МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

РАРОГА ДМИТРО ІВАНОВИЧ

Допускається до захисту:
завідувач кафедри інформаційних систем управління
д-р. екон. наук, професор
_____ О.М. Анісімова
«____»_____ 20___ р.

ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС У ДОКУМЕНТАХ

Спеціальність 029 Інформаційна, бібліотечна та архівна справа

Кваліфікаційна (бакалаврська) робота

Керівник:
Ковальська Л.А., професор кафедри
інформаційних систем управління
д-р істор. наук, доцент

Оцінка: ____ / ___ / _____
(бали / за шкалою ЄКТS / за національною шкалою)
Голова ЕК: _____
(підпис)

Вінниця – 2021

АНОТАЦІЯ

Рарога Д.І. Електронний цифровий підпис у документах. Спеціальність 029 «Інформаційна, бібліотечна та архівна справа». Донецький національний університет імені Василя Стуса, 2021.

Наведено визначення поняття електронний цифровий підпис та проаналізовано його змістову сторону. Досліджено атрибуцію застосування реквізиту цифрового підпису й особливості функціонування, встановлено його юридичну силу та можливості безпеки інформації документа. Розкрито особливості впровадження електронного цифрового підпису в документообіг та показано варіативність механізмів підпису різних форматів електронного документа. Наведено переваги використання електронного цифрового підпису в документах. Висвітлено зміст криптографічного перетворення інформації з використанням закритого ключа підпису. **Ключові слова**: документ, електронний документ, електронний цифровий підпис, криптографічний захист, електронний документообіг.

Рис. 20. Бібліограф.: 50 найменувань.

Raroga D.I. Electronic digital signature in documents. Specialty 029 «Information, library and archivna on the right». Donetsk National University named after Vasyl Stus, 2021.

The definition of the concept of electronic digital signature is given and its content is analyzed. The attribution of application of digital signature requisites and peculiarities of functioning are investigated, its legal force and possibilities of document information security are established. The peculiarities of introduction of electronic digital signature in document circulation are revealed and the variability of signature mechanisms of different formats of electronic document is shown. The advantages of using an electronic digital signature in documents are given. The content of cryptographic transformation of information using the private key of the signature is covered. **Key words:** document, electronic document, electronic digital signature, cryptographic protection, electronic document management.

Fig. 20. Bibliographer.: 50 items..

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Згідно з вимогами документообігу та використання документованої інформації відомо, що для того щоб документ став дійсним, він повинен бути підписаний. Далі підпис засвідчується печаткою організації, зареєстрованої в державних реєстрах, або підписом іншої особи – нотаріуса, якого уповноважено відповідними органами завіряти підписи. Але відомо, що підпис і печатку можна підробити. Особливо це питання актуалізується в умовах розвитку сучасного віртуального простору, обігу документів і техніко-технологічних можливостей втручання у документообіг.

В сучасному світі більшість документів це одиниці інформації, що пересилаються між серверами, які можуть перебувати де завгодно. Постає потреба довести одержувачу автентичність цих документів / підтвердити автора, як адресат може перевірити, що отримана ним інформацію не спотворена / не порушена її цілісність. Для цього і призначено електронний цифровий підпис (далі ЕЦП). Захист цифрового підпису набагато кращий ніж звичайний підпис та печатка, і не тільки авторитетом компаній, які ідентифікують власника ключа для шифрування інформації, але й міццю математичних алгоритмів, завдяки яким ЕЦП реалізується. Отримання документа, підписаного ЕЦП означає, що разом з документом отримано зашифрований (закритий ключем) результат (хеш) застосування хеш-функції над підписаним документом і відкритий ключ для розшифровки цього хешу.

Впровадження в документообіг ЕЦП відбувається впевнено але повільно, що викликає потребу роз’яснення користувачам специфіки електронного цифрового підпису документа і зумовлено питаннями реалізації такої функції та можливостями обігу інформації засвідченої подібним чином.

Мета дослідження: розкрити особливості отримання та використання в роботі з документами електронного цифрового підпису.

Реалізація мети передбачає послідовне вирішення наступних **завдань:**

- вивчити змістові характеристики поняття електронний цифровий підпис;

- показати переваги використання електронного цифрового підпису в документах;

- обстежити правовий статус цифрового підпису;

- проаналізувати становлення українського законодавства про цифровий підпис;

- висвітлити специфіку криптографічного перетворення інформації з використанням закритого ключа підпису;

- розглянути особливості функціонування цифрового підпису;

- продемонструвати варіативність механізму використання електронного цифрового підпису в електронних документах;

- конкретизувати специфіку регулювання використання електронного цифрового підпису.

Об'єктом дослідження є електронний цифровий підпис як засіб ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Предметом дослідження є нормативне регулювання та функціональні можливості електронного цифрового підпису як засобу ідентифікації особи-підписувача електронного документа.

Структура кваліфікаційної (бакалаврської) роботи визначена метою і завданнями та складається із вступу, трьох розділів восьми підрозділів, висновків, списку використаних посилань, додатків. Список використаних посилань включає 50 найменувань. Робота викладена на 57 сторінках друкованого тексту, основна частина якої становить 50 сторінки.

РОЗДІЛ 1
ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС В СИСТЕМІ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

1.1. Основний зміст електронного цифрового підпису та електронного документа

Електронним цифровим підписом називають дані в електронній формі, які ідентифікують власника. ЕЦП містить інформацію – ПІБ, ідентифікаційний код платника податків, дата народження, адреса електронної пошти, номер телефону. Електронний підпис не є аналогом фізичного підпису, який звикли бачити в документах. Це персональний файл з електронним ключем, дані якого надійно зашифровані. Що стосується юридичного аспекту – і фізичний підпис, і ЕЦП по закону мають однакову силу. ЕЦП містить закритий (приватний) ключ, його необхідно зберігати в таємниці, щоб уникнути підробок підписів електронних документів. Він завжди працює в парі з відкритим (публічним) ключем, за допомогою якого і перевіряється справжність ЕЦП.

Рис 1.1. – Електронний цифровий підпис у документі

Електронний цифровий підпис – це блок інформації, який прикріпляється до файлу даних автором і захищає файл від несанкціонованої модифікації та

вказує на власника підпису, використовується фізичними та юридичними особами як аналог власноручного підпису для надання електронному документу юридичної сили, відповідає юридичній силі документа на паперовому носії, підписаного власноручним підписом правомочної особи, та скріпленого печаткою. Електронний підпис – це «дані, подані в електронній формі, які додаються чи логічно поєднуються з іншими електронними даними та які служать в якості методу засвідчення достовірності».

«Удосконалений електронний підпис», що означає електронний підпис, який відповідає певним вимогам, а саме, знаходиться під повним контролем особи, яка його ставить, і пов'язаний винятково із цією особою, дозволяє за підписом ідентифікувати особу і пов'язаний з даними таким чином, що будь-яку зміну даних після додавання підпису можна виявити.

Електронний цифровий підпис є якісно новим етапом розвитку сучасного документообігу. Використання електронного цифрового підпису в системі електронного документообігу здатне прискорити проведення численних комерційних операцій, скоротити об'єми паперової бухгалтерської документації, економить час співробітників і витрати підприємства, пов'язані з укладенням договорів, оформленням платіжних документів, наданням звітності в контролюючі органи, отриманням довідок від різних держустанов. Підробити ЕЦП, створений акредитованим сертифікаційним центром, неможливо [2].

Метою застосування систем цифрового підпису є автентифікація інформації – захист учасників інформаційного обміну від нав'язування хибної інформації, встановлення факту модифікації інформації, яка передається або зберігається, й отримання гарантії її справжності, а також вирішення питання про авторство повідомлень. Система цифрового підпису припускає, що кожен користувач мережі має свій таємний ключ, який використовується для формування підпису, а також відповідний цьому таємному ключу відкритий ключ, відомий решті користувачів мережі й призначений для перевірки підпису. Цифровий підпис обчислюється на основі таємного ключа відправника інформації й власне інформаційних бітів документу (файлу). Один з

користувачів може бути обраним в якості «нотаріуса» й завіряти за допомогою свого таємного ключа будь-які документи. Решта користувачів можуть провести верифікацію його підпису, тобто пересвідчитися у справжності отриманого документу. Спосіб обчислення цифрового підпису такий, що знання відкритого ключа не може призвести до підробки підпису. Перевірити підпис може будь-який користувач, що має відкритий ключ, в тому числі незалежний арбітр, якого уповноважено вирішувати можливі суперечки про авторство повідомлення (документу).

Електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Електронний документ може бути створений, переданий, збережений і переведений електронними засобами у візуальну форму.

Законом України «Про електронні документи та електронний документообіг» встановлено організаційно-правові засади електронного документообігу та використання електронних документів. Так, електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, зокрема електронний цифровий підпис (ст. 5). Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму [1]. Проте Закон встановлює певні обмеження на застосування електронного документа як оригіналу. В електронній формі не може бути створено оригінал свідоцтва про право на спадщину; інший документ, який згідно із законодавством може бути створений лише в одному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів (ст. 8 Закону).

Обов'язковим реквізитом електронного документа є електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору, або логічно з ним поєднується, і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис

накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа (ст. 1 Закону «Про електронний цифровий підпис») [2].

Особистий ключ відомий лише його володільцеві. Відкритий ключ доступний всім учасникам електронного документообігу. Такий ключ включається до сертифіката відкритого ключа та може розповсюджуватись в електронній формі або у формі документа на папері.

Засвідчення чинності відкритого ключа здійснюється шляхом формування сертифіката відкритого ключа – документа, що видається центром сертифікації ключів. Посилений сертифікат відкритого ключа видається акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом. Зазначена особливість дає можливість поряд із звичайним електронним цифровим підписом виділити цифровий підпис, підтверджений посиленим сертифікатом відкритого ключа.

Сертифікат відкритого ключа містить :

– найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);

– позначку, що сертифікат виданий в Україні;

– унікальний реєстраційний номер сертифіката ключа;

– основні дані (реквізити) підписувала-власника особистого ключа;

– дату і час початку та закінчення строку чинності сертифіката;

– відкритий ключ;

– найменування криптографічного алгоритму, що використовується власником особистого ключа;

– інформацію про обмеження використання підпису [27].

Посилений сертифікат відкритого ключа, крім обов’язкових даних, які містяться в сертифікаті відкритого ключа, повинен мати ознаку посиленого сертифіката відкритого ключа. Інші дані можуть вноситися у посилений сертифікат ключа на вимогу його власника

Юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом відкритого ключа, а також

використовувати електронний цифровий підпис без сертифіката відкритого ключа. Розподіл ризиків збитків, що можуть бути заподіяні підписувачам, користувачам та третім особам, які застосовують електронні цифрові підписи без сертифіката відкритого ключа, визначається суб'єктами правових відносин у сфері послуг електронного цифрового підпису на договірних засадах.

Щодо органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій державної форми власності, то для них законодавець встановив імперативну (обов'язкову) норму, згідно з якою зазначені організації можуть застосовувати електронний цифровий підпис лише за умови використання надійних засобів електронного цифрового підпису, що повинно бути підтверджено сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, отриманим на ці засоби від спеціально уповноваженого центрального органу виконавчої влади у сфері криптографічного захисту інформації, та наявності посилених сертифікатів відкритих ключів у своїх працівників-підписувачів [10].

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) лише в тому разі, якщо:

– електронний цифровий підпис підтверджено з використанням посиленого сертифіката відкритого ключа за допомогою надійних засобів цифрового підпису.

Для порівняння: у Німеччині, за законодавством, електронний цифровий підпис не прирівнюють до власноручного підпису; у Франції, навпаки, згідно зі статтею 1316 Цивільного кодексу, сторонам надається право вибору, оскільки в суді як докази визнаються (допускаються) літери та цифри чи будь-який інший знак або символ, значення (зміст) якого може бути з'ясовано незалежно від способу створення та передачі.

Підробити електронний цифровий підпис, а разом з ним і засвідчений документ неможливо, адже це потребуватиме величезної кількості обчислень, які, як вважається, не можуть бути реалізовані за сучасного рівня математики й

обчислювальної техніки за прийнятний час, тобто поки інформація, що міститься в підписаному документі, є актуальною. Додатковий захист від підробки забезпечує центр сертифікації, який серед іншого цілодобово приймає заяви про скасування, блокування та поновлення сертифікатів ключів.

1.2. Переваги електронного цифрового підпису в документообігу

Електронний цифровий підпис може використовуватися юридичними і фізичними особами як аналог власноручного підпису для надання електронному документу юридичної сили. Юридична сила електронного документа, підписаного ЕЦП, еквівалентна юридичній силі документа на паперовому носієві, підписаного власноручним підписом правомочної особи та скріпленого печаткою.

Електронний цифровий підпис володіє всіма основними функціями власноручного підпису:

– засвідчує те, що отриманий документ надійшов від особи, що підписала його;

– гарантує цілісність і захист від виправлень підписаного документа;

– не дає можливості особі, яка підписала документ, відмовитися від зобов'язань, що виникли в результаті підписання цього електронного документа [25].

Безпека використання ЕЦП забезпечується тим, що засоби, які використовуються для роботи з ЕЦП, проходять експертизу і сертифікацію в Департаменті спеціальних телекомунікаційних систем СБУ, яка гарантує неможливість зламу і підробки ЕЦП.

Переваги ЕЦП:

– юридична сила електронних документів, підписаних ЕЦП, законами України прирівнюється до юридичної сили документів з власноручним підписом або друком, а також створює правову основу для застосування ЕЦП і здійснення юридично значущих дій шляхом електронного документообігу;

– конфіденційність і безпека інформації. Використовуючи ЕЦП, користувач дістає додаткову можливість шифрування документів. Завдяки надійним криптографічним алгоритмам забезпечується конфіденційність інформації, яка має на увазі неможливість доступу до неї будь-якої особи;

– безпека використання ЕЦП забезпечується тим, що програмне забезпечення, яке використовується для роботи з ЕЦП, пройшло експертизу і сертифікацію в Департаменті спеціальних телекомунікаційних систем СБУ, яка гарантує неможливість зламу і підробки ЕЦП;

– можливість ведення електронного документообігу з державними структурами та можливість використовувати одні і ті ж засоби ЕЦП при обміні даними зі всіма міністерствами, відомствами, при подачі звітності до будь-яких контролюючих органів на території України;

– удосконалення бізнес-процесів на підприємстві істотно скорочує об’єми паперової бухгалтерської документації, економить час співробітників і витрати підприємства, пов’язані з укладенням договорів, оформленням платіжних документів;

– ведення ділових відносин на сучасному рівні використання ЕЦП істотно прискорює проведення численних комерційних операцій, виключає необхідність додаткових зустрічей і багатогодинних переговорів;

– електронний цифровий підпис – ефективне рішення для всіх, хто хоче йти в ногу з новими вимогами часу. Документи, підписані електронним цифровим підписом, можуть бути передані до місця призначення протягом декількох секунд. Всі учасники електронного обміну документами дістають рівні можливості незалежно від їх віддаленості один від одного [15].

Електронний документообіг (оборот електронних документів) – сукупність процесів створення, обробки, відправки, передачі, отримання, збереження, використання і знищення електронних документів, які відбуваються із застосуванням перевірки цілісності і, у разі потреби, з підтвердженням факту отримання таких документів.

В Законі «Про електронні документи та електронний документообіг» указується, що обов'язковим реквізитом електронного документа є електронний цифровий підпис, який використовується для ідентифікації автора і/або підписувача електронного документа іншими суб'єктами електронного документообігу. Накладенням електронного підпису закінчується створення електронного документа [1].

