Управління доступом до інформації та конфіденційністю даних

Володимир Задворний
аспірант спеціальності 073 «Менеджмент»,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: zadvornyivs@krok.edu.ua,
ORCID: 0009-0005-9172-6732
Марта Копитко
д.е.н., професор,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: marta_kernytska@ukr.net,
ORCID: 0000-0001-6598-3798

Управління доступом до інформації є одним з ключових питань у забезпеченні інформаційної безпеки підприємства і є однією з основних функцій управління інформаційною безпекою підприємства. Управління доступом до інформації забезпечується шляхом розробки та впровадження політик контролю доступу до інформації, процедур щодо надання доступу до інформації та технологій завдяки яким це може бути реалізоване.

Політики контролю доступу мають бути встановлені, задокументовані та регулярно переглядатись, враховуючи вимоги бізнесу до відповідних нормативних документів, особливостей ведення бізнесу та вимог законодавства.

Правила контролю доступу, права та обмеження, а також глибина використовуваного контролю повинні відображати ризики інформаційної безпеки навколо інформації та прагнення організації керувати ними [1].

Контроль доступу може бути цифровим і фізичним за своєю природою, наприклад обмеження дозволів для облікових записів користувачів, а також обмеження щодо того, хто може отримати доступ до певних фізичних місць та об'єктів.

Політики доступу повинні враховувати:

• Вимоги щодо безпеки бізнес-застосунків і відповідність схемі класифікації інформації.

• Управління цифровими активами, хто має отримати доступ, знати, хто має використовувати інформацію підкріплюючись задокументованими процедурами та обов'язками.

• Управління правами доступу та привілейованими правами доступу, включаючи додавання змін у політики доступу і періодичні перевірки.

Технічний рівень управління доступом до інформації та забезпечення конфіденційності даних є рівнем на якому безпосередньо реалізуються процедури щодо надання доступу до інформації та політики доступу до неї. Заходи захисту інформації в засобах і мережах її передавання та обробки передбачають використання апаратних, програмних та криптографічних засобів захисту [2].

Захист інформації та контроль доступу до неї здійснюється шляхом управління ідентифікацією та доступом і стосується набору політик, процесів

і систем, які підтримують прив'язку окремої особи (або в деяких випадках системи) до набору дозволів у системі.

Ці дозволи можуть надавати права особі:

• виконувати функції (наприклад, процес зміни та промислового контролю)

• дані доступу (наприклад, кадрові записи, фінансовий та бухгалтерський облік)

• адмініструвати систему

Система керування доступом складається з низки технічних компонентів, зокрема: сервіси директорій, компоненти автентифікації та частини системи, які споживають інформацію аутентифікації та авторизації [3].

Ці технології та компоненти, можна розділити на різні типи на основі їх функціональних можливостей. Деякі з поширених типів технологій IAM (Identity Management) включають:

• Інструменти керування паролями: ці інструменти допомагають користувачам керувати своїми паролями, забезпечуючи їх надійність і регулярну зміну для підтримки безпеки.

• Програмне забезпечення для ініціалізації: це програмне забезпечення допомагає керувати створенням, зміною та видаленням ідентифікаторів користувачів і прав доступу.

• Програми для забезпечення виконання політики безпеки: ці програми гарантують, що всі користувачі дотримуються політики безпеки організації.

• Програми для звітування та моніторингу: ці програми допомагають відстежувати дії користувачів і створювати звіти для цілей аудиту та відповідності.

• Репозиторії ідентифікаційних даних: це бази даних, де зберігається та керується ідентифікаційна інформація користувача.

• Єдиний вхід (SSO): ця технологія дозволяє користувачам увійти один раз і отримати доступ до всіх систем без запиту повторного входу в кожну з них.

• Багатофакторна автентифікація (MFA): Ця технологія вимагає більше одного методу автентифікації з незалежних категорій облікових даних для перевірки особи користувача для входу в систему або іншої транзакції.

• Автентифікація на основі ризику (RBA): метод застосування різних рівнів жорсткості до процесів аутентифікації на основі ймовірності того, що доступ може бути скомпрометований зловмисниками.

• Біометрична автентифікація: ця технологія використовує унікальні біологічні характеристики, такі як відбитки пальців, розпізнавання обличчя або голосові шаблони, для перевірки особи для безпечного доступу.

• Identity-as-a-Service (IDaaS): ця хмарна служба керує ідентифікацією користувачів і контролем доступу.

Важливо зазначити, що вибір технології IAM має ґрунтуватися на конкретних потребах організації. Фактори, які слід враховувати, включають кількість користувачів, яким потрібен доступ, рішення, пристрої, додатки, послуги, які використовує організація, і наявні IT-налаштування. Правильно обраний набір технології забезпечує оптимальний баланс між потребами у

безпеці інформаційних ресурсів та зручністю й гнучкістю системи управління інформаційною безпекою, що на пряму впливає на ефективність та продуктивність підприємства що є одними з ключових вимог у сучасному світі.

Ключові слова: управління інформаційною безпекою.

Список використаних джерел

1. ISO 27001 – Annex A.9: Access Control. URL: https://www.isms.online/iso-27001/annex-a-9-access-control/ (дата доступу 10.04.2024)

2. Курченко О.А. Підвищення ефективності системи управління захистом персональних даних клієнтів банку / О. А. Курченко, А. В. Головатенко, Л. Ю. Карасевич // Сучасний захист інформації. - 2014. - № 1. - С. 32-37.

3. Introduction to identity and access management. URL: https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management#section_3 (дата доступу 10.04.2024)