**ПРИКЛАД ОФОРМЛЕННЯ**

*Платоненко* Оксана Едуардівна

*студентка групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна*

**УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ**

Управління привілейованим доступом до інформаційної системи - це важлива складова інформаційної безпеки, яка допомагає забезпечити, що лише вповноважені користувачі отримують доступ до конфіденційної інформації та ресурсів.

Привілейований доступ означає отримання повних або розширених прав доступу до системи, даних або ресурсів, який зазвичай надається адміністраторам та іншим важливим користувачам.

Управління привілейованим доступом полягає в установленні, моніторингу та забезпеченні безпеки цих прав (Рис.1).

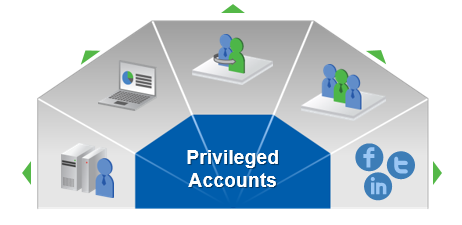


Рис.1. Привілейований доступ. Основні принципи

До основних принципів управління привілейованим доступом відноситься:

*Мінімізація прав*. Це є принцип "найменшого призначення", який передбачає, що користувачам надаються лише ті права, які необхідні для виконання їхніх обов'язків.

*Прозорість та відслідковування*. Всі дії привілейованих користувачів повинні відслідковуватись та журналюватись для аудиту та аналізу безпеки.

*Ревізія та оновлення*. Права доступу повинні періодично переглядатися, а також оновлюватися відповідно до змін в обов'язках користувачів.

*Ідентифікація та аутентифікація.* Перед наданням привілейованого доступу користувачі повинні бути ідентифіковані та аутентифіковані для підтвердження їхньої ідентичності. Двофакторна аутентифікація є важливим засобом підвищення безпеки при вході в систему.

*Управління паролями.* Паролі повинні бути складними, унікальними та періодично змінюватися. Використання парольних менеджерів може допомогти у безпеці паролів.

*Програмне забезпечення для управління доступом*. Інструменти, такі як системи керування доступом (IAM), допомагають автоматизувати та спростити процес управління привілейованим доступом. IAM системи дозволяють легко додавати, видаляти та змінювати права доступу користувачів.

*Загрози та відповідь на інциденти*. Управління привілейованим доступом також включає в себе планування та реагування на інциденти, такі як несанкціонований доступ або компрометація облікових записів.

Зробимо висновки. Ефективне управління привілейованим доступом є ключовою складовою інформаційної безпеки та допомагає забезпечити захист конфіденційної інформації та ресурсів в інформаційній системі. Дотримання принципів мінімізації прав, аутентифікації та періодичного оновлення прав допомагає зменшити ризики та забезпечити безпеку усієї системи.

**Перелік посилань**

1. Привілейований доступ. Чому це важливо і як його контролювати URL: <https://ko.com.ua/privilejovanij_dostup_chomu_ce_vazhlivo_i_yak_jogo_kontrolyuvati_129976> (дата звернення 02.10.2023)
2. Привілейований доступ Delinea URL: https://channel4it.com/publications/ostann-onovlennya-delinea-server-suite-znizhu-rizik-zagroz-bekdoru-na-serverah.html (дата звернення 03.10.2023)