При підписанні електронного документа його початковий зміст не змінюється, а додається блок даних – електронний цифровий підпис.

Отримання цього блоку можна розділити на два етапи:

- На першому етапі за допомогою програмного забезпечення і спеціальної математичної функції обчислюється так званий «відбиток повідомлення» (message digest). Цей відбиток має наступні особливості: фіксовану довжину, незалежно від довжини повідомлення; унікальність відбитку для кожного повідомлення; неможливість відновлення повідомлення по його відбитку. Таким чином, якщо документ був модифікований, то зміниться і його відбиток, який відобразиться при перевірці електронного цифрового підпису.
- На другому етапі відбиток документа шифрується за допомогою програмного забезпечення і особистого ключа автора. Таким чином, обчислення відбитку документа захищає його від модифікації сторонніми особами після підписання, а шифровка особистим ключем автора підтверджує авторство документа.

Переваги використання електронного документообігу:

– перехід до зручнішого, швидшого і економнішого безпаперового документообігу;

– удосконалення процедури підготовки, подачі / передачі / доставки, обліку і збереження документів, їх аутентифікація, цілісність, конфіденційність і неспростовність;

– криптографічний захист інформації (електронних документів) при їх передачі відкритими каналами;

– мінімізація фінансових ризиків за рахунок підвищення конфіденційності інформаційного обміну документами;

– економія ресурсів за рахунок використання оперативного електронного архіву.

Процедура підписання електронного документа з використанням ЕЦП включає в себе наступні дії. Для прикладу розглянемо підписання документа на сайті Міністерства цифрової трансформації України:

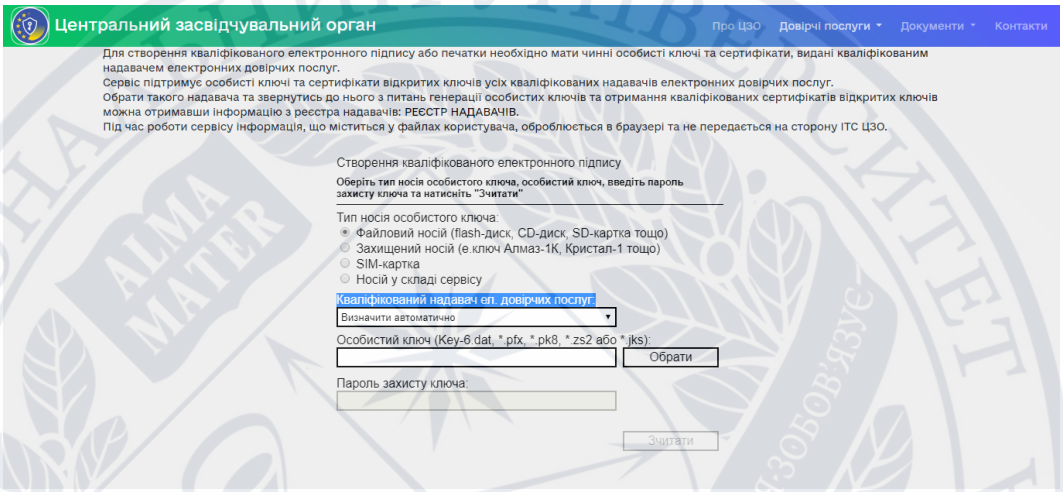


Рисунок 1.2. – Підписання електронного документа

1. відкрийте ваш інтернет-браузер і перейдіть за посиланням http://czo.gov.ua/sign
2. оберіть тип носія приватного ключа, кваліфікованого представника електронних довірчих послуг.
3. прикріпіть свій приватний ключ.
4. введіть свій пароль і натисніть кнопку «Зчитати».
5. у вікні, оберіть документ, який необхідно підписати.
6. натисніть кнопку «Підписати».
7. збережіть підписаний файл за допомогою кнопки «Зберегти».

Для юридичних осіб та ФОП, які працюють без печатки, підписання документу за допомогою ЕЦП буде достатньо.

Як перевірити ЕЦП на справжність

Для того щоб перевірити отриманий ЕЦП, потрібно перейти за посиланням https://czo.gov.ua/verify і перетягнути або обрати потрібний файл для перевірки.

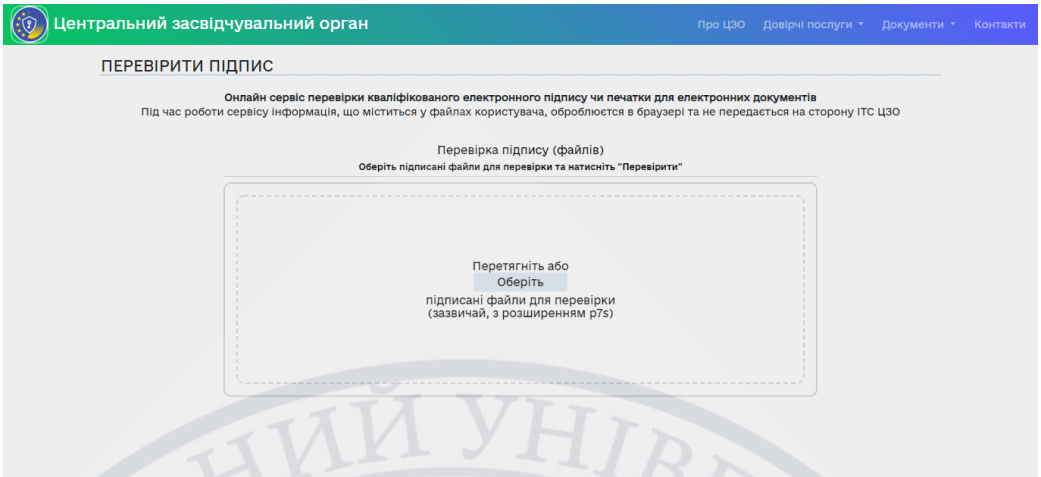


Рисунок 1.3. – Перевірка отриманого електронного цифрового підпису

На порталі Дія можна онлайн підписати документ за допомогою електронного підпису. Зміст підписуваного документа нікуди не передається. Він залишається у браузері, тому конфіденційність не може бути порушена. Використання електронних документів дозволено законодавством України.

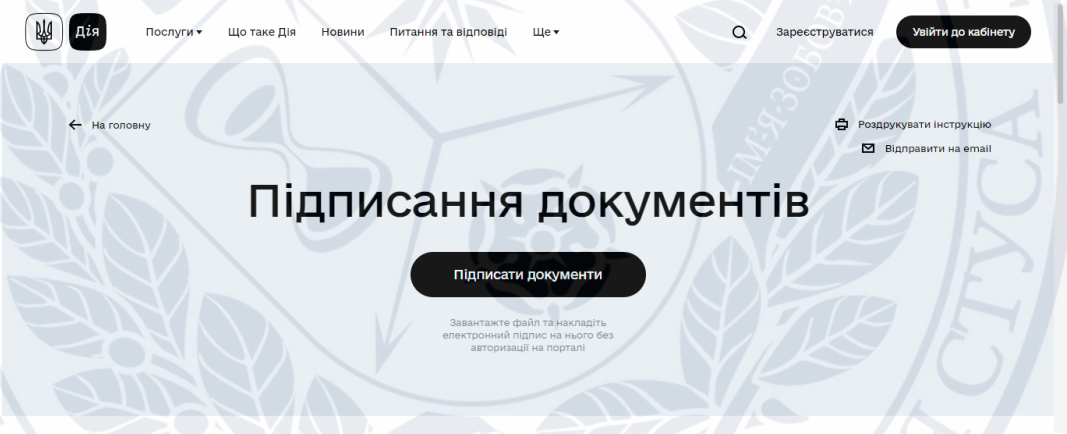


Рисунок 1.4. – Послуги електронного цифрового підписування документів на порталі Дія

Для цього потрібні чинні особисті ключі та сертифікати, видані кваліфікованим надавачем електронних довірчих послуг. Далі слід обрати тип носія особистого ключа: файловий носій (flash-диск, CD-диск, SD-картка тощо) або захищений носій (Алмаз-1К, Кристал-1 тощо). Ввести пароль та натиснути кнопку «Зчитати ключ».

Далі постає питання перевірки підпису. Тут можна розглянути наступний алгоритм на порталі Дія:

1. перейдіть за посиланням «Перевірити підпис».

2. перетягніть у браузер або виберіть на своєму носії файл з підписом у форматі .p7s. Натисніть кнопку «Перевірити».

3. портал видасть інформацію про накладені підписи.

4. можна завантажити оригінальний файл, на який було накладено підпис, та ознайомитись з його змістом. Для цього натисніть кнопку «Зберегти файл».

5. щоб завантажити підтвердження перевірки підпису, натисніть кнопку «Завантажити квитанцію».

Отже, електронний цифровий підпис отримується в акредитованих центрах сертифікації ключів (АЦСК), перелік яких можна знайти на сайті Міністерства цифрової трансформації України. Підписання документів ЕЦП є найнадійнішим способом ідентифікації підписувача та фіксації волевиявлення. Окрім підписання документів ЕЦП, на практиці можуть використовувати скановані документи зі зразками підписів та печаток; простий текстовий підпис в електронному листі; погодження з договором (офертою) може відбуватися шляхом проставлення відповідного «прапорця», «галочки» на веб-сайті.

РОЗДІЛ 2
ОСОБЛИВОСТІ ЗАСТОСУВАННЯ РЕКВІЗИТУ ЦИФРОВОГО ПІДПИСУ

2.1. Електронний цифровий підпис і його правовий статус

У 1976 році Уітфілдом Діффі і Мартіном Хеллманом було вперше запропоновано поняття «електронний цифровий підпис», хоча вони всього лише припускали, що схеми ЕЦП можуть існувати.

У 1977 році Рональд Ривест, Аді Шамір і Леонард Адлеман розробили криптографічний алгоритм RSA, який без додаткових модифікацій можна використовувати для створення примітивних цифрових підписів. Незабаром після RSA були розроблені інші ЕЦП, такі, як алгоритми цифрового підпису Рабина, Меркле.

У 1984 році Шафи Гольдвассер , Сільвіо Мікалі і Рональд Ривест першими строго визначили вимоги безпеки до алгоритмів цифрового підпису. Ними були описані моделі атак на алгоритми ЕЦП, а також запропонована схема GMR, що відповідає описаним вимогам (Криптосистема Гольдвассер - Мікалі).

Електронний цифровий підпис (ЕЦП) – вид підпису, що надає можливість здійснювати підпис документів в електронній формі. Фактично це електронний файл з набором зашифрованих даних для ідентифікації підписанта.

Закон України «Про електронні довірчі послуги» визначає електронний підпис як електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов’язуються і використовуються ним як підпис. Закон України «Про електронні документи та електронний документообіг», визначає правову природу електронного документу та закріплює, що юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму [2].

Існує кілька схем побудови цифрового підпису:

На основі алгоритмів симетричного шифрування. Дана схема передбачає наявність у системі третьої особи – арбітра, що користується довірою обох

сторін. Авторизацією документа є сам факт шифрування його секретним ключем і передача його арбітра.

На основі алгоритмів асиметричного шифрування. На даний момент такі схеми електронного підпису найбільш поширені і знаходять широке застосування. Крім цього, існують інші різновиди цифрових підписів (груповий підпис, незаперечний підпис, довірений підпис), які є модифікаціями описаних вище схем. Їх поява обумовлена різноманітністю завдань, що вирішуються за допомогою електронного підпису.

Електронно-цифровий підпис – реквізит електронного документа, отриманий внаслідок перетворення інформації з використанням закритого ключа електронно-цифрового підпису і що дозволяє встановити автентичність і цілісність інформації, що міститься в електронному документі, а також володаря електронно-цифрового підпису. Електронно-цифровий підпис в електронному документі стає рівнозначним власноручному підпису при наступних умовах:

- сертифікат ключа електронно-цифрового підпису не втратив силу;
- підтверджена автентичність електронно-цифрового підпису в електронному документі;
- електронно-цифровий підпис використовується у відносинах, що мають юридичне значення;

Суб’єктами електронно-цифрового підпису виступають:

- користувачі інформаційної системи;
- володарі електронно-цифрового підпису;
- засвідчуючі центри;
- уповноважені органи;

Електронний цифровий підпис - це сучасний, надійний юридичний інструмент, що дозволяє практично вмить, незалежно від часу діб і відстаней, укласти юридично повноцінну операцію, а також у разі необхідності однозначно і без сумнівів вирішити самі різноманітні спори, в тому числі і в судовому порядку.

Електронне повідомлення, підписане електронним цифровим підписом або інакшим аналогом власноручного підпису, визнається електронним документом, рівнозначним документу, підписаному власноручним підписом, у випадках, якщо законами або інакшими нормативними правовими актами не встановлюється або не мається на увазі вимога про складання такого документа на паперовому носії.

З метою висновку цивільно-правових договорів або оформлення інакших правовідносин, в яких беруть участь особи, що обмінюються електронними повідомленнями, обмін електронними повідомленнями, кожне з яких підписане ЕЦП або іншим аналогом власноручного підпису відправника такого повідомлення, в порядку, встановленому законами, іншими нормативними правовими актами або угодою сторін, розглядається як обмін документами.

ЕЦП – це програмно-криптографічний (тобто зашифрований відповідним чином) засіб, який дозволяє підтвердити, що підпис, який стоїть на тому або іншому електронному документі, поставлений саме його автором, а не якою-небудь іншою особою [7].

Для автора документа генерується закритий ключ – послідовність цифр певної довжини. Будь-який електронний документ з технічної точки зору також являє собою послідовність цифр. ЕЦП це деяке число, отримане внаслідок перетворення електронного документа як цифрової послідовності за допомогою закритого ключа автора. На базі закритого ключа створюється відкритий ключ, доступний будь-якому. Будь-хто може перевірити ЕЦП під документом за допомогою відповідних перетворень з використанням електронного зразка документа, відкритого ключа відправника і власне значення ЕЦП. Відкритий і закритий ключі однозначно пов’язані між собою, однак обчислити закритий ключ за відкритим практично неможливо; як мінімум, це вимагає дуже тривалого періоду часу.

Закритий ключ, зрозуміло, міститься в таємниці і відомий тільки власнику, щоб ніхто, крім власника, не зміг сформувати ЕЦП під документом. У той же час буквально будь-яка зацікавлена особа може перевірити за допомогою

опублікованого відкритого ключа, що документ підписав саме власник, що документ не спотворений (інакше міняється похідна величина). Таким чином, підробити електронний документ, підписаний ЕЦП, істотно складніше, ніж документ на паперовому носії. Захищеним є і сам текст документа, причому не потрібно допомоги експертів для виявлення факту спотворення документа. Перевірка здійснюється суворо математичним шляхом, автоматично, не треба проробляти які-небудь обчислення. Внаслідок запуску програми відкритого ключа користувач отримує результати перевірки в наочному вигляді як повідомлення про те, що документ підписаний особою, можливо й деякі інші додаткові дані. Або отримує негативний результат [9].

Однак в деяких країнах сфера застосування ЕЦП набагато ширше і визначається методом виключення. Наприклад, в США згідно з Законом про електронні підписи в світовій і національній торгівлі (Electronic Signatures in Global and national Commerce Act), відомим як Закон про електронний підпис (E-Sign Act), що набрав чинності 1 жовтня 2000 р., будь-який контракт, угода, документ, заставна або інша форма документа, що стосується нерухомості, або будь-який інший діловий документ може бути підписаний за допомогою електронного підпису.

