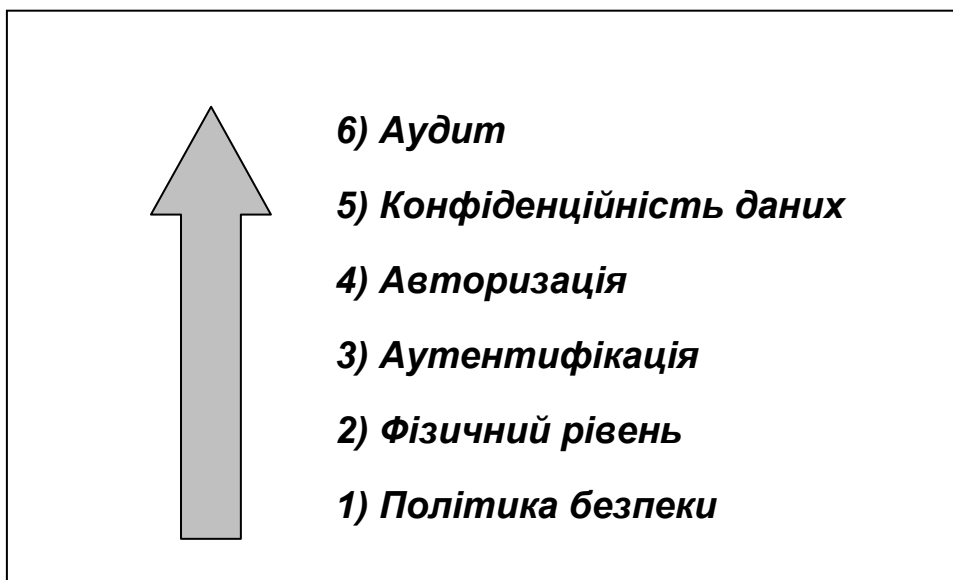


Рівні системи захисту



Так само як будувати хату треба з фундаменту, систему захисту інформацію треба вибудовувати знизу до гори.

Політика безпеки – це набір чітко визначених правил, які мають виконувати особи, що мають доступ до інформаційних фондів та технологій організації. /2.1.1 “Site Security Handbook” RFC 2196/

Фізичний рівень - безпосередній доступ до об’єкту захисту, на відміну від віддаленого доступу.

Аутентифікація – перевірка того, що певний об’єкт дійсно є тим, за кого себе видає.

Авторизація – надання особі певних повноважень на виконання деяких дій в системі.

Конфіденційність даних – забезпечення доступу до даних тільки тих осіб, що мають на це право.

Аудит – регулярна перевірка системи на відповідність певним вимогам (аналіз, діагностика, профілактика).