, як різні оточення, наприклад хмарні програми, будуть пов'язані з локальними програмами, такими як вхід до домену. Бувають випадки, коли для різних типів застосунків або різного використання можуть знадобитися різні системи. Розуміння того, які ще системи існують за межами підприємства, теж корисне, оскільки ці системи можуть потребувати специфічних способів об'єднання. Наприклад, один постачальник хмарних послуг може бути підімкнений через SAML, а інший — через OpenID Connect.

Крок 3. Потрібно ретельно розглянути, які спеціальні можливості IAM будуть задіяні. Наступний перелік запитань допоможе підприємствам оцінити потенційних постачальників та системи, які пропонує ринок.

1. Чи потрібна багатофакторна автентифікація (MFA)?

2. Чи мають клієнти та співробітники обслуговуватися в одній і тій самій системі або в різних?

3. Чи потрібне автоматичне поширення інформації про користувачів зкерованими системами з автоматичною їх активацією/блокуванням?

4. Які протоколи під'єднання мають підтримуватись?

Висновки

Упровадження IAM-системи допоможе прискорити надання доступу до ресурсів підприємства новим працівникам, підвищить безпеку наявних інформаційних систем, спростить співробітникам процедуру входу до тієї чи іншої системи перед початком роботи з ними.

Незважаючи на складнощі, пов'язані з упровадженням IAM-систем, та на те, що процес упровадження може відбуватися протягом тривалого часу, плюси від здобутого результату безумовно компенсують усі ті ресурси, що знадобляться на етапі впровадження.

Список використаної літератури

*1. **Gittlen S., Rosencrance L.** What is identity and access management? Guide to IAM [Електронний ресурс]. 2021. URL:*

https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system (дата звернення: 28.10.2023).

*2. **Що таке** система керування ідентичністю та доступом? [Електронний ресурс]. 2023. URL:*

https://www.microsoft.com/uk-ua/security/business/security-101/what-is-identity-access-management-iam (дата звернення: 17.11.2023).

*3. **Identity** and Access Management (IAM) [Електронний ресурс]. 2023. URL:*

https://www.oracle.com/ca-en/security/identity-management (дата звернення: 17.11.2023).

*4. **Identity** and Access Management або система керування обліковими даними. Рішення Microsoft Azure AD [Електронний ресурс]. 2023. URL:*

https://www.globallogic.com/ua/insights/blogs/identity-and-access-management-azure-ad (дата звернення: 18.11.2023).

*5. **Ruchini C.** Introduction to Identity and Access Management [Електронний ресурс]. 2021. URL:*

https://medium.com/identity-beyond-borders/introduction-to-identity-and-access-management-2f3b80862647 (дата звернення: 21.10.2023).

*6. **Understanding** the Importance of IAM (Identity and Access Management) [Електронний ресурс]. 2021. URL:*

https://www.auditboard.com/blog/importance-of-iam/ (дата звернення: 22.10.2023).

*7. **Strom D.** What is IAM? Identity and access management explained [Електронний ресурс]. 2021. URL:*

https://www.mufgamericas.com/insights-and-experience/what-iam-identity-and-access-management-explained (дата звернення: 14.10.2023).

*8. **5 keys** to success when implementing Identity and Access Management [Електронний ресурс]. 2022. URL:*

https://www.trustbuilder.com/articles/5-keys-to-success-when-implementing-iam/ (дата звернення: 10.11.2023).

*9. **Brooks S.** Tips for Getting IAM Implementation Right [Електронний ресурс]. 2023. URL:*

https://convergetp.com/2023/05/09/tips-for-getting-iam-implementation-right/ (дата звернення: 15.10.2023).

*10. **Moyle E.** How to build an effective IAM architecture [Електронний ресурс]. 2020. URL:*

https://www.techtarget.com/searchsecurity/feature/How-to-build-an-identity-and-access-management-architecture (дата звернення: 11.11.2023).

*11. **Magnusson A.** Identity and Access Management (IAM) Best Practices [Електронний ресурс]. 2022. URL:*

https://www.strongdm.com/blog/iam-best-practices (дата звернення: 12.11.2023).

M. Baklykov, A. Tushych, Yu. Kargamanova

EFFICIENCY OF USING IAM SYSTEM AT THE ENTERPRISE

The article discusses the problems on a common enterprise that does not have an Identity and Access Management system and describes the benefits which the implementation an IAM system can provide. The main components are listed and the technologies used in IAM systems are described. Effectivity of using an IAM system at the enterprise and the first steps for its implementation are analyzed. Questions that need to be answered before choosing a particular Identity and Access Management system are listed. The aim of this work is to find a solution that will eliminate the problems described in the article, and especially to optimize the employee accounting process, increase password security, and make it easier to grant access to the corporate resources. The choice of IAM solutions on the market is quite diverse. There are solutions that can be installed on company servers, as well as solutions that can be rented as cloud service (Identity as a Service). You can also build your own IAM system using open-source solutions or developing proprietary software. There are many articles in the Internet describing what Identity and Access Management is and why it is so important to use it. But these articles do not include any practical steps or specific recommendations which IAM system to choose. This article focuses on the practical side of the issue. The implementation an IAM system will accelerate the provision access to the enterprise resources for new employees, increase the security of existing information systems, and simplify the procedure for employees to log in the corporate resources before starting to work with them. Despite the difficulties related with the implementation of IAM systems and the fact that the implementation process can take a long time, the benefits of the result will compensate for all the resources spent on implementation.

Keywords: IAM system; identity management; access management; authentication; authorization; accounting.