2.2. Становлення українського законодавства про цифровий підпис

У XXI ст. інформаційно-комунікаційні технології стають провідним чинником, що істотно впливає на розвиток суспільства. Багато країн уже усвідомили ті переваги, які надає їх розвиток та поширення. Нині в Україні є відчутною потреба унормувати нові відносини, що виникають у зв’язку з бурхливим розвитком комп’ютерних технологій.

Розвиток електронної комерції і електронного документообігу в Україні стикається з недостатністю правового регулювання застосування ЕЦП і електронного документообігу [3].

Правові основи для застосування електронних документів у цивільних відносинах уперше закладено Цивільним кодексом України, що набрав чинності з 1 січня 2004 р. Згідно зі ст. 207 «Вимоги до письмової форми правочину»: «правочин вважається таким, що вчинений у письмовій формі, якщо воля сторін виражена за допомогою телетайпного, електронного або іншого технічного засобу зв'язку». Під час здійснення правочинів допускається застосування електронно-цифрового підпису. Тим самим Цивільний кодекс України прирівнює електронні документи до паперових і допускає засвідчення їх електронним підписом.

На виконання рекомендацій Парламентських слухань з питань побудови інформаційного суспільства в Україні у державі створено нормативно-правове підґрунтя і технологічну основу функціонування юридично значимого електронного цифрового підпису. Законами України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV, а також «Про електронний цифровий підпис» від 22 травня 2003 року № 852-IV встановлено основні організаційно-правові засади електронного документообігу та використання електронних документів, а також правовий статус електронного цифрового підпису (ЕЦП) та порядок його застосування юридичними і фізичними особами, визначено організаційну інфраструктуру ЕЦП та її суб'єктів. Передбачалася послідовна розробка нормативно-правових актів, сфера регулювання яких визначена вперше, визначено необхідність підтримки функціонування центрального засвідчувального органу, як основного елемента інфраструктури електронного цифрового підпису.

На виконання вищеназваних законів протягом 2004 року прийнято шість постанов Кабінету Міністрів України (від 26 травня 2004 р. № 680, від 13 липня 2004 р. № 903, від 28 жовтня 2004 р. №№ 1451-1454), які стосуються сфер електронного документообігу та електронного цифрового підпису.

Дорученням Кабінету Міністрів України від 23.02.2005 № 6056/2/1–05 передбачалось створення центрального засвідчувального органу та

забезпечення умов для акредитації центрів сертифікації ключів інфраструктури електронного цифрового підпису.

Постановою Кабінету Міністрів України від 6 травня 2005 р. № 324 «Про заходи щодо виконання у 2005 році Програми діяльності Кабінету Міністрів України «Назустріч людям» підтверджено необхідність прийняття цільової програми впровадження й розвитку електронного документообігу з використанням електронного цифрового підпису.

В Указі Президента України «Про першочергові заходи щодо впровадження новітніх інформаційних технологій» від 20 жовтня 2005 р. № 1497 одним із пріоритетних напрямків сфери інформаційних технологій визначено впровадження в Україні електронного документообігу із застосуванням електронного цифрового підпису.

Проте, жодним із вищезазначених законів та нормативно-правових актів не було передбачено конкретних заходів щодо створення, впровадження й утримання інфраструктури електронного цифрового підпису та не визначені механізми фінансування цих заходів [17].

З метою вирішення питань, які стосуються проблематики запровадження в Україні системи електронного урядування, 24 лютого 2003 року було прийнято Постанову Кабінету Міністрів України № 208 «Про заходи щодо створення електронної інформаційної системи «Електронний уряд».

Відповідно до цієї Постанови передбачено створити належні нормативно-правові засади функціонування системи «Електронний уряд», забезпечити умови для більш швидкого та доступного надання інформаційних послуг громадянам та юридичним особам шляхом використання електронної інформаційної системи «Електронний уряд», яка забезпечує: взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій, інтегрувати державні електронні інформаційні ресурси і системи в Єдиний вебпортал органів виконавчої влади.

Вдосконалення та оновлення нормативно-правової бази України, створення спеціальних юридичних норм сприятиме ефективному

впровадженню та функціонуванню електронного документообігу та електронного цифрового підпису. Для регулювання правовідносин у сфері інформаційних технологій Верховна Рада України вже ухвалила кілька Законів України, які набули чинності:

– «Про електронні документи та електронний документообіг» від 22 травня 2003 р. № 851–IV;

– «Про електронний цифровий підпис» від 22 травня 2003 р. № 852–IV;

– «Про Національну програму інформатизації» від 4 лютого 1998 р. № 74/98–ВР;

– «Про телекомунікації» від 18 листопада 2003 р. № 1280–IV;

– «Про Національну систему конфіденційного зв'язку» від 10 січня 2002 р. № 2919–111;

– «Про захист інформації в інформаційно–телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР [32].

Прийняття згаданих нормативно-правових актів, предметом регулювання яких є процеси електронного документообігу, дало можливість створити сприятливі умови в сфері застосування сучасних інформаційних технологій, стимулювати в Україні розвиток ринку та інфраструктури послуг, що надають за допомогою засобів інформатизації.

В Україні порядок застосування засобів ЕЦП у порівнянні із зарубіжними країнами регламентований набагато жорсткіше. На даний час діє Указ Президента «Про заходи з дотримання законності в області розробки, виробництва, реалізації і експлуатації шифрувальних засобів, а також надання послуг в області шифрування інформації». Відповідно до нього заборонена діяльність юридичних і фізичних осіб, пов'язана з розробкою, виробництвом, реалізацією і експлуатацією шифрувальних засобів, а також захищених засобів зберігання, обробки і передачі інформації, наданням послуг в області шифрування інформації без ліцензій. Забороняється також використання державними організаціями і підприємствами в інформаційно-телекомунікаційних системах шифрувальних засобів, включаючи

криптографічні засоби забезпечення достовірності інформації (електронний підпис), що не мають сертифікату. Така політика держави в області регулювання застосування і реалізації криптографічних засобів, у тому числі і засобів ЕЦП, мабуть, пояснюється прагненням використовувати тільки засоби, сертифіковані уповноваженими державними органами.

Зміст нормативно-правових актів України, які регулюють застосування шифрувальних засобів, у тому числі і засобів ЕЦП, демонструє існуючу тенденцію встановлення «тоталітарного підходу» в цій справі. Безумовно, для вирішення безлічі проблем, пов'язаних з національною безпекою, необхідна наявність певних обмежень в сфері розробки, застосування і обороту засобів ЕЦП. Проте нав'язування продукції тільки одного або декількох виробників у цій галузі (а для самих виробників – обов'язкова платна сертифікація їх діяльності), особливо якщо воно супроводжується закритістю алгоритму, може у результаті призводити до посилення корупції і зниження справжньої, а не декларованої захищеності засобів ЕЦП.

Правове регулювання застосування засобів ЕЦП повинно прагнути до більшої гнучкості у віддзеркаленні вимог об'єктивної дійсності. Можливо, враховуючи особливості України, було б доцільно розглянути багаторівневий підхід до визнання дійсності ЕЦП і ліцензування її засобів: одні вимоги – для адміністративної сфери, інші – для корпоративної і треті – для особистого документообігу. У зарубіжному законодавстві спостерігаються окремі ознаки багаторівневого підходу, наприклад введення поняття кваліфікованого ЕЦП в Директиві.

Таким чином, проаналізувавши розвиток сфери інформаційних правовідносин та інформатизації, зокрема, впровадження системи електронного документування в Україні, різноманітні документи та матеріали, можна зробити висновок, що у цьому напрямку здійснюються певні заходи. Можливо, не настільки інтенсивно, як в інших державах, але можна стверджувати, що через деякий час Україна, за умови системної правової та практичної розбудови

системи електронного документування, також буде характеризуватися неабиякими здобутками у цій сфері.

2.3. Криптографічне перетворення інформації з використанням закритого ключа підпису

Сервіси електронного підпису документів. Крім державних сайтів, працювати з електронними документами можна через спеціальні сервіси. Вони зручні у використанні, а деякі з них є абсолютно безкоштовними.

Рисунок 2.1. – Сервіс електронного підпису Вчасно

Цей сервіс електронного документообігу знайомий багатьом, хто працює з е-документами в Україні (https://vchasno.ua/terms-of-use). Працювати з сервісом досить просто, необхідно лише зареєструвати себе і співробітників. Безкоштовний тариф включає:

- підписання документів в офісі контрагентам;
- підписання документів в офісі від контрагентів;
- коментарі зі співробітниками та контрагентами;
- зберігання документів в хмарному архіві протягом 3-х років.

Платні тарифи містять такі функції, як внутрішнє узгодження та сценарії документів.

Рисунок 2.2. – Сервіс електронного підпису Paperless

Сервіс Paperless (https://paperless.com.ua/) дозволяє обмінюватися компаніям і підприємцям електронними документами, з допомогою якого можна: підписувати за допомогою ЕЦП документи всіх основних АЦСК України, включаючи Податкову службу, Міністерство юстиції, ПриватБанк та ін.; зберігати договори і акти; користуватися сервісом безкоштовно, незалежно від кількості завантажених файлів.

Рисунок 2.3. – Сервіс електронного підпису DocuSign

Американський сервіс дає можливість користувачам завантажувати документи, підписувати їх або відправляти контрагентам на підпис. DocuSign також може працювати з факсимільними підписами (відтворює фізичний підпис) і створювати сторінку під клієнта для автоматизованого заповнення шаблонів. Щоб отримати доступ до роботи з DocuSign, необхідно безкоштовно завантажити тріал-версію і створити обліковий запис [12].

Рисунок 2.4. – Сервіс електронного підпису Adobe Acrobat

Пакет програм для роботи з PDF від Adobe Systems дозволяє перенести звичне підписання документів в онлайн-формат. В Adobe Acrobat можна підписати будь-який PDF-документ, вставивши електронну версію фізичного підпису. Якщо вам необхідно підписати документ не через ЕЦП, а

використовуючи свій підпис в електронному форматі, в Adobe це зробити найзручніше [12].

Рисунок 2.5. – Сервіс електронного підпису HelloSign

Цей закордонний сервіс — ще один популярний інструмент для роботи з документами онлайн. Ви можете використовувати Chrome, Google Docs, інтегруватися з хмарними сервісами і навіть Gmail-поштою. Ви можете використовувати шаблони і створювати індивідуальний брендинг. Безкоштовна версія дозволяє підписувати тільки 3 документа протягом місяця. Тарифи стартують від $13/міс [12].

Підписання документів теж переходить в онлайн. У 2019 представники уряду України заявили про те, що вони планують діджиталізувати паперовий документообіг. Карантин 2020 прискорив процес переходу від паперових документів до електронних з використанням ЕЦП. Для фахівців це прекрасна можливість не тільки спростити роботу зі співробітниками (особливо новачками) в онлайні, а й швидко і безпечно організувати підписання необхідних документів в електронній формі.

РОЗДІЛ 3
ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ В ДОКУМЕНТООБІГ

3.1. Особливості функціонування цифрового підпису

Законодавством України передбачена можливість документообігу з використанням електронного підпису. Одночасно існує можливість уникнути підписання документів «на папері». Електронну форму документа передбачає ЗУ «Про електронні документи та електронний документообіг», ЗУ «Про електронні довірчі послуги», ЗУ «Про захист прав споживачів», ЗУ «Про зовнішньоекономічну діяльність», ЗУ «Про електронну комерцію», Цивільний кодекс України та інші нормативно-правові акти.

Відповідно до ст. 205 ЦКУ Цивільного кодексу України – Правочин може вчинятися усно або в письмовій (електронній) формі. Також передбачено право сторін обирати форму правочину. А стаття 639 ЦКУ передбачає, що договір, укладений за допомогою інформаційно-телекомунікаційних систем за згодою обох сторін вважається укладеним в письмовій формі. Вищезазначені нормативно-правові акти визнають укладеними договори, що підписані за допомогою електронного підпису, а також визначають механізми, способи та порядок укладання таких договорів [8]. Електронний цифровий підпис підтверджує достовірність і цілісність документа. Якщо в документ в процесі пересилки були внесені які-небудь зміни, нехай навіть зовсім незначні, то підміна виявиться. Сертифікат відкритого ключа містить персональну інформацію про власника, що дозволяє ідентифікувати автора документа.

Однією з додаткових можливостей при роботі з ЕЦП є послуга фіксації точного часу підписання документа ЕЦП відмітка точного часу. Відмітка точного часу при підписанні документа дозволяє точно ідентифікувати момент накладання підпису, причому змінити його значення згодом, навіть особою, яка наклала підпис, неможливо. Можливе лише повторне підписання з фіксацією

нового часу. Точне значення часу, який використовується для формування відмітки точного часу, здійснюється апаратними засобами Центру сертифікації ключів шляхом синхронізації з джерелами точного часу з точністю до 1 секунди [16].

Під електронним підписом може матися на увазі будь-який спосіб підписання електронного документа, зокрема графічне зображення рукописного підпису та звичайних паролів. Проте в Законі про ЕЦП наголошується на регулюванні відносин, пов'язаних з використанням одного різновиду електронного підпису – електронного цифрового підпису. Його особливість полягає в тому, що він ґрунтується на алгоритмах криптографічного захисту інформації. ЕЦП накладається за допомогою особистого ключа – спеціального коду, відомого тільки особі, яка підписала документ. Застосування будь-яких інших видів електронного підпису допускається на договірних засадах. Інакше кажучи, такі електронні підписи матимуть якусь значущість тільки для сторін конкретного договору, в межах якого вони застосовуються [9].

Щоб кожний «підписувач» мав свій, унікальний, підпис, використовується так званий особистий ключ – код, який має бути відомий лише його власнику. Якщо цей код повідомити програмі, то відповідно до криптографічного алгоритму вона сформує унікальне контрольне значення і додасть його до документу. Тобто підпише електронний документ унікальним ЕЦП господаря даного особистого ключа.

Для перевірки вірогідності ЕЦП та цілісності електронного документа використовується інший код – так званий відкритий ключ. На відміну від особистого, відкритий ключ доступний усім іншим зацікавленим учасникам електронного документообігу. Цей код не дозволяє підробити ЕЦП автора електронного документа, але дозволяє перевірити його справжність. Отримавши цей код, програма, використовуючи вже згаданий алгоритм, звірить його з отриманим разом з документом ЕЦП автора.

3.2. Варіативність механізму використання електронного цифрового підпису в електронних документах

Використання сьогодні різних редакторів виготовлення документа потребує окремого підходу до його підписання. Як підписати документ в Word: покрокова інструкція Microsoft Word Document, Excel Workbook, або PowerPoint Presentation: Office 2013, 2010 і 2007.

Рис. 3.1 - Відображення цифрового підпису в документі Word

Додавання цифрових підписів до документів в Microsoft Office. Цифрові підписи ідентифікують / автентифікують підписувача документа і дозволяють одержувачам документів перевіряти, що ніхто не змінив вміст документа з моменту його підписання.

Microsoft Office надає два методи для підписання (додавання цифрового підпису) ваших документів.

Метод 1: Додавання невидимого цифрового підпису. Так можна додати невидимий цифровий підпис в документ Word, книгу Excel або презентацію PowerPoint. Цей підпис не відображається в документі. Замість цього в нижній частині вікна документа з’являється невеликий значок, який означає, що документ був підписаний. Одержувачі можуть натиснути значок, щоб переглянути інформацію про передплатника.

Метод 2: Додавання видимого цифрового підпису. Можна додати видимий цифровий підпис до документа Word або книги Excel. Цей підпис з'являється в документі разом з маленьким значком підпису в нижній частині вікна документа, щоб позначити, що документ був підписаний. Одержувачі можуть двічі клацнути підпис або клацнути значок, щоб переглянути інформацію про пристрій, що підписує. Примітка. Не можна створити підпис всередині презентації PowerPoint.

