Лехов О.С.
студент,
Науковий керівник: **Деревнін В.С.**
кандидат юридичних наук, доцент,
Національний університет «Одеська юридична академія»

ОСОБЛИВОСТІ РОЗВИТКУ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ В ЦИВІЛЬНОМУ ЗАКОНОДАВСТВІ

Світ не стоїть на місці і з ровитком нових технологій розвивається і юриспруденція. Велика кількість документів вже давно перейшли в еклетронний вигляд і щоб прирівняти за юридичною силою до паперових документів їх потрібно скріпити електронним підписом. Одні з перших ЕЦП почали застосовувати публічні службовці при заповненні е-декларацій.

Електронний підпис – це отриманий за результатом криптографічного перетворення набору електронних даних. Його неможливо підробити стороннім особам, тому що він реалізується за допомогою математичного перетворення над змістом документа.

Система ЕЦП припускає, що кожен користувач має свій особистий ключ, не відомий іншим користувачам, а також ще один ключ у відкитому доступі для інших користувачів, щоб перевірити належність першого. Ще однією великою позитивною рисою користування ЕЦП є його непідробність. Той користувач який має при собі ключ, що знаходиться у відкритому доступі не може змінити чи підробити підпис що знаходиться в даному документові, тому що тому що математична основа цього ключа повністю відрізняється від інформаційних бітів електронного підпису.

Також цифровий підпис надає інформацію про особу, про зміни в документі та час його підписання і робить документ таємним, для запобігання від несанкціонованого доступу до нього.

ЕЦП не тільки надає інформацію про людину, що підписала документ, але дозволяє впевнитись, що сам документ не був змінений або підроблений після підписання. Також завдяки ЕЦП можна вказати реальний час підписання документа, на відміну від дати, вказаної у самому документі. Разом з тим, ви можете забезпечити конфіденційність

інформації, тобто шифрувати документи, отримуючи при цьому захист інформації від несанкціонованого доступу.

У сертифікать містить інформацію що закріпленна документом RFC 2459 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile). Також сертифікат містить адреси, встановлені витратні ліміти або права доступу власника сертифікату. Іншими словами, сертифікат може містити будь-яку інформацію, яку здатен опрацювати центр сертифікації.

Кожен сертифікат має свій термін дії. Це може бути термін від місяця до кількох років. Коли термін дії сертифіката спливає, користувач отримує новий.Але у цьому власне і міститься недоліки у користувані електронними документами, тому що, чим більше інформації що по потребують зміни у документі, тим більше часу потрібно користувачу щоб її змінити до закінчення терміну дії сертифікату. Також при втраті ключа чи зміні роботи користувача, потрібно відкликати сертифікат, щоб отримати мати новий.

Якщо використовувати не сертифіковані засоби, то є велика вірогідність того, що документ може бути зміненний чи підроблений, тому що у ньому не міститься тієї криптостійкості що й у сертифікованих засобах підписання. Ще один ризик з використання таких засобів полягає у неможливості доведення авторства його підписання, тому що такі засоби ніхто не перевіряв. Часто автор доводить, що ЕЦП неправильно перетворив документ, та відбулися зміни, яких він не робив і тому програма показує збій. Хоча таке відбувається досить рідко і такий ризик є просто віртуальни, але все ж не потрібно нехтувати достовірністю інтвормації що міститься на електронному носії. Тому що при використанні сертифікованих засобів криптографічного захисту це досить легко довети [1].

Пр1и використанні засобів із належною сертифікацією інформації гарантом якості виконання основної функції й відсутності бічної дії виступає Державна служба спеціального зв’язку та захисту інформації України. А при використанні несертифікованих засобів крипто-графічного захисту інформації таких гарантій не може дати ніхто.

Тому електронний документообіг спрощує роботу будь якого користувача, і вже у недалекому майбутньому ми всі будем користуватися ЕЦП, як це роблять деякі європейські країни. Також це може дуже сильно спростити виборчу систему в Україні. Виборцю буде досить відправити бланк із своїм вибором закріпленний цифровим

підписом до відповідної установи, цим самим виключити ризик фальсифікації [2].

Але найбільш істотною проблемою на сьогодні є відсутність практичного механізму застосування ЕЦП. Незважаючи на існування Закону України «Про цифровий електронний підпис» [3] до цього часу відсудній єдиний підхід що до запровадження цифрового електронного підпису у сфері інформаційних технологій невеликого центрального державного органу.Для подальшої успішної реалізації проектів з впровадження таких систем необхідно врахувати всі типові проблеми та розрахувати всі витрати на використання ЕЦП.

Список використаних джерел:

1. Yesina, O.G. The information security software in business [Електронний ресурс] / O.G. Yesina, L.N. Lingur // Економіка: реалії часу. Науковий журнал. – 2013. – № 5 (10). – С. 175-180.

2. Голобуцький О.П., Шевчук О.Б. Електронний уряд. – К.: ЗАТ «Атлант UMS», 2002. – 174 с.

3. Закон України про цифровий підпис // Відом. Верховної Ради України. – 2003. – № 36. – Ст. 276.

Панченко І.С.
аспірантка,
Київський національний університет
імені Тараса Шевченка

НОТАРІАЛЬНІ АКТИ У ПРОЦЕДУРІ НОТАРІАЛЬНОГО ПОСВІДЧЕННЯ ДОГОВОРІВ ВІДЧУЖЕННЯ НЕРУХОМОГО МАЙНА

У провадженні з посвідчення договорів відчуження нерухомого майна, як і у інших нотаріальних провадженнях нотаріус видає низку нотаріальних актів як виражених в процесуальній формі правозастосовчих рішень нотаріуса по окремій справі, які містять його волевиявлення на вчинення нотаріальної дії, прийняті ним на підставі норм матеріального та нотаріального процесуального права [1, с. 71].

У науці нотаріального процесу нотаріальні акти за процесуальною метою поділяються на основні (завершальні), якими закінчується