ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЗАХИСТ ДОКУМЕНТІВ ПІД ЧАС ПРАКТИЧНОЇ ПІДГОТОВКИ СТУДЕНТІВ

Л. М. Колєчкіна, *д. ф.-м. н., професор;*
Ю. О. Литвиненко, *асистент*
ВНЗ Укоопспілки «Полтавський університет економіки і торгівлі»

Термін «інформаційна безпека» з'явився разом з появою засобів інформаційних комунікацій між людьми, а також, з усвідомленням того, що інтересам конкретної людини може бути завдано збитку шляхом дії на засоби інформаційних комунікацій.

Інформація, з точки зору інформаційної безпеки, володіє наступними категоріями:

- конфіденційність – гарантія того, що конкретна інформація доступна лише певному колу осіб;
- цілісність – гарантія того, що інформація існує у початковому виді;
- автентичність – гарантія того, що автором інформації є особа, яка заявлена як автор;
- апелюємість – гарантія того, що за необхідності можна довести, що автором повідомлення є саме заявлена людина, а не хтось інший.

А тому студенти повинні володіти практичними та елементарними навиками підготовки документів до яких відносяться такі дії як збереження документа з паролем, надання обмеженого доступу до даного документу та електронний цифровий підпис.

Перша з цих дій дає можливість частково захистити електронний документ, оскільки не знаючи пароль, не можна скористатися даним документом, а на злам паролю піде деякий час. оскільки, при такому захисті документа, комп'ютер відрізняє великі та малі літери, то пароль бажано встановлювати такий, щоб максимально затрудняти його зламування, наприклад, використовувати як мінімум 8-10 символів, до складу яких входили б цифри, великі та малі літери, тощо.

Теж саме стосується і такої технології як надання доступу. При цьому доступ до документу може надаватися наступний: вільний доступ, лише перегляд та з правом редагування. При використанні цієї технології документ є практично незахищеним, а, тому, бажано поєднувати дану технологію з попередньою, тобто захистити електронний документ паролем.

Електронний цифровий підпис використовується для автентифікації текстів, що передаються телекомунікаційними каналами. Функціонально він аналогічний звичайному рукописному підпису й має його основні переваги:

- засвідчує, що підписаний текст виходить від особи, що поставила підпис;
- не дає цій особі можливості відмовитися від зобов'язань, пов'язаних із підписаним текстом;
- гарантує цілісність підписаного тексту.

Система ЕЦП включає дві процедури:

1) процедуру постановки підпису;
2) процедуру перевірки підпису.

У процедурі постановки підпису використовується секретний ключ відправника повідомлення, у процедурі перевірки підпису – відкритий ключ відправника.

Принциповим моментом у системі ЕЦП є неможливість підробки ЕЦП користувача без знання його секретного ключа підписування.

Документом, що підписується, може бути будь-який файл. Підписаний файл створюється з непідписаного за допомогою додавання до нього одного або більше електронних підписів.

Кожен підпис містить таку інформацію:

- дату підпису;
- термін закінчення дії ключа цього підпису;
- інформацію про особу, яка підписала файл (ПІБ, посада, коротке найменування фірми);
- ідентифікатор підписанта (ім.'я відкритого ключа);
- власне цифровий підпис.

Всі вищевказані моменти є суттєвими при збереженні електронного документу. При цьому студенти повинні вільно володіти ними і постійно їх використовувати на практиці.