Розглянемо механізм підписування документа Microsoft Word, Excel Workbook або презентації PowerPoint.

❖ Приклад застосування ЕЦП для документа *Microsoft Office 2013*.

Скріншоти, наведені далі, відносяться до слова Microsoft і майже ідентичні екранам в Excel і PowerPoint. Підключіть маркер сертифіката підпису документа. В Microsoft Word, Excel або PowerPoint відкрийте документ, який ви хочете підписати.

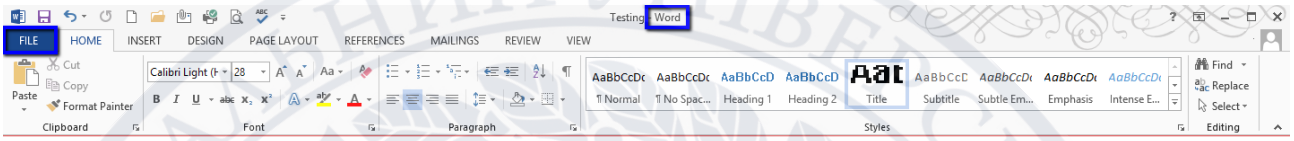


Рис. 3.2 – У вибраній програмі Microsoft натисніть кнопку Файл.

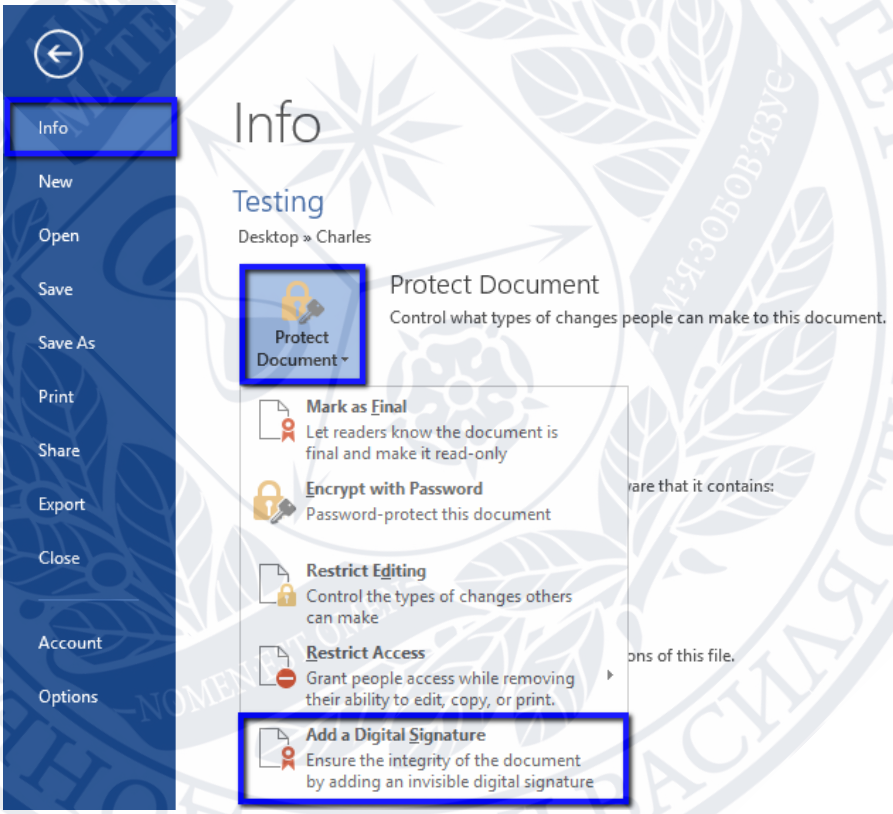


Рис. 3.3 – На вкладці Файл натисніть Інформація а потім, Microsoft Word.

Натисніть Захистити документ > Додати цифровий підпис

•Microsoft Excel - Натисніть Захистити робочу книгу > Додати цифровий підпис.

•Microsoft PowerPoint - Натисніть Захистіть презентацію > Додати цифровий підпис.

У вікні Підписати у спадному списку Тип зобов’язання виберіть тип зобов’язань, який найкраще відображає роль підписувача:

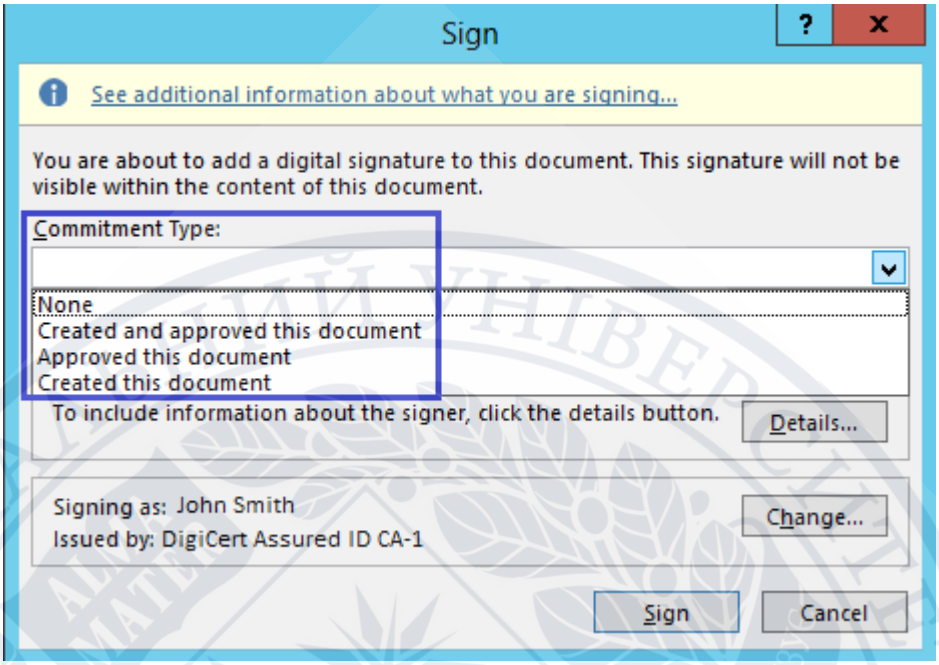


Рис. 3.4 – Тип зобов’язання:

- Ніхто
- Створено та затверджено цей документ
- Затверджено цей документ
- Створено цей документ

У вікні Мета для підписання цього документа введіть мету підписання документа.

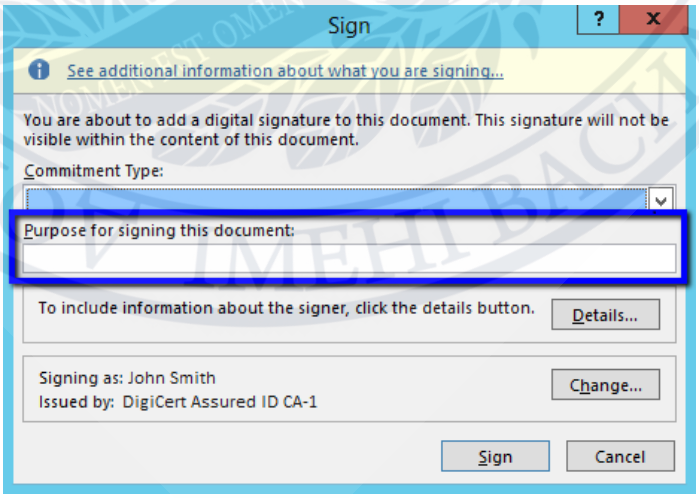


Рис. 3.5 – Мета підписання документа

Щоб додати інформацію про підписувача, натисніть кнопку Подробиці. Тоді, в вікні Додаткова інформація про підпис введіть інформацію та OK.

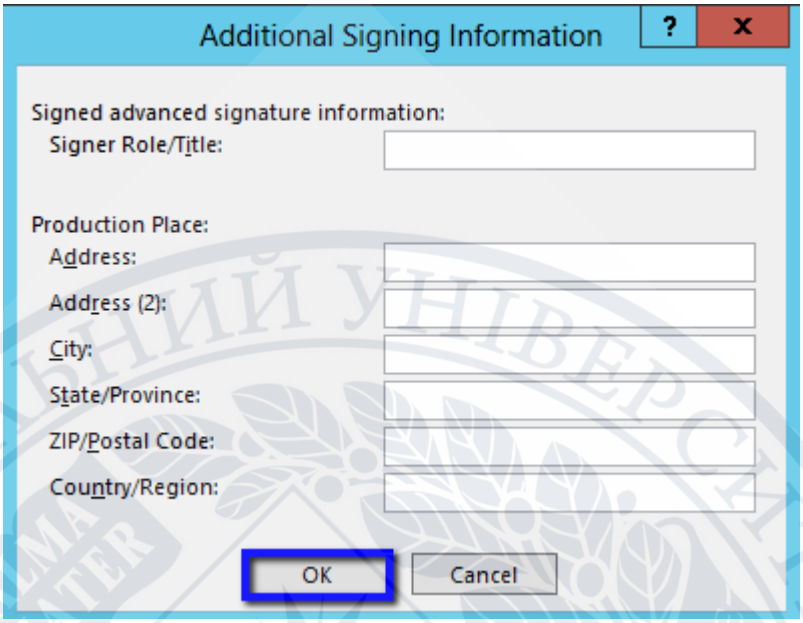


Рис. 3.6 – Додаткова інформація

Далі, в вікні Підписати натисніть Змінити.

У вікні Windows Безпека виберіть сертифікат, який ви хочете використовувати для підписання документа, а потім натисніть кнопку OK. У вікні Підписати натисніть Підписувати.

Якщо ви використовуєте сертифікат підписування документів DigiCert®, введіть свій токенний пароль, а потім натисніть кнопку OK.

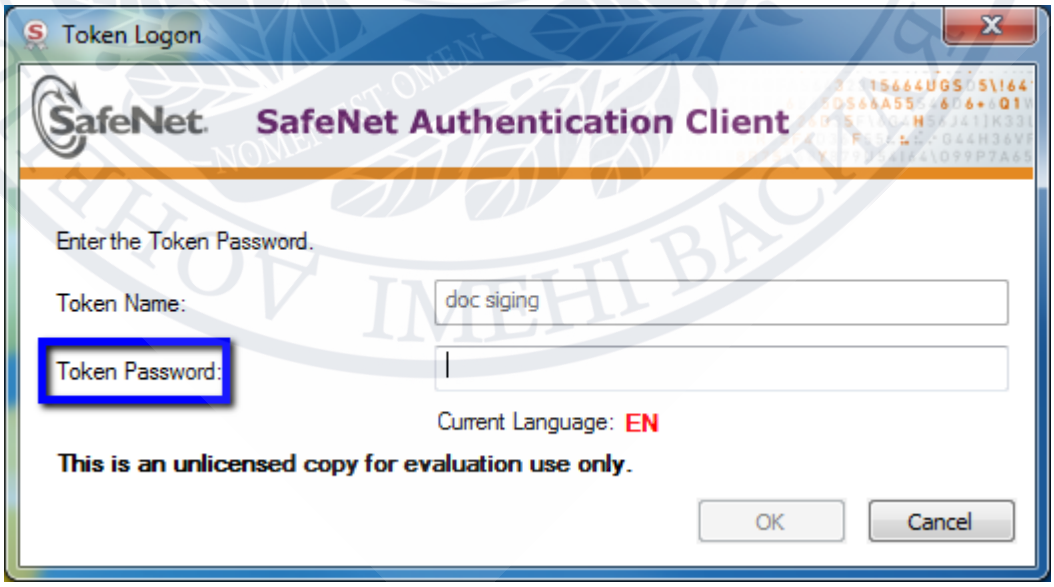
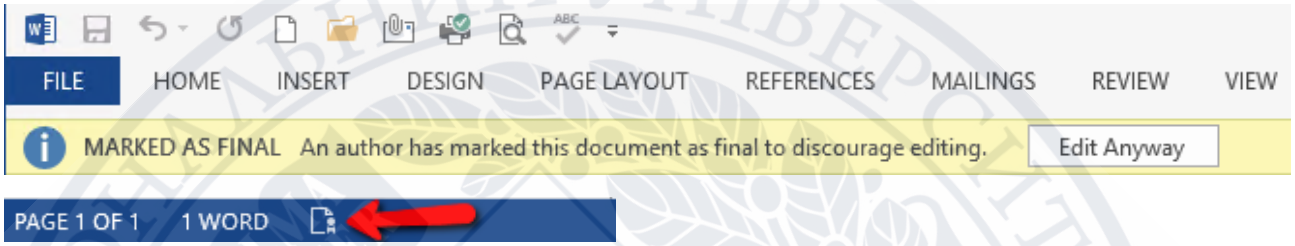


Рис. 3.7 – Сертифікат підписування документів DigiCert®

У вікні Підтвердження підпису прочитайте повідомлення, а потім натисніть кнопку ОК. Примітка: Якщо ви позначили пункт Не показувати це повідомлення ще раз, це вікно не з’явиться.

Документ маркується як фінальний, а в нижній частині вікна документа відображається маленька сторінка з піктограмою стрічки, що означає, що документ був підписаний. Якщо редагуєте будь-яку інформацію в документі, підпис видаляється, і він має бути ліквідований.



Щоб переглянути інформацію про підписувача, натисніть кнопку Цей документ містить підписи (маленька сторінка з піктограмою стрічки). Ви також можете натиснути Файл > Інформація >Переглянути підписи.

