М-01-3 Вправа: З'єднай термін і визначення (для Liveworksheets)

Інструкція: з'єднайте кожен термін зліва з правильним визначенням справа.

ПІБ: Група: Дата:

Терміни		Визначення	
1	Електронний документ	A.	електронний підпис, який: (1) однозначно пов'язаний із підписувачем, (2) дозволяє ідентифікувати підписувача, (3) створюється даними підпису, що перебувають під одноосібним контролем підписувача, (4) пов'язаний з даними документа так, що будь-яка зміна документа після підписання виявляється під час перевірки
2	Електронний документообіг (ЕДО)	B.	електронний документ, який зв'язує відкритий ключ з ідентифікаційними даними власника (ПІБ/організація тощо) і підписаний (виданий) центром/надавачем сертифікації
3	Електронний підпис (ЕП)	C.	організований процес роботи з електронними документами: створення, погодження, підписання, передавання, зберігання та архівування
4	Удосконалений електронний підпис (УЕП)	D.	секретні криптографічні дані, які використовуються для створення електронного підпису і не повинні бути доступні іншим особам
5	КЕП (кваліфікований електронний підпис)	E.	процедура, яка встановлює: (1) що підпис математично відповідає даним документа і відкритому ключу, (2) що сертифікат підписувача чинний на
6	Закритий ключ підпису	F.	удосконалений електронний підпис, який створений кваліфікованим засобом і ґрунтується на кваліфікованому сертифікаті підписувача
7	Відкритий ключ перевірки	G.	коротке значення, отримане застосуванням криптографічної хеш-функції до даних документа; використовується як "відбиток" документа для підписання/перевірки цілісності.
8	Сертифікат відкритого ключа	H.	інформація в електронній формі (файл або набір файлів), яка містить зміст і дані для ідентифікації документа (наприклад: назва/номер/дата/автор/версія)
9	Криптографічний хеш документа	I.	криптографічні дані, які використовуються для перевірки підпису; математично пов'язані із закритим ключем, але не дозволяють відновити закритий ключ
10	Перевірка електронного підпису (валідація)	J.	електронні дані, що додаються до документа або логічно з ним пов'язуються і використовуються підписувачем для підписання документа

Порада: якщо змінити документ після підписання, перевірка повинна показати помилку цілісності.