УДК 004.056.523

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ЦЕНТРАЛІЗОВАНОЇ ІДЕНТИФІКАЦІЇ, АВТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ КОРИСТУВАЧІВ У ОСВІТНІХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Малініч П. П., Коваленко О. О., Малініч І. П. (pavlo.malinich@vntu.edu.ua)
Вінницький національний технічний університет (Україна)

У тезах розглядаються особливості процесу впровадження системи єдиного входу у інформаційних системах закладів вищої освіти, а також технології, які при цьому використовуються. Приділяється увага прикладам використання таких технологій в українських та закордонних університетах. У висновку підведено підсумок перспектив розвитку цієї технології в українських ЗВО.

Освіта, як і будь-яка інша галузь, потребує надійних рішень для централізованої ідентифікації, автентифікації та авторизації своїх користувачів. Необхідність мати окремий логін та пароль для різних онлайн-сервісів одного ЗВО є не лише не комфортним для учасників освітнього процесу, але й забирає багато робочого часу на відновлення доступу до них, ускладнює адміністрування бази користувачів на кожному окремому такому сервісі, а також створює додаткові безпекові ризики. Вирішується подібна проблема завдяки впровадженню системи єдиного входу (*англ*. Single Sign-On, SSO), яка у свою чергу має доступ до єдиної бази ідентифікації користувачів підприємства (*англ*. Identity Provider, IdP).

Системи єдиного входу (SSO) являє собою сукупність інструментів та засобів для забезпечення зручної та швидкої автентифікації з окремих додатків чи систем. Здебільшого SSO складаються із двох основних компонентів: постачальників ідентифікації (IdP) та постачальників сервісу автентифікації та авторизації (*англ*. Authentication and Authorization Service Provider, A&A SP). IdP відповідає за перевірку ідентичності користувача та його аутентифікацію. SP виступає посередником у цих процесах між користувачем та IdP та контролює доступ до ресурсів чи даних, до яких користувач матиме доступ. IdP створює і надає токени користувачу після автентифікації, користувач представляє їх SP для отримання доступу. Іноді можуть існувати додаткові елементи SSO, які можуть додаватись у залежності від вимог. Такими можуть бути: (2) засоби обміну даними аутентифікації – наприклад токени SAML, ідентифікаційні токени OpenID Connect, токени доступу OAuth 2.0, тощо; (3) федерація – обмін та визначення довіри ідентичності користувачів між різними системами; (4) метадані – інформація про конфігурацію та відкриті ключі; (5) керування сеансами – відстеження автентифікованого стану користувача в різних додатках; (6) одночасний вихід (SLO) – вихід із всіх додатків у системі SSO при виході з одного додатку. Невід'ємною складовою SSO-рішень є багатофакторна автентифікація (*англ*. Multi-factor authentication, MFA), яка полягає у комбінації двох чи більше видів автентифікації користувача. MFA поділяється на три категорії: "що я знаю" – пароль, ключова фраза тощо; "що я маю" – смартфон, фізичний ключ (смарт-карта), мікрочіп тощо; "ким я є" – відбиток пальця, сітківки ока тощо. Подібні підходи дозволяють ускладнити компрометацію доступу кожного окремого користувача.

Для обміну даних між компонентами SSO-систем є протоколи SAML, OAuth та LDAP. SAML – протокол, що забезпечує безпечний та надійний зв'язок між IdP та SP із форматом даних на основі XML. Протокол OAuth призначений для надання обмеженого доступу до ресурсів користувача без розкриття його облікових даних. Основна відмінність від SAML полягають у відсутності конкретного формату даних, зокрема "Client Credentials", "Authorization Code",

"Implicit" тощо. У свою чергу LDAP зазвичай використовується для доступу до даних в каталогах та пошуку ідентифікаційних даних. У той час як SAML та OAuth сфокусовані на обмін інформацією та авторизацію у різних середовищах, LDAP використовується для доступу до даних ідентифікації у каталогах.

Серед найбільш використовуваних у освітньому середовищі SP-реалізацій для автентифікації та авторизації онлайн можна визначити такі: SimpleSAMLphp, OpenAM та Shibboleth. SimpleSAMLphp розроблений для реалізації систем автентифікації на основі SAML. Він має менш складну реалізацію порівняно зі більш складними системами, такими як OpenAM і Shibboleth. OpenAM має широкий спектр можливостей для управління ідентичністю та доступом, включаючи аутентифікацію, авторизацію та управління сеансами. Якщо визначати яке рішення найбільш краще підходить для вищої освіти, то найбільш оптимальним вибором можна вважати саме Shibboleth. В якості найбільш вживаних IdP-систем у сфері освіти можна виділити наступні: Apache Directory, FreeIPA, Microsoft Active Directory та OpenLDAP. FreeIPA – ще одна реалізація IdP для Unix-подібних систем, яка призначена для тісної інтеграції з операційними системами Unix та Linux. FreeIPA та OpenLDAP потребують спеціальних прошарків для інтеграції з не-Unix системами, наприклад Samba (для Windows).