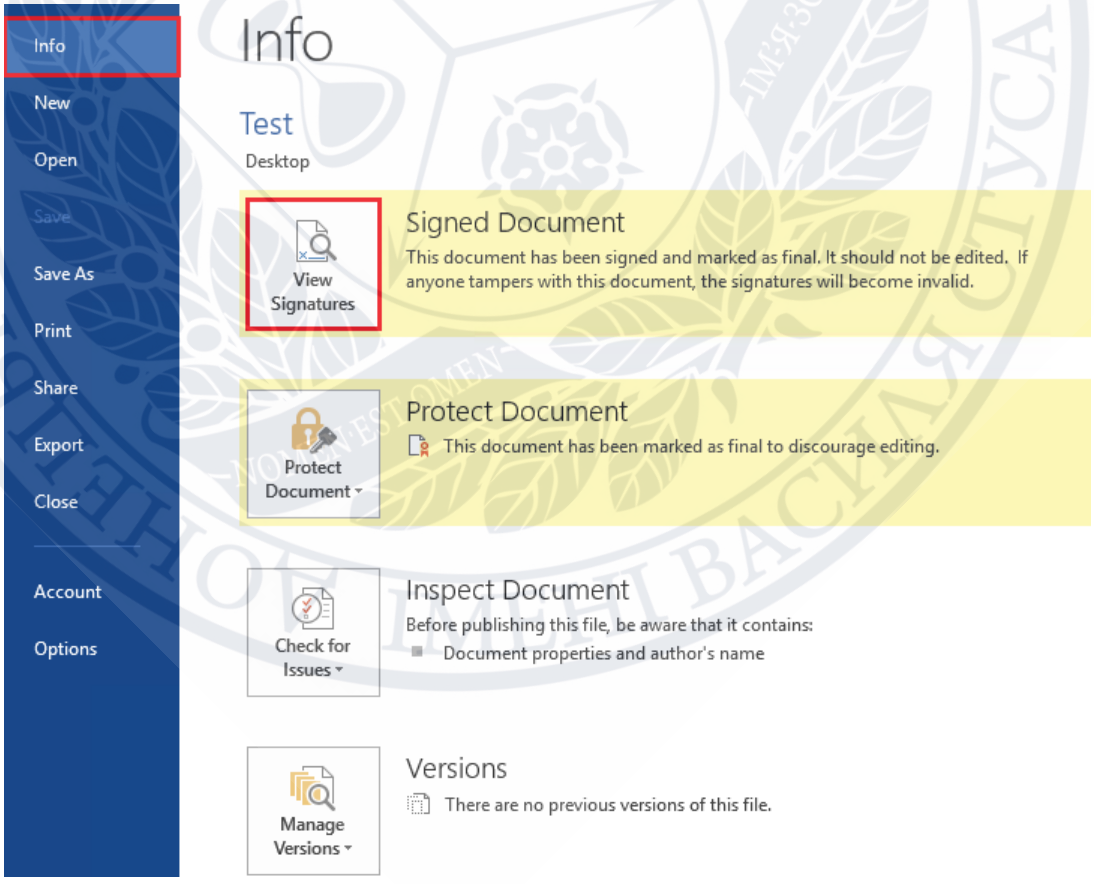
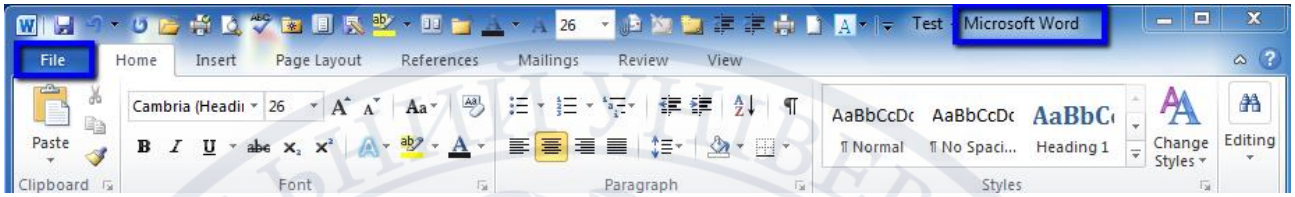


Рис. 3.8 – Перегляд інформації про підписувача

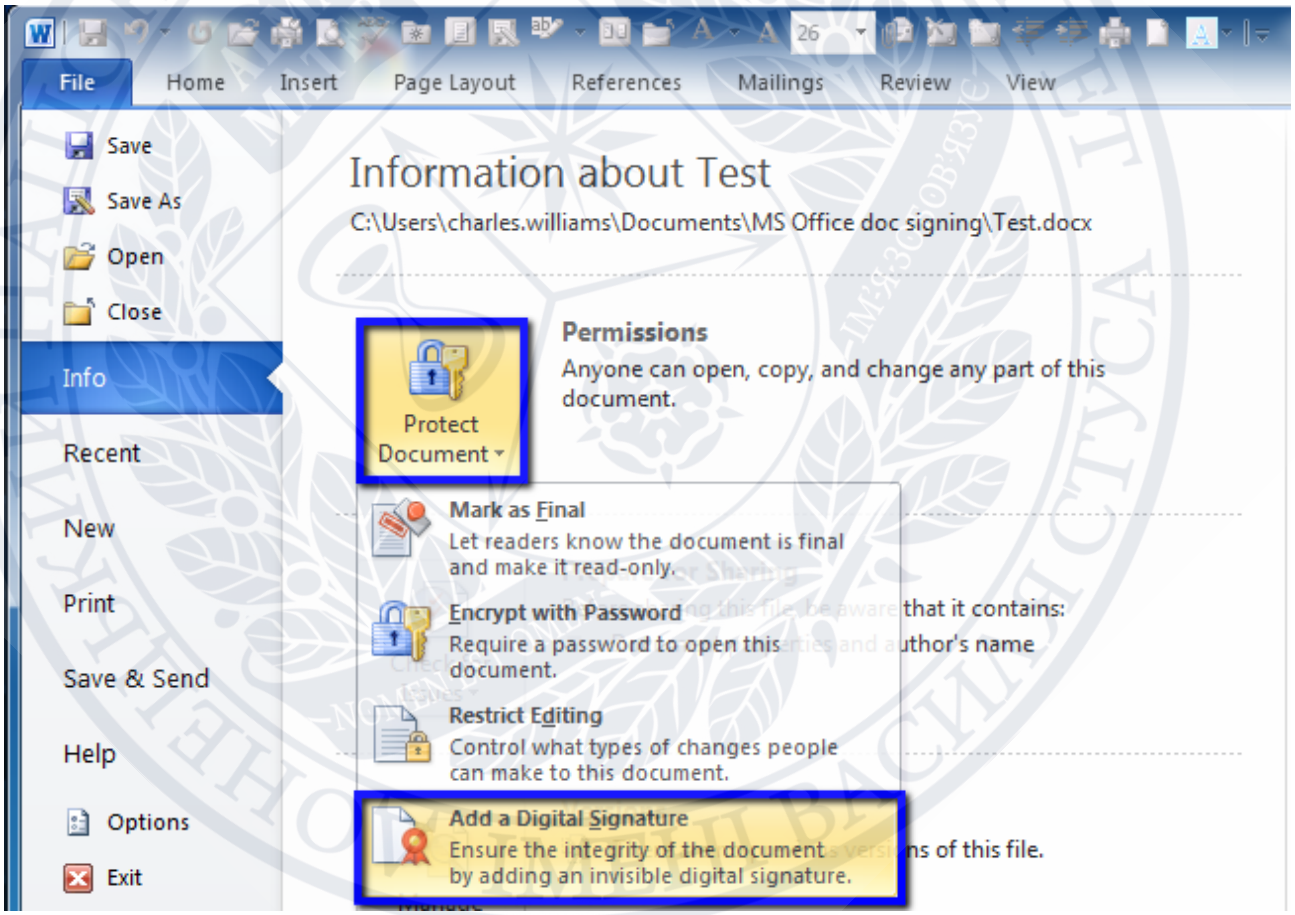
❖ *Microsoft Office 2010*

Скріншоти екрана, надані в цій інструкції, є словами Microsoft і майже ідентичні екранам в Excel і PowerPoint.

Розглянемо наступні команди. Вставте токен сертифіката підпису документів. В Microsoft Word, Excel або PowerPoint відкрийте документ, який ви хочете підписати. У вибраній програмі Microsoft натисніть кнопку Файл.



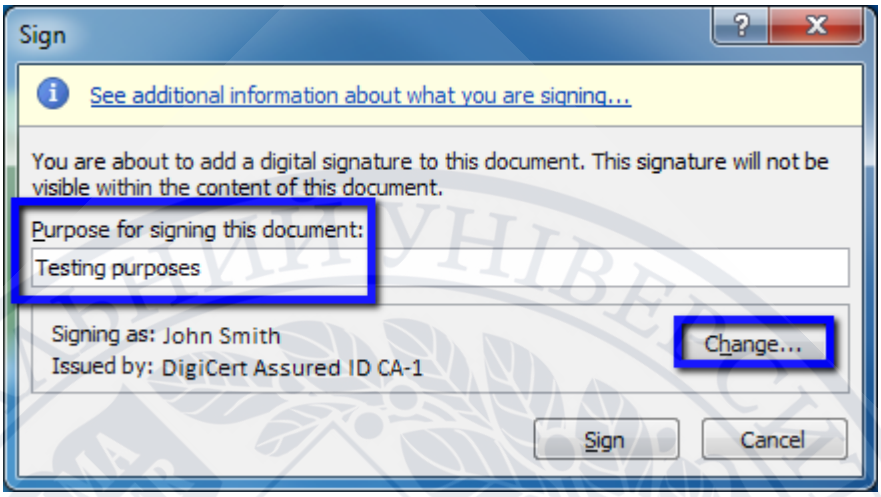
На вкладці Файл натисніть Інформація а потім, *Microsoft Word,* Натисніть Захистити документ> Додати цифровий підпис.



Microsoft Excel – Натисніть Захистити робочу книгу > Додати цифровий підпис.

Microsoft PowerPoint – Натисніть Захистіть презентацію > Додати цифровий підпис.

Якщо з’явиться вікно Цифрові підписи Microsoft Office натисніть ОК. У вікні Підписати у полі Мета для підписання цього документа введіть свою мету для підписання документа.



Натисніть ще раз Змінити.

У вікні Windows Безпека під Виберіть сертифікат виберіть сертифікат, який ви хочете використовувати для підписання документа, а потім натисніть кнопку ОК. У вікні Підписати натисніть Підписувати.

Якщо ви використовуєте сертифікат підписування документів DigiCert®, введіть свій токенний пароль, а потім натисніть кнопку ОК.

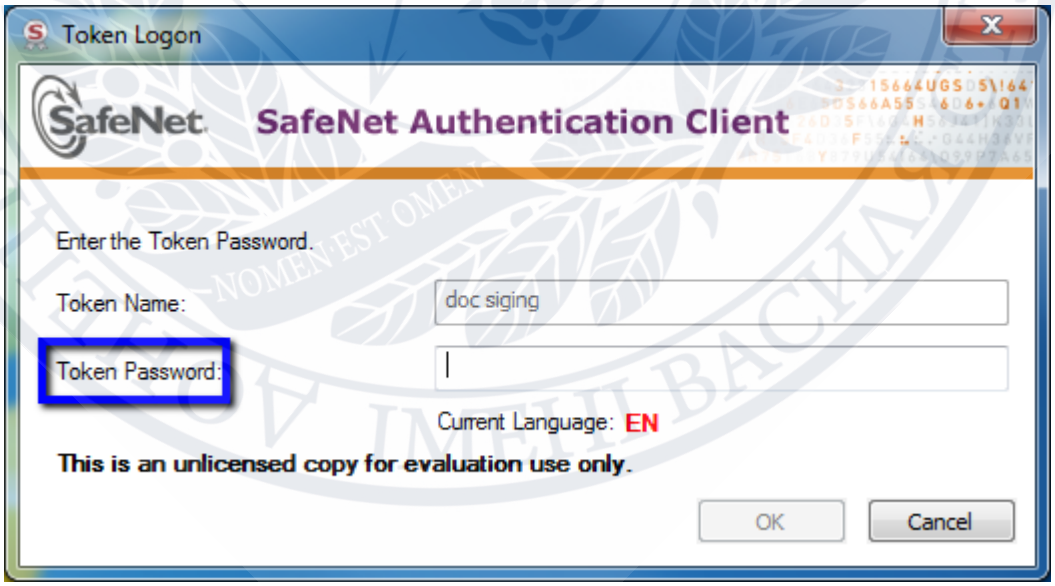
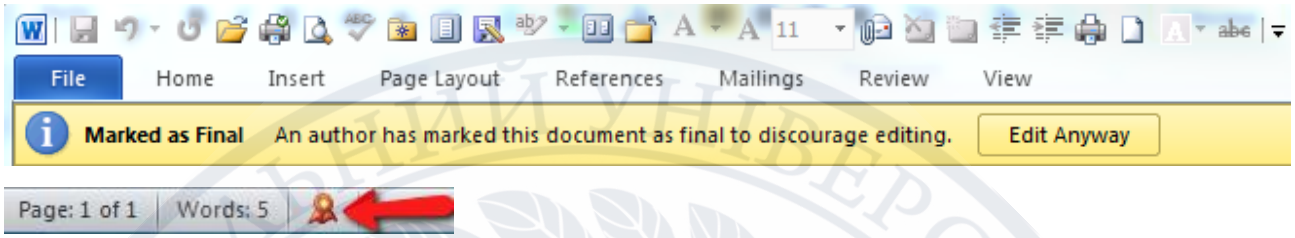


Рис. 3.9 – Сертифікат підписування документів DigiCert®

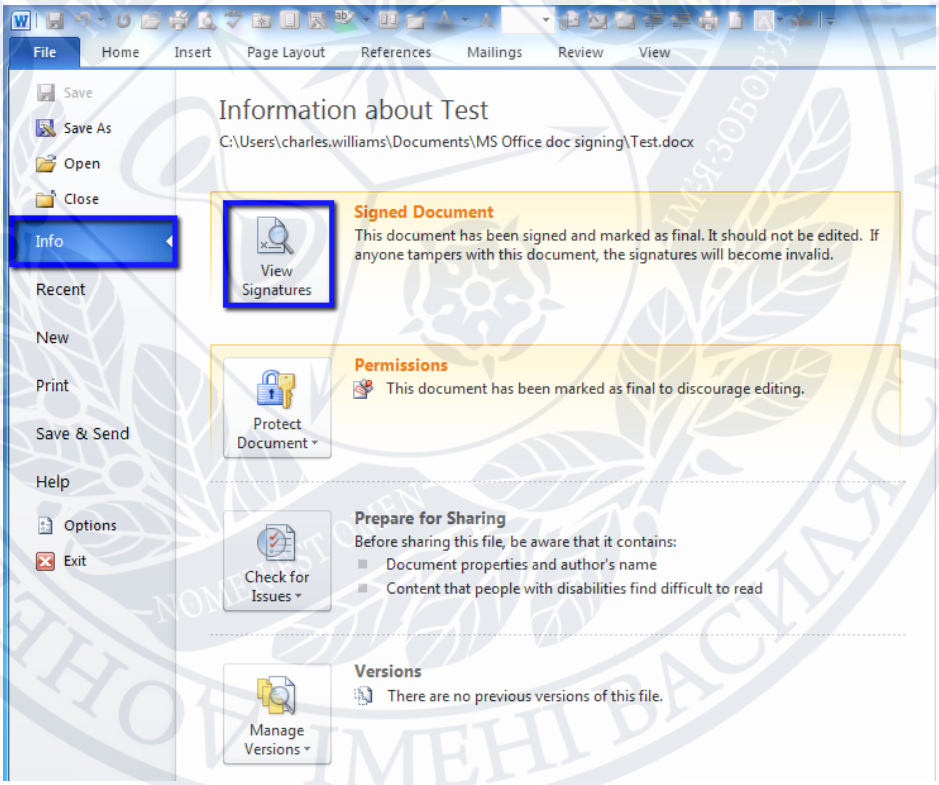
У вікні Підтвердження підпису прочитайте повідомлення, а потім натисніть ОК.

Примітка: Якщо ви позначили пункт Не показувати це повідомлення ще раз, це вікно не з’явиться. Документ позначається як фінальний і в нижній частині вікна документа відображається маленька піктограма червоної стрічки, що означає, що документ був підписаний. Якщо ви редагуєте будь-яку інформацію в документі, підпис видаляється, і він має бути ліквідований.



Щоб переглянути інформацію про підписувача, натисніть кнопку. Цей документ містить підписи(червона піктограма стрічки).

Ви також можете натиснути Файл > Інформація > Переглянути підписи.



❖ *Microsoft Office 2007*

Скріншоти екрана, надані в інструкції, є словами Microsoft і майже ідентичні екранам в Excel і PowerPoint.

