32. Які класи захищенності рекомендуються для оцінки захищенності механізмів автентифікації та можливості їх реалізації?

Міжнародний стандарт рекомендує використовувати для оцінки захищенності такі класи механізмів автентифікації:

**Клас 0 – незахищений;**

**Клас 1 – захищений від розкриття заявленої ІА (ідентифікація та автентифікація);**

**Клас 2 – захищений від розкриття заявленої ІА й атаки типу «повтор» для різних перевірників;**

**Клас 3 – захищений від розкриття заявленої ІА й атаки типу «повтор» на одного перевірника;**

**Клас 4 – захищений від розкриття заявленої ІА й атаки типу «повтор» на одного перевірника або різних перевірників, модифікації та імітації.**

Під час розгляду механізмів автентифікації й аналізу криптографічних протоколів усе вищезазначене робиться з точки зору пред'явника, і тому пред'явник завжди є ініціатором. На основі цього застосовують усі класи механізмів направленої автентифікації, а потім проводиться уточнення, де ініціатором є перевірник, оскільки вони застосовуються для однонаправленої та взаємної автентифікації.

**Для забезпечення захисту у разі автентифікації джерела даних необхідно використовувати ЕЦП, або її деякий аналог засобом застосування асиметричного направленого шифрування.** Може також застосовуватись симетричне шифрування, наприклад, у вигляді коду автентифікації повідомлення (імітовставки), або криптографічного контрольного значення від даних, що виготовлені з використанням особистого ключа ЕЦП.