Копішинська Олена Петрівна1, к. ф.-м. н., доцент

Хоменко Світлана Олегівна2, магістрант

1,2Полтавський державний аграрний університет, м. Полтава

1ORCID ID [0000-0002-3138-7215](http://orcid.org/0000-0002-3138-7215)

**УДОСКОНАЛЕННЯ КЛЮЧІВ ЦИФРОВОГО ЕЛЕКТРОННОГО ПІДПИСУ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ**

В умовах інформатизації суспільного життя цифрові технології стають неодмінними атрибутами повсякденної діяльності кожної людини. Динаміка впровадження цифрових образів об’єктів матеріального світу й оперування ними помітно зросла за 2020-2021 рр. пандемії, під час повномасштабної війни в Україні 2022-2023 рр. Інформаційні системи та технології грають ключову роль у забезпеченні комунікацій між людьми, організаціями в штатних і непередбачуваних умовах, допомагають зберігати й передавати, обробляти величезні обсяги як особистих, так і комерційних, державних даних.

Серед багатьох інновацій, впроваджених в діяльність приватних, державних підприємств та організацій, фінансових установ особливу увагу приділяють системам електронного документообігу (ЕДО), засобам захисту даних, юридичному підтвердженню електронних документів (ЕД) [1]. ЕД – документ, створений за допомогою засобів комп’ютерної обробки даних, підписаний кваліфікованим електронним підписом (КЕП) і збережений на машинних носіях у вигляді відповідного файлу.

Сутність, значимість та складність отримання й використання електронних цифрових підписів (ЕЦП) пройшла кілька етапів удосконалення. Оскільки використовують цифрові підписи все частіше і фізичні особи, і підприємці, і державні службовці, то доцільним є структурування уявлень про особливості таких інструментів надання юридичної значимості документів. Терміни КЕП та удосконалений електронний підпис (УЕП) – це підписи на різних носіях із різними рівнями захисту. Названі ключі працюють відповідно до Закону України «Про електронні довірчі послуги» [2], але реалізуються за допомогою різних механізмів (рис. 1).



Рис. 1. Класифікація електронних підписів та відповідних носіїв

УЕП — це ключ старого зразка, він має вигляд звичайного файлового носія, захищеного лише приватним паролем. Цей файл може зберігатися у вас на комп’ютері, флешці, телефоні тощо – тобто на будь-якому цифровому носії. Даний ключ має найменший рівень захисту. Тому все більше підприємців відмовляються від УЕП.

КЕП – більш досконалий та сучасний (якщо говорити про хмарні КЕП) варіант електронного підпису, адже має найвищий рівень захисту і зберігається лише на захищених носіях – хмара або токен, не має обмежень у підписанні електронної документації. Таким чином, це рішення є пріоритетним на сьогодні для багатьох підприємців. Окремі аспекти використання КЕП наведено в табл. 1.

Таблиця 1 – Переваги використання КЕП для різних груп підписантів

|  |  |
| --- | --- |
| Користувачі електронного підпису КЕП | Характер, переваги і особливості використання |
| Юридична особа | •Швидке підписання юридичних та фінансових документів, подання звітності в державні органи;  •Зручне управління - створення нових електронних ключів для співробітників, оновлення та відкликання підписів;  •Використання хмарного електронного підпису онлайн економить час і кошти |
| Фізична особа | •Підписання електронних документів в один клік  •Зручний доступ з електронних пристроїв  •Проста процедура авторизації  •Немає ризику втрати особистого ключа |

КЕП – це удосконалений цифровий електронний підпис, що прийшов на зміну ЕЦП. Він створений на основі кваліфікованого цифрового сертифіката відкритого ключа і має найвищий рівень захисту. Електронний обіг з державними органами складається з електронної звітності, яка підписується з використанням КЕП. Отримати його можуть як фізичні, так і юридичні особи.

Електронний підпис може зберігатися у вигляді токена (апаратний КЕП) або у хмарному сховищі (див. рис. 1) на сервері надавача довірчих послуг (хмарний КЕП). Хмарний носій – мобільний, надійний. За його допомогою можна підписувати будь-який тип документа, в контрагентів питань не виникне.

Апаратний носій, він же токен, - також надійний і відноситься до КЕП, але без цінної мобільності, адже ви прив’язані до фізичного носія.

Файловий носій вважається носієм із найменшим рівнем захисту, можна використовувати для каси і для підпису первинної документації, але контрагент може не прийняти даний підпис і попросити підписати документи саме КЕП.

Отже, хмарний КЕП – найбільш удосконалена альтернатива файловим ключам та токенам і має суттєві переваги за наступними ознаками:

1. Зручність – можна створити зі смартфона, планшета чи ноутбука з будь-якої точки світу.
2. Вигідно – хмарний КЕП дешевший за апаратний, отже зменшує витрати.
3. Безпечний – особистий ключ зберігається в захищеному хмарному сховищі на сервері надавача довірчих послуг.
4. Надійність – хмарний електронний ключ доступний 24/7. Його неможливо загубити, вкрасти чи скопіювати.

Як правило, компанії, що поставляють системи ЕДО, все більше надають в комплексі різні види КЕП, особливо у вигляді токенів або хмарних сервісів . Звичайний ЕЦП фізичні або юридичні особи можуть замовити на порталах зареєстрованих надавачів послуг, наприклад, в АК «Приватбанк».

**Література**

1. Ситник І. П., Мельниченко А. І. Системи електронного документообігу в електронному бізнесі. *Науковий вісник Ужгородського національного університету*. 2015. №4. С. 174-178.
2. Про електронні довірчі послуги: Закон України. Відомості Верховної Ради (ВВР), 2017, № 45, ст.400.