Вставте токен сертифіката підпису документів. ІВ Microsoft Word, Excel або PowerPoint відкрийте документ, який ви хочете підписати. У вибраній програмі Microsoft натисніть кнопку Microsoft Office

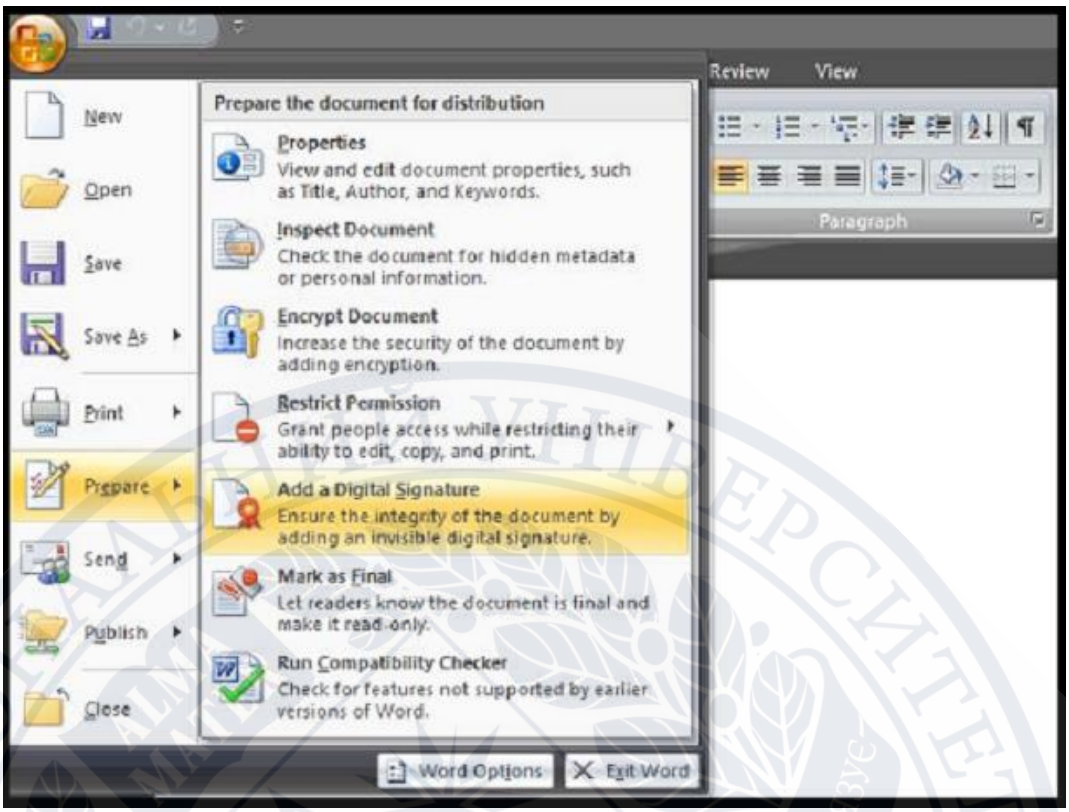
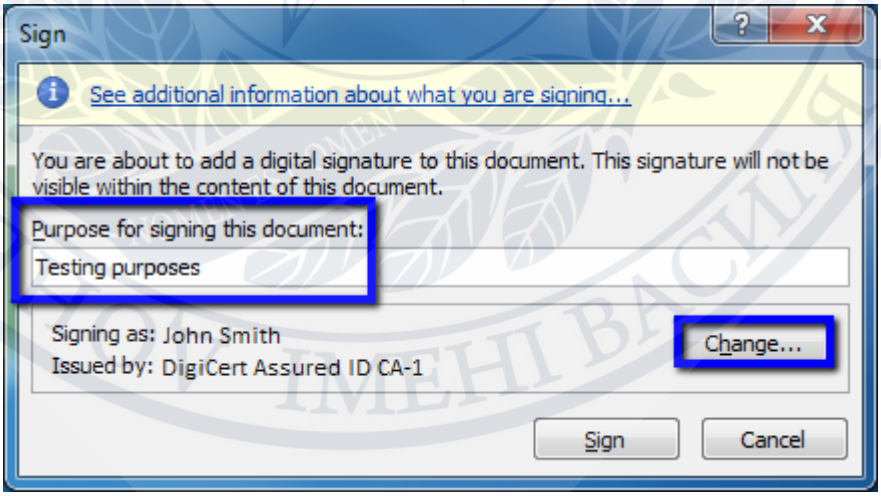


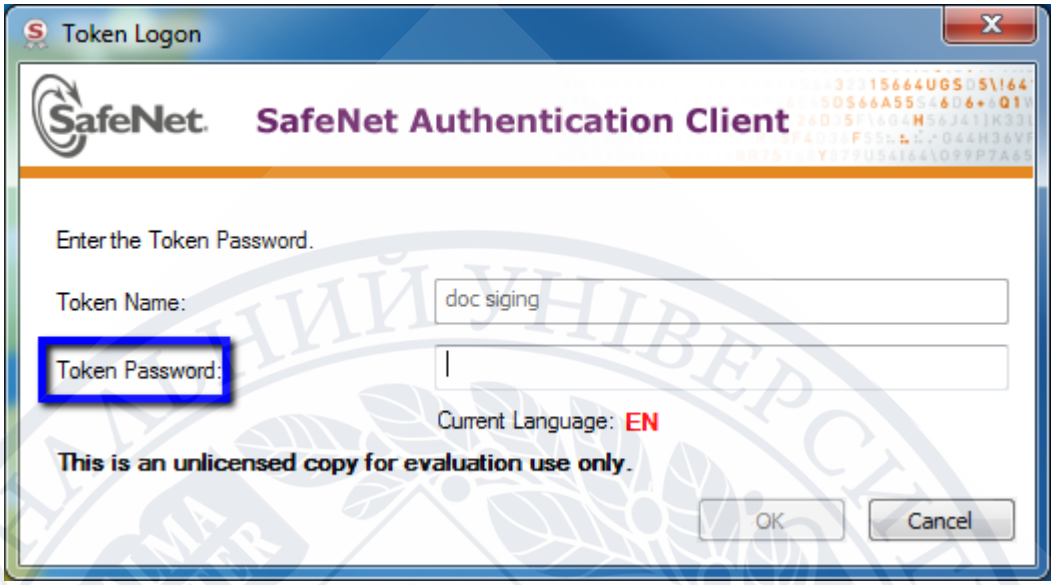
Рис. 3.10 – Microsoft Office 2007

Потім натисніть кнопку Підготовка > Додати цифровий підпис. Якщо з'явиться вікно Цифрові підписи Microsoft Office натисніть кнопку OK. У вікні Підписати у полі Мета для підписання цього документа введіть свою мету для підписання документа.

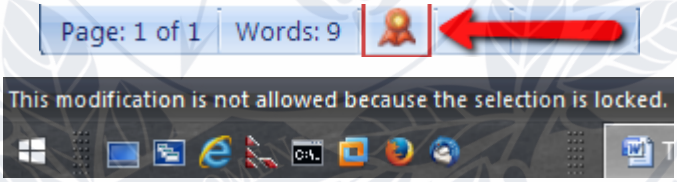


Потім натисніть кнопку Змінити. У вікні Windows безпека у розділі Вибір сертифіката виберіть сертифікат, який ви хочете використовувати для підписання документа, а потім натисніть кнопку OK. У вікні Підписати натисніть кнопку Підписувати.

Якщо ви використовуєте сертифікат підписування документів DigiCert®, введіть свій токенний пароль, а потім натисніть кнопку OK.



У вікні Підтвердження підпису прочитайте повідомлення, а потім натисніть кнопку OK. Примітка: Якщо ви позначили пункт Не показувати це повідомлення ще раз це вікно не з'явиться. Невелика червона піктограма стрічки відображається внизу вікна документа, що означає, що документ був підписаний. Щоб відредагувати будь-яку інформацію в документі, підпис необхідно видалити, і документ має бути ліквідований.

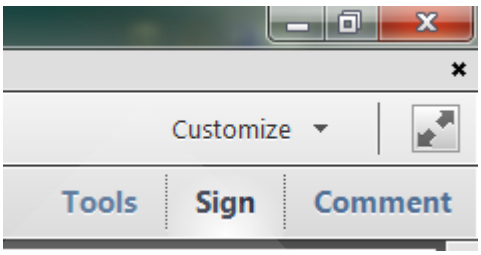


Щоб переглянути інформацію про передплатника, натисніть Цей документ містить підписи(червона піктограма стрічки). Ви також можете натиснути символ Microsoft Office, а потім натисніть Підготовка > Переглянути підписи [15].

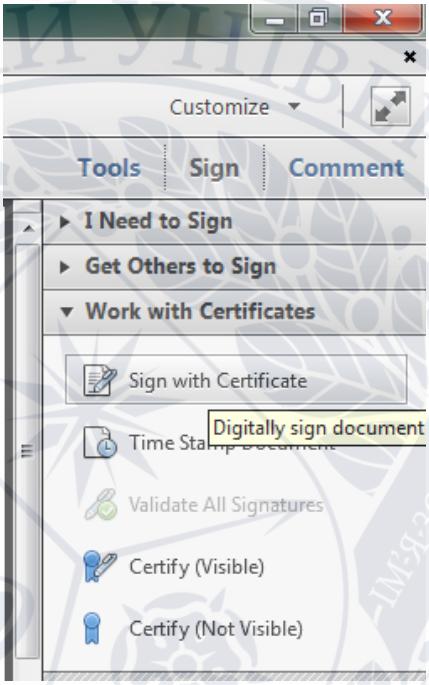
Механізм підписування PDF документа в Adobe Acrobat и Adobe Reader: покрокова інструкція

Підписати PDF документ в Adobe Acrobat XI

Відкрийте файл PDF, який ви хочете підписати. Натисніть кнопку Sign справа зверху:

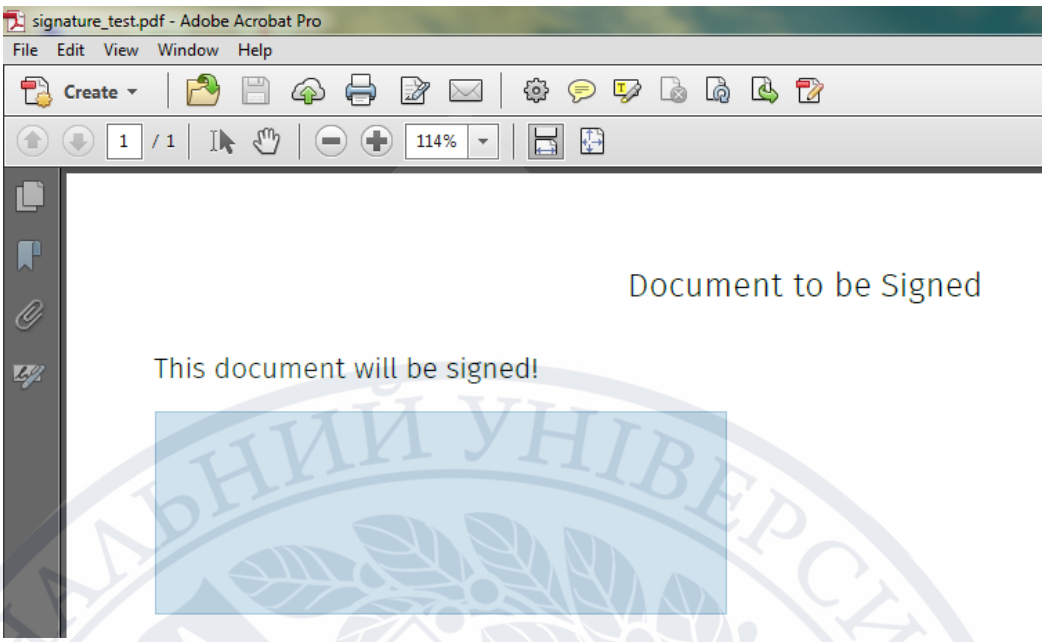


З правого боку розгорніть розділ «Робота з сертифікатами». Натисніть «Підписати сертифікатом» :



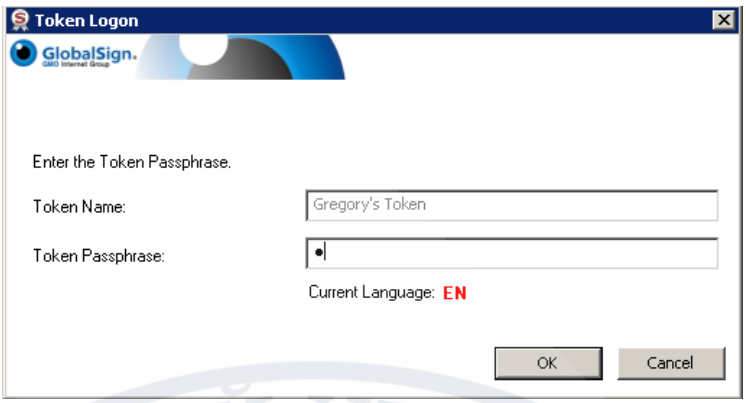
Натисніть Перетягнути новий прямокутник для підпису:

Перетягніть, щоб створити поле підпису:

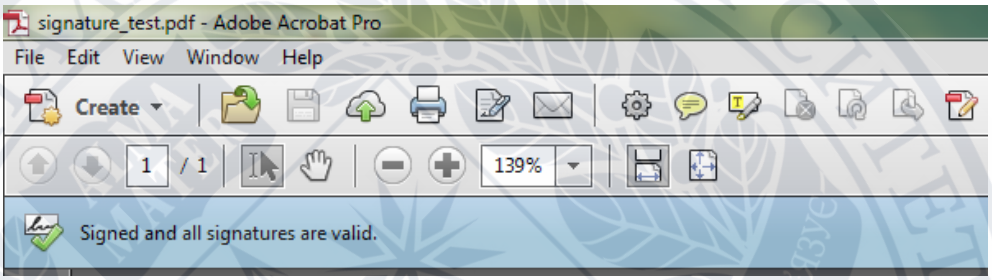


Коли ви відпустите курсор, з’явиться екран Sign Document. Виберіть свій сертифікат в випадаючому меню. Натисніть Sign:

Повторно збережіть документ. Введіть свій пароль. Натисніть ОК:



Ваш підпис з’явиться разом з «Синьою панеллю», що означає, що підпис дійсний:

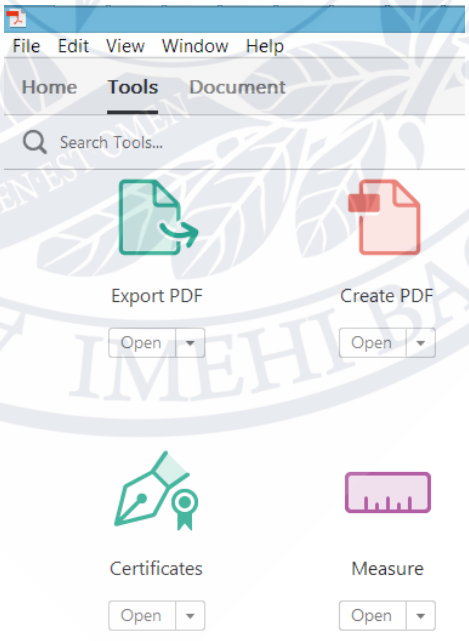


Ваш PDF документ підписаний !