Для розгортання Self-hosted системи, яка могла б поєднати у собі функціонал як IdP-систем так і A&A SP-систем необхідно будувати та налаштовувати досить складну інфраструктуру з різних програмних рішень, перед чим необхідно виконати достатньо ретельний аналіз існуючої IT-інфраструктури та розробку архітектури. Для супроводу подібних систем потрібно мати штат висококваліфікованих DevOps-інженерів та системних адміністраторів, що далеко не завжди можливо для IT-відділів навчальних закладів, зокрема і ЗВО України технічного спрямування.

Завдяки розвитку хмарних технологій, нині можливо використати відповідні хмарні рішення для впровадження SSO у організації, які поєднують у собі функціонал IdP та SP. Таким чином можливо суттєво спростити налаштування таких рішень, а також позбутись необхідності самостійно підтримувати ряд складних програмних сервісів. Серед переваг використання хмарних SSO-сервісів найбільш суттєвими є легкість впровадження, адміністрування, інтеграції з іншими сервісами та високий рівень кіберзахищеності. Легкість впровадження полягає у тому, що подібні сервіси мають потужні плагіни та засоби штучного інтелекту для видобутку та уніфікації розрізнених баз користувачів з різних онлайн-ресурсів певної організації. Подібні сервіси легко адмініструвати, тому що вони мають централізовану веб-консоль управління. Уніфікація різних підсистем також дозволяє спростити адміністрування. Іншою перевагою є гарний рівень інтеграції з іншими хмарними сервісами, такими як Google Workspace, Microsoft 365 (Office 365), Zoom, Salesforce, AWS, Zoho, WordPress тощо. Безпека акаунтів користувачів забезпечується завдяки використанню MFA та регулярній ротації паролів. Над глобальною безпекою хмарних SSO-сервісів працюють цілі команди кібербезпеки, DevOps та розробники, оскільки захищеність цих сервісів є запорукою їх репутації, що максимально зменшує можливість експлуатації вразливостей менш захищених мережевих протоколів [1].

Серед існуючих хмарних сервісів з функціоналом IdP та SP виділено наступні, які є популярними серед українських та закордонних ЗВО: Microsoft Entra ID, Delinea, Okta та Zluri. Microsoft Entra ID постачається разом із підпискою Microsoft 365 та Azure. Перевагою для ЗВО є наявність безкоштовної підписки. Користувачі освіти: Університет "КРОК", EPAM Academy, Донецький національний університет імені Василя Стуса, Дніпровський національний університет імені Олеся Гончара [2, 3]. Delinea (раніше відома як Centrify) також має досить широке коло освітніх клієнтів: Гарвардська медична школа, Університет Флориди, Північно-східний університет (США), Університет Східної Кароліни [4]. Маючи гарні конкурентні переваги у сфері інтеграції Okta є також і найбільш дорогим сервісом, серед його користувачів є Університет Нотр-Дам [5]. Останній, Zluri відомий завдяки потужній інтеграції з сервісом LinkedIn Learning [6]. Одним із недоліків даних сервісів є їх недоступність для бюджетних ЗВО так як вони не продають свої послуги на майданчиках держзакупівель України.

Висновок. При впровадженні систем централізованої ідентифікації, автентифікації та авторизації користувачів, заклади вищої можуть зіткнутися із недостатком функціоналу існуючих SSO-систем, складність міграції та адаптації до потреб освітнього процесу, а також недостаток кваліфікованого персоналу для впровадження подібних систем. Найкращою опцією є

користування послуг компаній, що займаються системною інтеграцією у сфері IT, однак це не завжди можливо для бюджетних установ.

Список використаної літератури

[1] І. П. Малініч і В. І. Месюра, "Ін‘єктивний метод отримання даних користувацького досвіду в ігрових симуляторах комп‘ютерних мереж", *Вісник ВПІ*, вип. 5, с. 49–54, Жовт. 2019.

[2] "Дистанційна освіта в університеті «КРОК» під час карантину", Освіта.UA, 31.07.2020. [Online]. Available: https://osvita.ua/consultations/75374/ [Accessed: September 13, 2023].

[3] "Primary and Secondary Education", Microsoft Customer Stories, 21.09.2021. [Online]. Available: https://customers.microsoft.com/en-us/search?sq=&ff=story_industry_friendlyname%26%3EPrimary%20and%20Secondary%20Education&p=0&so=story_publish_date%20desc [Accessed: March 03, 2023].

[4] "Privileged access management for educational institutions", Delinea, 08.08.2022. [Online]. Available: https://delinea.com/solutions/privileged-access-management-for-educational-institutions [Accessed: September 13, 2023].

[5] "A look into how Notre Dame is protecting and enabling campus users with Okta", Okta, 20.09.2020. [Online]. Available: https://www.okta.com/resources/webinar-a-look-into-how-notre-dame-is-protecting-and-enabling-campus-users-with-okta/ [Accessed: September 13, 2023].

[6] "Get more out of LinkedIn Learning with Zluri", Zluri, 27.11.2021. [Online]. Available: https://www.zluri.com/catalog/linkedin-learning/ [Accessed: September 14, 2023].