|  |
| --- |
| Додаток 3  до Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації, що встановлюються схемами електронної ідентифікації для сфери електронного урядування  (пункт 2 розділу III) |

**ЕЛЕМЕНТИ ТЕХНІЧНИХ СПЕЦИФІКАЦІЙ ТА ПРОЦЕДУР**

**до автентифікації**

**Вимоги до механізму автентифікації засобів електронної ідентифікації**

|  |  |
| --- | --- |
| Рівні довіри до засобів електронної ідентифікації | Обов’язкові елементи технічних специфікацій та процедур |
| Низький | 1. Перед переданням ідентифікаційних даних має здійснюватися надійна верифікація засобів електронної ідентифікації та встановлення їх дійсності.  2. Якщо ідентифікаційні дані зберігаються як частина механізму автентифікації, має здійснюватися захист такої інформації від втрат та компрометації, у тому числі захист від втрат та компрометації в режимі офлайн.  3. Механізм автентифікації має забезпечувати впровадження методів контролю безпеки для верифікації засобів електронної ідентифікації, направлених на якнайбільше зниження ймовірності порушення механізму шляхом реалізації атак підбору, перехоплення, повторного відтворення та підміни порушником з потенціалом здійснення нападу вище ніж базовий. |
| Середній | Такі самі, як для низького рівня довіри.  1. Перед переданням ідентифікаційних даних мають здійснюватися надійна верифікація засобів електронної ідентифікації та встановлення їх дійсності за допомогою динамічної автентифікації.  2. Механізм автентифікації має забезпечувати впровадження методів контролю безпеки для верифікації засобів електронної ідентифікації, направлених на якнайбільше зниження ймовірності порушення механізму шляхом реалізації атак підбору, перехоплення, повторного відтворення та підміни порушником із середнім потенціалом здійснення нападу. |
| Високий | Такі самі, як для середнього рівня довіри.  Механізм автентифікації має забезпечувати впровадження методів контролю безпеки для верифікації засобів електронної ідентифікації, направлених на якнайбільше зниження ймовірності порушення механізму шляхом реалізації атак підбору, перехоплення, повторного відтворення та підміни порушником з високим потенціалом здійснення нападу. |