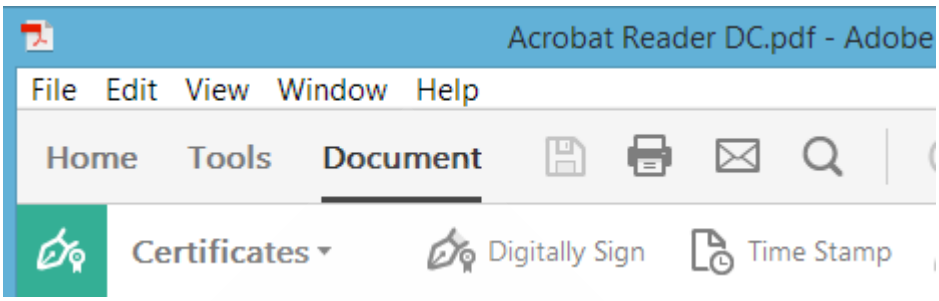
Підписати PDF документ в Adobe Reader DC

1. Відкрийте PDF-файл, який ви хочете підписати в Adobe Reader DC

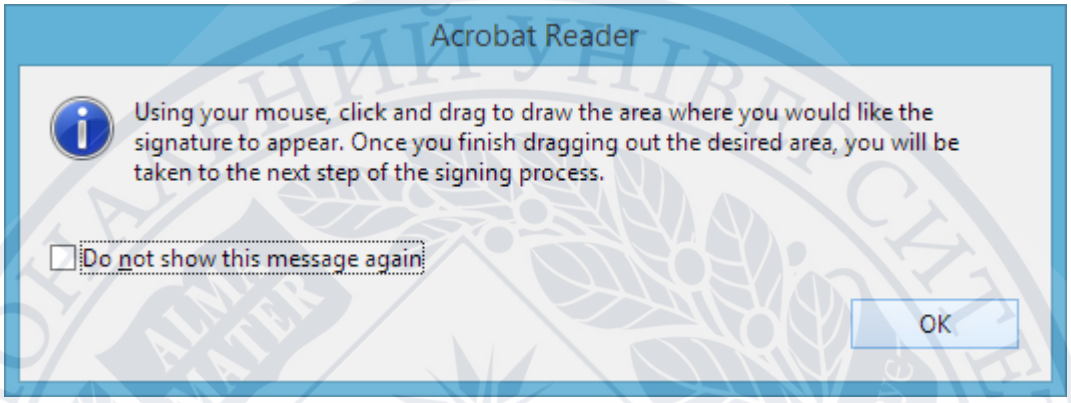
2. Натисніть кнопку «Інструменти» у верхньому лівому кутку, потім натисніть «Сертифікати»:



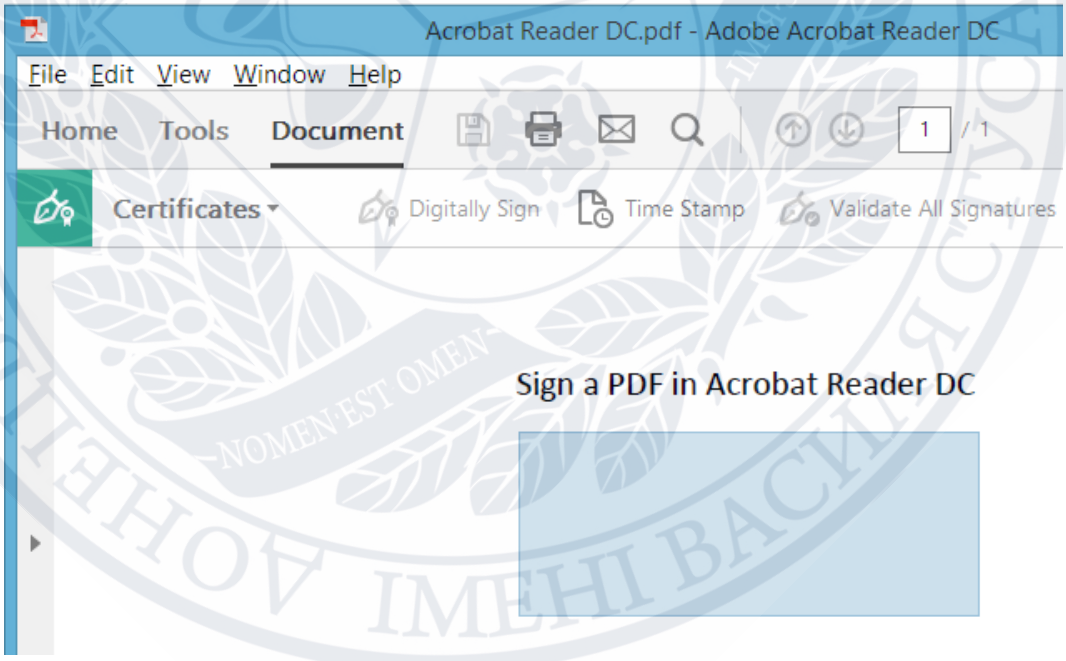
Потім натисніть кнопку Цифровий підпис :



Натисніть «ОК», щоб перетягнути прямокутник підпису:

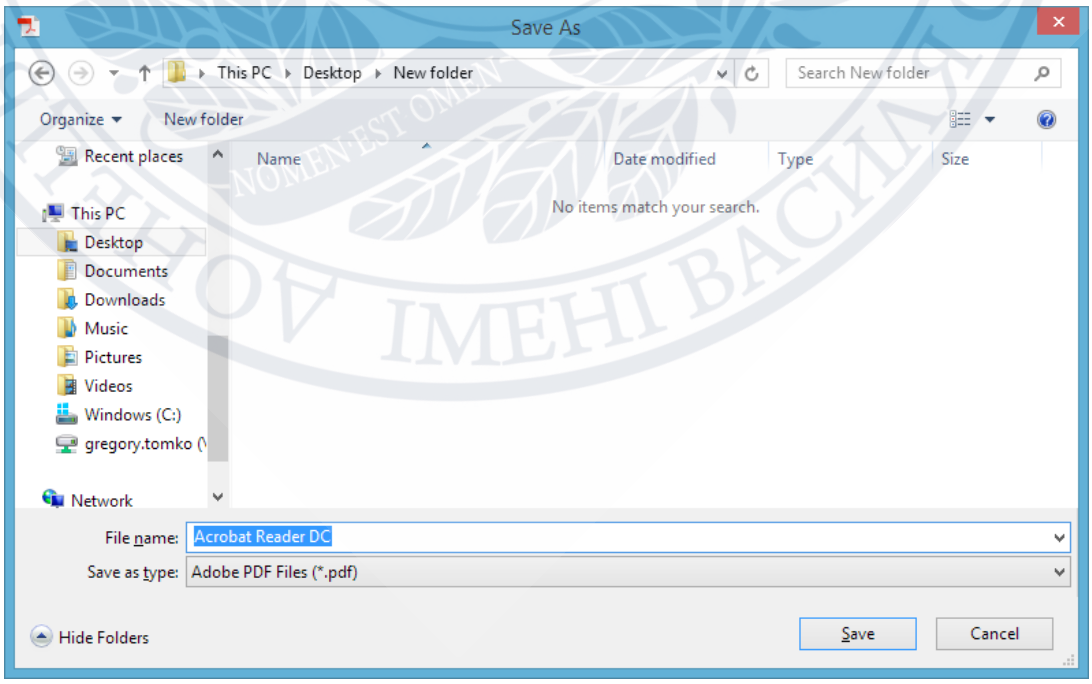


Перетягніть прямокутник підпису, в те місце, де ви хочете, щоб підпис з’явився:

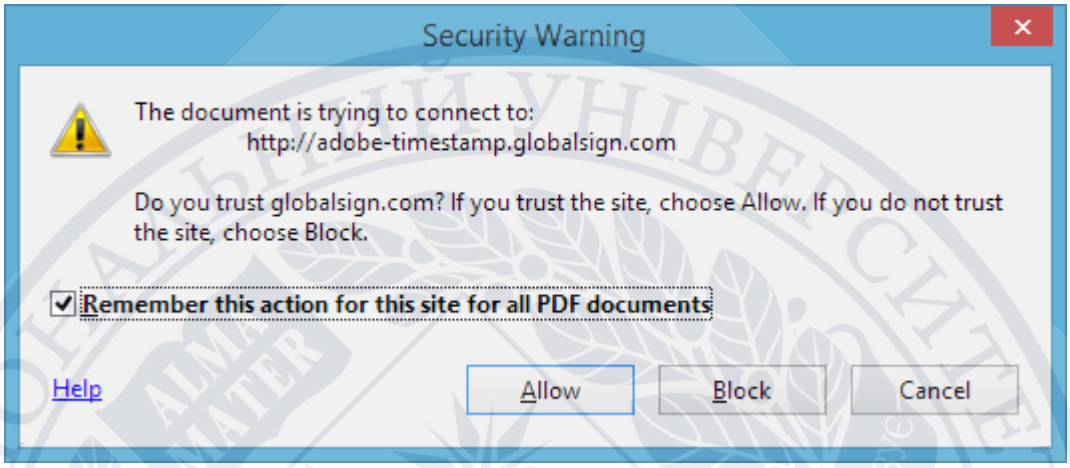


Коли ви відпустите прямокутник підпису, з’явиться вікно з параметрами підпису. Виберіть сертифікат підпису в меню, що розкрилось. Ви можете за бажанням налаштувати зовнішній вигляд свого підпису. Натисніть Sign.

Вам буде запропоновано повторно зберегти документ. Ви можете або замінити існуючий файл, або зберегти його під новим ім'ям. Натисніть «Зберегти» .



Якщо перший раз підписується документ, може бути запропоновано дозволити Reader отримувати доступ до позначки часу. Якщо отримаєте це запрошення, натисніть «Дозволити». Третій учасник підпису timeatmp дозволяє відмовитися від вашого сіганта «неспростовності», він діє як цифровий нотаріус.



Потім введіть пароль для свого сертифіката AATL або CDS:

Після того, як підпис буде розміщено, побачите свій підпис у документі, і «Синя панель» буде активована, показуючи, що ваш підпис дійсний:

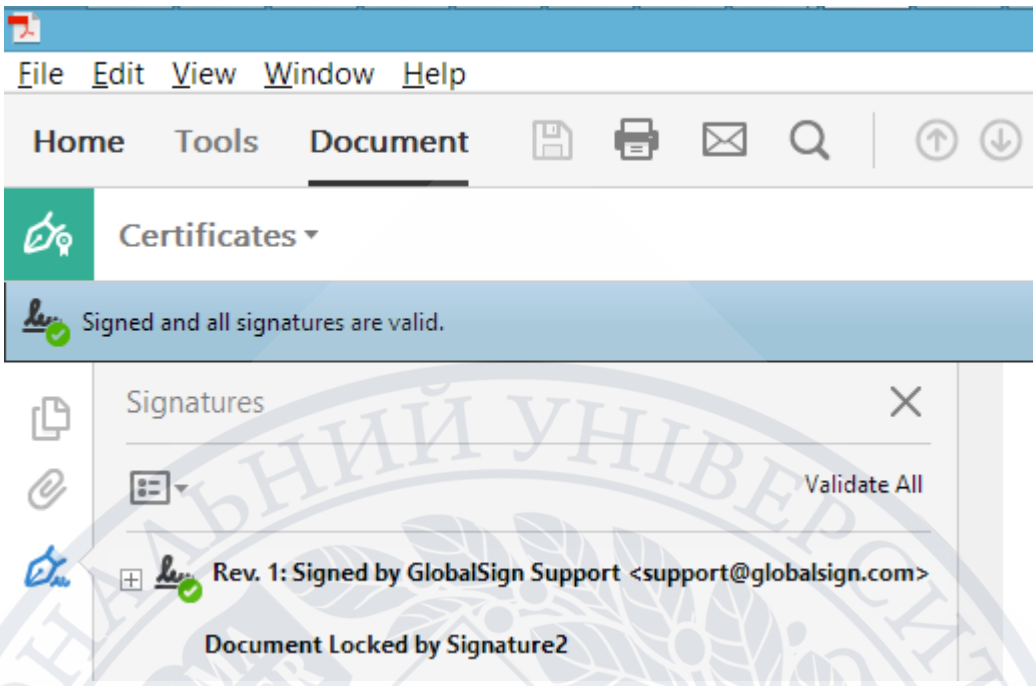


Рис. 3.11 – Підпис у документі PDF

Ваш PDF документ тепер підписаний [16]. Підписування документів передбачає простий механізм дій, а умовою є наявність ЕЦП.

3.3. Регулювання використання електронного цифрового підпису

Первісно Закон України «Про електронний цифровий підпис» (2003 р.) приймався з метою удосконалення чинного законодавства та наближення його до законодавства Європейського Союзу, а саме директиви 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 р. про рамки Співтовариства для електронних цифрових підписів. Однак 23 липня 2014 р. на заміну директиві 1999/93/ЄС було прийнято регламент (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій у межах внутрішнього ринку та скасування директиви 1999/93/ЄС, який набрав чинності 1 липня 2016 р. Внаслідок цього з'явилась необхідність оновлення системи електронного цифрового підпису й в Україні, у зв'язку з чим було прийнято Закон «Про електронні довірчі послуги», який органічно імплементовано у систему взаємодії суб'єктів у сфері електронного цифрового підпису, яка вже була сформована в Україні [2].

Для запровадження електронного бізнесу типу «Бізнес–Бізнес» ключовою правовою проблемою є надання правового статусу документам, які передаються електронним шляхом. Наприклад, електронним шляхом можуть укладатися угоди, надаватись доручення банкам для перерахування коштів, можуть пересилатися сертифікати на продукцію тощо. У звичайному режимі документи засвідчуються підписами відповідальних осіб та печатками. В електронному режимі роль підпису може виконувати електронний (або ж цифровий) підпис. Таким чином, електронний підпис виступає аналогом звичайного підпису в застосуванні до електронних документів [32].

Технологія електронного підпису може бути не менш ефективною, ніж звичайного. Але для практичного використання виникають проблеми правового визнання електронного підпису нарівні із звичайним, що в свою чергу потребує певного регулювання процедур надання засобів цифрового підпису.

Засоби для цифрового підпису (програмне забезпечення для шифрування та коди) надають уповноважені на це установи – центри сертифікації, які засвідчують надання засобів електронного підпису особі сертифікатом. Українське законодавство передбачає два види сертифікатів: звичайний та посилений. Звичайний може видаватися будь–якою особою (центром сертифікації), яка вирішила займатися цим видом діяльності. Для видачі посиленого сертифіката центр сертифікації повинен користуватися засобами електронного цифрового підпису, які в Законі названо «надійними засобами електронного цифрового підпису» та пройти акредитацію уповноваженим на це органом – центральним засвідчувальним центром [36].

Крім того, при систематичному співробітництві підприємства з партнерами за допомогою електронних технологій, можуть виникати й інші проблеми при розв’язанні господарських конфліктів. Все це потребує доповнення законодавства, перш за все Господарського та Цивільного кодексів і відповідних процесуальних кодексів, що поки що залишається лише перспективою.

Проблеми запровадження в Україні електронного документу та електронного цифрового підпису стають все більш актуальними. Вони набувають значної політичної та економічної ваги у зв'язку з розширенням використання інформаційно-комунікаційних технологій у суспільних відносинах, розбудові систем електронних платежів, електронної торгівлі тощо. При цьому, якщо у Цивільному кодексі (1963 року із наступними змінами, внесеними до нього) було багато обмежень щодо використання електронного документа, то новий Цивільний кодекс 2003 року дозволив широке застосування електронних документів у цивільних правовідносинах [49].

Одне з проблемних питань, що повинно вирішити законодавство у цій сфері, – це робота центрів сертифікації ключів, які мають надавати послуги цифрового підпису. Спеціалісти вважають, що кількість бажаючих займатися такою діяльністю, можливо, буде досить незначною. Зокрема, тому, що фінансовий бар'єр виходу на ринок таких структур за нинішніх умов буде досить високим з огляду на специфіку їх функцій (надання засобів цифрового підпису, формування, розповсюдження, скасування, блокування та поновлення сертифікації ключів, генерація відкритих та особистих ключів тощо). А враховуючи те, що все повинно починатися практично з нуля, оскільки майже таким на даному етапі є ринок користувачів, «повернення» зроблених вкладень буде досить довгим [50].

