

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»



**Факультет інформаційних технологій
Кафедра системного аналізу та управління**

Звіт

з практичної роботи №1 з дисципліни
«Аналіз програмного забезпечення»

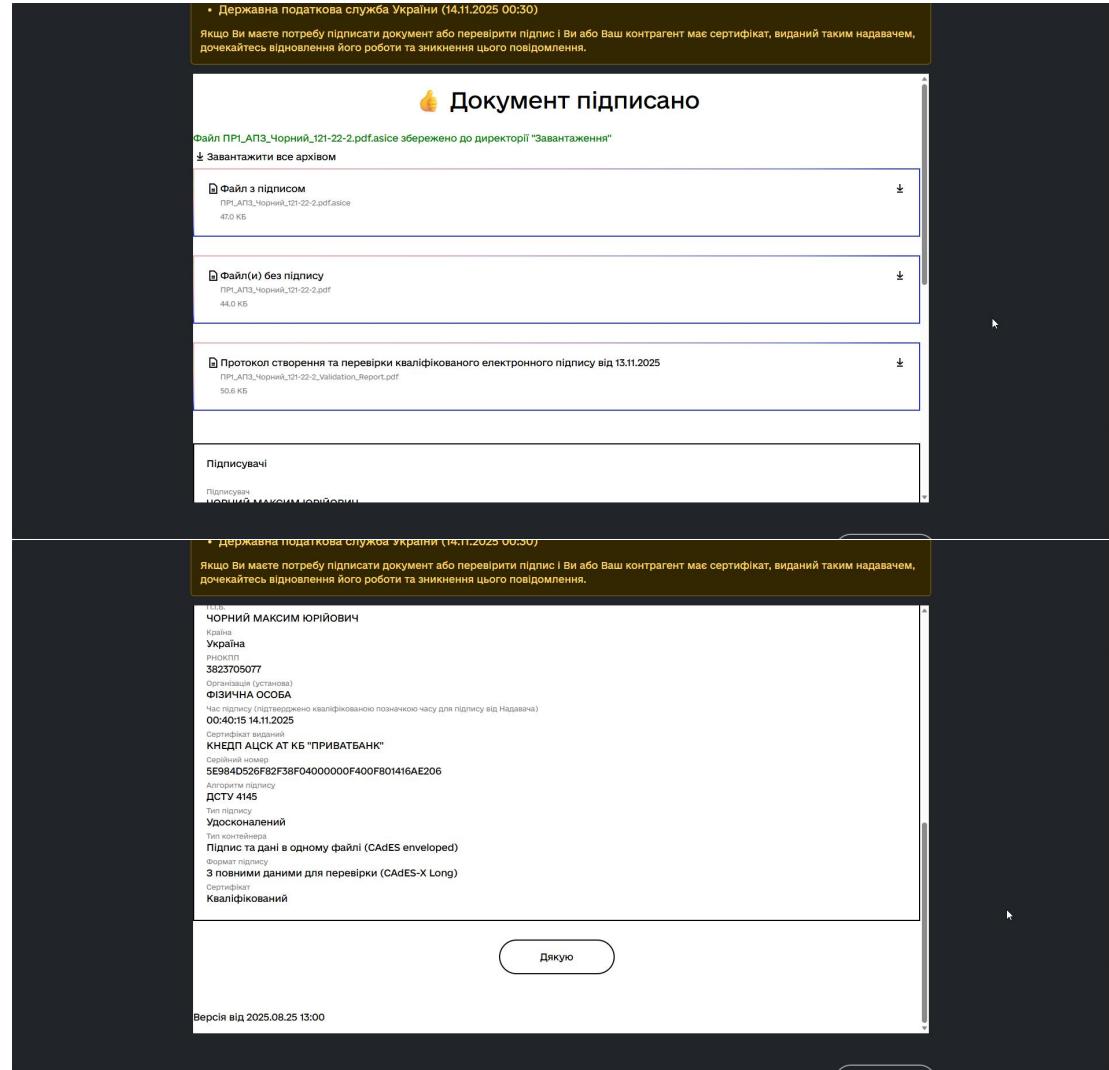
Виконала:
студент групи 121-22-2
Чорний М.Ю.
Перевірили:
доц. Мінєєв О.С.
ас. Шевченко Ю.О.

**Дніпро
2025**

Тема: Підписання персонального документа за допомогою кваліфікованого

електронного підпису (КЕП).

Мета: Набування навичок підписання особистої документації з використанням кваліфікованого електронного підпису.



Контрольні запитання:

1. Що таке ЕЦП?

Електронний цифровий підпис (ЕЦП) - це вид електронного підпису, отриманий внаслідок криптографічного перетворення набору електронних даних. Він додається до інших електронних даних (основного документа) або логічно з ними пов'язується. ЕЦП слугує для двох основних цілей:

- 1) Ідентифікація підписувача: Підтвердження особи, яка створила підпис.
- 2) Забезпечення цілісності даних: Гарантія того, що в підписаний документ не вносилися зміни після його підписання.

2. Навіщо використовують КЕП?

Кваліфікований електронний підпис (КЕП) - це вдосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису та базується на кваліфікованому сертифікаті відкритого ключа.

Основна мета використання КЕП - надання електронним документам юридичної сили, рівнозначної власноручному підпису на паперових носіях. Він забезпечує найвищий рівень довіри та автентифікації, що є критичним для:

- 1) Взаємодії з державними електронними сервісами (наприклад "Дія", електронний кабінет платника податків).
- 2) Подання офіційної звітності до контролюючих органів.
- 3) Укладання юридично значущих договорів та ведення електронного документообігу.

3. Які сервіси і застосунки використовуються для створення ЕЦП?

Отримання сертифікатів ключів для ЕЦП (зокрема КЕП) здійснюється через Кваліфікованих надавачів електронних довірчих послуг (КНЕДП), які раніше називалися Акредитованими центрами сертифікації ключів (АЦСК).

Найпоширеніші способи отримання КЕП для фізичних та юридичних осіб:

- 1) Інтегровані державні сервіси: Наприклад, генерація "Дія.Підпис" безпосередньо у мобільному застосунку "Дія".
- 2) Системи інтернет-банкінгу: Багато банків (як-от ПриватБанк, Монобанк та інші) надають послугу генерації КЕП для своїх клієнтів онлайн.
- 3) Сервіси державних органів: Наприклад, КНЕДП Інформаційно-довідкового департаменту ДПС України.
- 4) Комерційні КНЕДП: Спеціалізовані організації, що надають повний спектр довірчих послуг (наприклад, "Вчасно", АЦСК "Україна" тощо).

4. Який формат має документ після підписання ЕЦП?

Формат файлу після накладання підпису залежить від обраного типу підпису - чи він приєднується до файлу, чи зберігається окремо:

- 1) Зовнішній підпис (Detached signature): Це найпоширеніший варіант, при якому створюється окремий файл підпису. Для перевірки такого підпису необхідно мати два файли: оригінальний документ (наприклад, договір.doc) та файл підпису (договір.doc.p7s).

- 2) Внутрішній підпис (Attached signature) / Контейнер: Документ та один або декілька підписів запаковуються в єдиний файл-контейнер. Поширеним форматом для цього є .asice (Associated Signature Containers).
- 3) Інтегрований підпис: Для деяких форматів, зокрема PDF, підпис може бути вбудований безпосередньо в структуру самого PDF-файлу (згідно зі стандартом PAdES), при цьому розширення файла не змінюється.