Отже, центр сертифікації ключів є критичним елементом в системі застосування ЕЦП. Неналежна організація надання послуг ЕЦП, незабезпечення відповідного рівня безпеки функціонування, захисту інформації або збої у роботі зазначеного суб'єкта може створити умови, що сприятимуть масовим зловживанням при застосуванні ЕЦП, в тому числі їх підробленню, компрометації та неможливість використовувати даний механізм підписувачами, що отримують послуги ЕЦП у цих суб'єктів та особами, які перевіряють ЕЦП.

ВИСНОВКИ

Електронний цифровий підпис є набором зашифрованих даних, що ідентифікує особу підписанта та засвідчує його волевиявлення. Електронний документообіг значно спрощує процес підписання та обміну документами. Встановлено, що в Україні існують законодавчі та технічні можливості для організації процесу обміну документами в електронній формі, проте відповідні умови слід належним чином передбачати у документах (договорах, угодах тощо). Електронний документообіг в публічному управлінні сьогодні є невід'ємною складовою електронного урядування і розглядається як критерій що встановлює загальні правила документування управлінської діяльності органів виконавчої влади, місцевого самоврядування та публічного управління і регламентує порядок роботи з документами з моменту їх створення або надходження до відправлення або передачі в архів установи У роботі акцентовано увагу на можливості та перспективі електронного підписання документів, процедурі обміну електронними даними, належних реквізитах сторін тощо.

Виявлено, що завданням застосування систем цифрового підпису є автентифікація інформації – захист учасників інформаційного обміну від нав'язування хибної інформації, встановлення факту модифікації інформації, яка передається або зберігається, й отримання гарантії її справжності, а також вирішення питання про авторство повідомлень.

У роботі наголошено, що електронний цифровий підпис отримується в акредитованих центрах сертифікації ключів (АЦСК), перелік яких можна знайти на сайті Міністерства цифрової трансформації України. Підписання документів ЕЦП є найнадійнішим способом ідентифікації підписувача та фіксації волевиявлення.

У дослідженні встановлено, що кожен «підписувач» повинен мати свій, унікальний, підпис і використовувати так званий особистий ключ – код, відомий лише його власнику. Якщо цей код повідомити програмі, то відповідно

до криптографічного алгоритму вона сформує унікальне контрольне значення і додасть його до документу. Інакше кажучи, підпише електронний документ унікальним ЕЦП власника даного особистого ключа. Для перевірки вірогідності ЕЦП та цілісності електронного документа використовується інший код – так званий відкритий ключ. Цифрові підписи ідентифікують / автентифікують підписувача документа і дозволяють одержувачам документів перевіряти, що ніхто не змінив зміст документа з моменту його підписання.

Підробити електронний цифровий підпис, а разом з ним і засвідчений документ, неможливо, адже це потребуватиме величезної кількості обчислень, які, як вважається, не можуть бути реалізовані за сучасного рівня математики й обчислювальної техніки за прийнятний час, тобто поки інформація, що міститься в підписаному документі, є актуальною.

Одне з проблемних питань, що повинно вирішити законодавство у цій сфері, – це робота центрів сертифікації ключів, які мають надавати послуги цифрового підпису.

Підсумовуючи дослідження, варто зазначити що впровадження електронного цифрового підпису має багато переваг, які певним чином перекривають зазначені недоліки і проблеми з використання електронного документообігу та цифрового підпису. До таких позитивних наслідків можна віднести – юридична сила електронних документів, конфіденційність і безпека інформації, можливість ведення електронного документообігу з державними структурами, удосконалення бізнес-процесів на підприємстві, ведення ділових відносин на сучасному рівні.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Закон України Про доступ до публічної інформації. Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

2. Закон України Про електронні довірчі послуги. Відомості Верховної Ради (ВВР), 2017, № 45, ст.400. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

3. Закон України Про електронні документи та електронний документообіг. Відомості Верховної Ради України (ВВР), 2003, № 36, ст.275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

4. Технічні специфікації форматів криптографічних повідомлень. Захищені дані: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14 травня 2010 р. № 112. URL: http://www.rada.gov.ua

5. Про затвердження Вимог до форматів даних електронного документообігу в органах державної влади. Державне агентство з питань електронного урядування України. Наказ 07.09.2018. № 60. URL: https://zakon.rada.gov.ua/laws/show/z1309-18#Text

6. Про кваліфікований електронний підпис. 1 липня 2019. URL: https://www.pfu.gov.ua/kr/327258-pro-kvalifikovanyj-elektronnyj-pidpys/

7. Крупський С.Н. Захист інформації від несанкціонованого доступу в системах обробки інформації. К.: Наука, 2018. 256 с.

8. Круковський М.Ю. Рішення електронного документообігу. К.: Азимут-Україна. 2018. 112 с.

9. Кузьменко Б. В. Організаційно-правові та програмно-технічні засоби забезпечення інформаційної безпеки: навч. посібник. К.: НАУ, 2018. – 364 с.

10. Кукарін О.Б., Логвинов В.Г., Мазуркевич М.В., Марчук О.В. Ресурс інформаційний. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2018. Т.2. Методологія державного управління. – с. 545-547.

11. Кукарін О.Б., Марчук О.В. Інфраструктура електронного урядування технологічна. Енциклопедія державного управління: у 8 т. – К.: НАДУ, 2017. Т.2. Методологія державного управління. – с. 235-236.

12. Леонова О. Підписання документів онлайн: що потрібно знати HR-фахівцю про роботу з ЕЦПURL: https://hurma.work/blog/pidpisannya-dokumentiv-onlajn-shho-potribno-znati-hr-fahivczyu-pro-robotu-z-eczp/

13. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2021. Т.2. Документообіг електронний. с. 144-146.

14. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2018. Т.2. Підпис електронний цифровий. с. 447-449.

15. Матвієнко О.В. Основи організації електронного документообігу. К.: Центр учбової л-ри, 2008. 111 с.

16. Почепцов Г. Г., Чукут С. А. Інформаційна політика. К.: Вид-во «Знання», 2018. 665 с.

17. Як підписати документ в Word: покрокова інструкція Microsoft Word Document, Excel Workbook, or PowerPoint Presentation: Office 2013, 2010, and 2007. Вебтраст Україна. URL: https://pdf.com.ua/pdf_how_to_sign_office_doc.html

18. Як підписати документ в Word: покрокова інструкція Microsoft Word Document, Excel Workbook, or PowerPoint Presentation: Office 2013, 2010, and 2007. Вебтраст Україна. URL: https://pdf.com.ua/pdf_how_to_sign_pdf_doc.html

19. Цимбалюк О. Використання ЕЦП для бізнесу в Україні. *Юридична газета.* 2018. URL: https://yur-gazeta.com/publications/practice/inshe/vikoristannya-ecp-dlya-biznesu-v-ukrayini.html

20. Рибак Я. Коли без ЕЦП ніяк. Юридична газета. 2018. URL: https://yur-gazeta.com/publications/practice/inshe/koli-bez-ecp-niyak.html

21. Електронний документообіг та захист інформації: навч. посіб. К.: НАДУ, 2015. 84 с.

22. Виноградова Г.В. Правове регулювання інформаційних відносин в Україні: навч. посібник. К.: Юстініан, 2006. 176 с.

23. Гречко А.В. Основи електронного документообігу: Навч. посібник. К., 2006. 156 с.

24. Дурняк Б.В. Семантичний захист інформації в системах документообігу. Інформаційні технології. Л.: Вид-во Укр. акад. друкарства, 2010. 160 с.

25. Клімушин П.С. Електронне урядування в інформаційному суспільстві. Х.: ХарРІ НАДУ-Магістр, 2010. 312 с.

26. Пронь Н.О. Документування в Україні: сучасний стан та напрямки наукових досліджень: наук. праці Кіровоградського національного технічного університету. *Економічні науки*. Вип. 20. Ч.1. Кіровоград: КНТУ. 2011. С. 47-52.

27. Лиско Н.А. Державне регулювання у сфері електронного документообігу в Україні. *Вісник соціально-економічних досліджень*. 2013 рік, випуск 1 (48). URL: https://core.ac.uk/download/pdf/147038258.pdf

28. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика. Х.: Форт, 2010. 593 с.

29. Крутова А.С. Електронний господарський документообіг: стан та перспективи розвитку. Х.: ХДУХТ, 2012. 212 с.

30. Електронний документообіг за галуззю знань «Інформаційна безпека». Луганськ: Вид-во СНУ ім. В. Даля, 2011. 260 с.

31. Електронний документообіг у державному управлінні. К.; Х.: ФОРТ, 2009. 232 с.

32. Сойко О. Захисні елементи паспортних документів та можливі способи їх фальсифікації : навч. посіб. К. : Міжн. центр розв. мігр. політики, 2009. 240 с.

33. ЕЦП або КЕП: чим підписувати електронні документи? URL: https://biz.ligazakon.net/analitycs/200366_etsp-abo-kep-chim-pdpisuvati-elektronn-dokumenti

34. Кукарін О.Б. Електронний документообіг та захист інформації. Національна академія державного управління при презедентові України. 2019.

84 с. URL: http://academy.gov.ua/infpol/pages/dop/2/files/dcc74a43-a939-4314-8f50-f6b1e80cf498.pdf

35. Семенченко А.І. Електронне урядування та електронна демократія: навчальний посібник: Частина 9. К.: ФОП Москаленко О. М., 2017. 64 с.

36. Глєбова Н.В. Електронний цифровий підпис: обліковий та податковий аспекти. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. 2018. Вип. 18(1). С. 94-97. URL: http://nbuv.gov.ua/UJRN/Nvuumevcg_2018_18%281%29__21

37. Верес І.Я. Правове регулювання електронних підписів: Підприємство, господарство і право. 2017. С. 11-15. URL: http://pgp-journal.kiev.ua/archive/2017/3/3.pdf

38. Кучаковська Н.О. Правове регулювання укладення електронних господарських договорів.: Зовнішня торгівля: економіка, фінанси, право. 2016. – С. 62-70. URL: http://zt.knteu.kiev.ua/files/2016/6(89)/07.pdf

39. Портал державних послуг: Веб-сайт. Електронні дані. Київ. URL: https://igov.gov.ua

40. Кваліфікований надавач електронних довірчих послуг Інформаційно-довідковий департамент ДПС: Веб-сайт. Київ. URL: https://acskidd.gov.ua

41. Горкуша М. Як отримати і для чого потрібен електронний підпис в Україні. URL: https://delo.ua/business/jak-otrimati-i-dlja-chogo-potriben-elektronnij-pidpis-v-ukrajini-331060/

42. Юринець В.Є. Інформаційні системи управління персоналом, діловодства і документообігу: навч. посіб. Львів : «Тріада плюс», 2008. 628 с.

43. Демчина Л.І. Документообіг у державній службі: навч. посіб. К.: ТОВ «СІК ГРУП УКРАЇНА», 2013. 168 с.

44. Державний класифікатор управлінської документації: ДК 010-98. К.: Держстандарт України, 1999. 50 с.

45. Матвієнко О., Цивін М. Основи організації електронного документообігу: Навчальний посібник. К.:Центр учбової літератури, 2008. 112с.

46. Радченко С.В. Особливості систем електронного документообігу у державних органах України. URL: http://www.arch V ives.gov.ua/Publicat/AU/AU_4_2013/02.pdf

47. Писаренко В.П. Проблеми кібербезпеки в Україні. *Науково-практичний журнал Економіка та держава*. Серія: Державне управління №8(18), 2018.

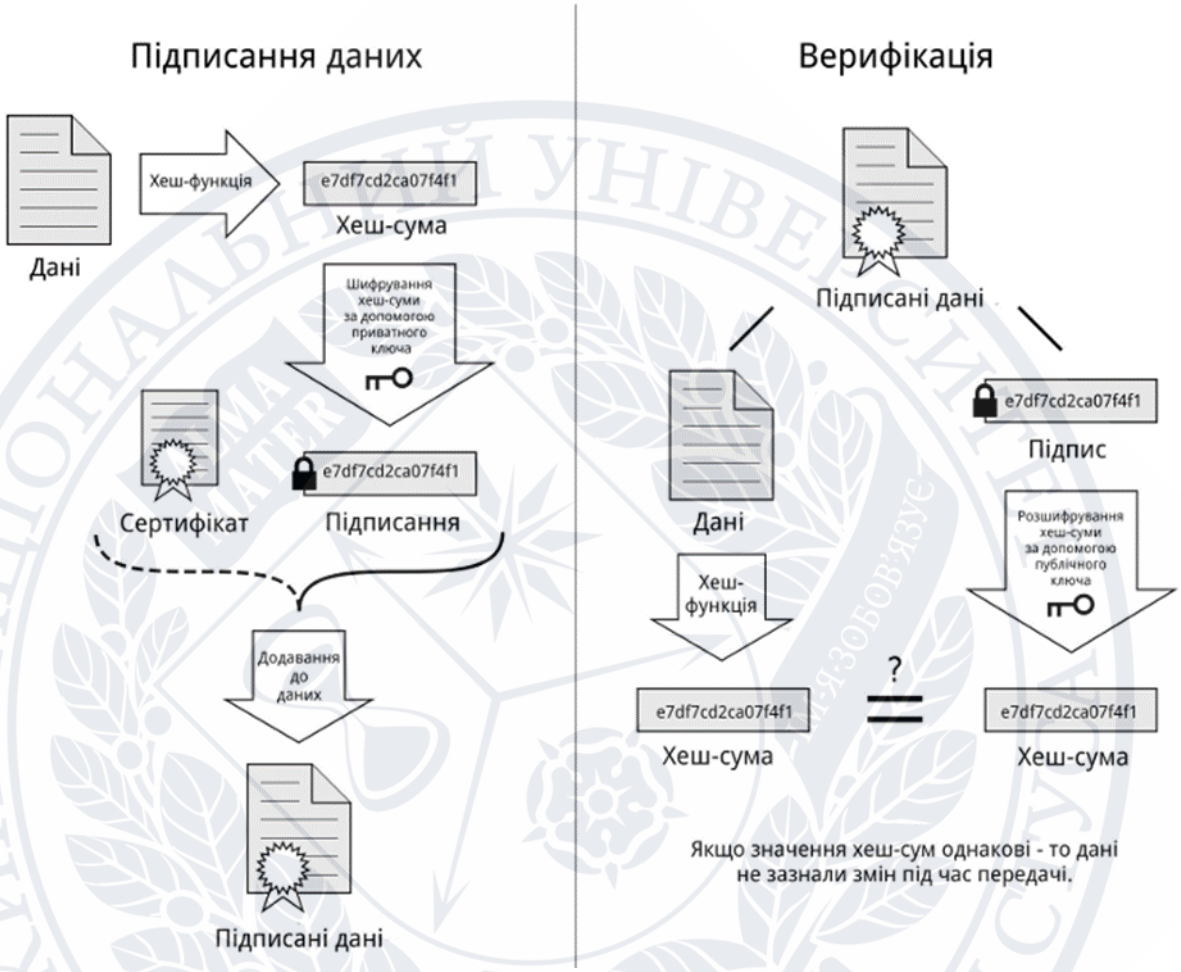
48. Писаренко В.П. Визначення понять «електронний документ» та «цифровий підпис» в зарубіжних країнах. *Університетські наукові записки*. 2011. № 4 (40). С. 384-388.

49. Писаренко В.П. Трансформація поєднання паперового та електронного документування. *Актуальні проблеми державного управління, педагогіки та психології*. Збірник наукових праць Херсонського національного технічного університету. Вип. 1(6). Херсон, 2012. С. 192-196.

50. Писаренко В.П. Електронний цифровий підпис: переваги та недоліки. Вісник Академії митної служби України. Серія: Державне управління, № 1 (6), 2012.- С.60-64.

ДОДАТКИ

ДОДАТОК А.



ДОДАТОК В

Способи захисту електронних документів