Підгорна Т.В.
НПУ імені М.П.Драгоманова

Вивчення теми «електронний підпис» в курсі економічної інформатики

Інтернет – найбільша глобальна комп'ютерна мережа, за допомогою якої можна здійснювати зв'язок між користувачами всіх континентів світу. В наш час Інтернет – це ціла індустрія, що проникла у всі галузі людської діяльності. Не є винятком і комерційні процеси – процеси пов'язані із купівлею та продажем товарів, а саме:

- *дослідження ринку товарів та послуг*: вивчення споживчого попиту та з'ясування потреб населення в товарах та послугах;
- *управління властивостями товарів та послуг*: прогнозування споживчого попиту та потреб населення в товарах та послугах;
- *сповіщення ринку про властивості товарів та послуг:* рекламно-інформаційна діяльність щодо збуту товарів та надання різних послуг;
- *підготовка ринку до використання заданих властивостей товарів і послуг:* рекламно-інформаційна діяльність щодо збуту товарів;
- *приймання, опрацювання і виконання замовлень на товари і послуги*: організація і технологія оптового і роздрібного продажу товарів, надання послуг, враховуючи форми і методи продажу товарів, умови їх застосування, якість обслуговування і т.п.;
- *оптимізація товарних потоків та складських запасів:* виявлення і вивчення джерел надходження і постачальників товарів, організація і технологія проведення оптових закупівель товару у різних постачальників (на оптових ярмарках, оптових продовольчих ринках, товарних біржах, аукціонах, у виробників продукції, торгівельних посередників і т.д.), формування торгового асортименту на складах та в магазинах, управління товарними запасами;
- *взаєморозрахунки із клієнтами та постачальниками:* організація раціональних господарських зв'язків з постачальниками товарів, включаючи укладення договору (контрактів) на постачання товарів, розробку і подання заявок і замовлень на товари, організацію обліку і контролю за виконанням договірних обов'язків, різні форми комерційних розрахунків та інше;
- *післяпродажеве обслуговування:* надання і здійснення післяпродажевого обслуговування товарів [1, 2].

Торгівельна діяльність, основною метою якої є отримання прибутку та яка базується на комплексній автоматизації комерційних процесів за рахунок використання засобів інформаційно-комунікаційних технологій, називається *електронною комерцією* [2].

При організації і функціонуванні комерційного циклу велика увага приділяється здійсненню обігу супровідної документації і платіжних засобів. При реалізації такого обігу найголовнішою проблемою є аутентифікація вмісту документів (цілісність і незмінність документу) і ідентифікація осіб (підтвердження відношення до особи, яка поставила підпис), які відповідають за них. Для вирішення цих проблем використовують електронний підпис і електронний цифровий підпис (ЕЦП).

Електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних [3].

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 [3].

Враховуючи вище зазначене, стає зрозумілим, що студенти економічних спеціальностей повинні *знати*:

- поняття електронного підпису;
- поняття електронного цифрового підпису;
- технічне забезпечення електронного цифрового підпису: криптографія; метод і ключ шифрування; симетричні і несиметричні методи шифрування;
- організаційне забезпечення електронного цифрового підпису: поняття електронного сертифікату, моделі сертифікації;
- правове забезпечення електронного цифрового підпису.

Студенти повинні вміти:

- створювати ключі для здійснення шифрування за допомогою відповідного програмного забезпечення;
- підписувати з використанням ЕЦП електронні документи;
- шифрувати і дешифрувати документи, використовуючи створені ключі;
- здійснювати аутентифікацію вмісту електронних документів та ідентифікацію осіб, яким належить ЕЦП, використовуючи відповідне програмне забезпечення.

Зміст теоретичного матеріалу добирається відповідно до вимог щодо знань студентів з цієї теми, які були зазначені вище. Щодо розгляду правового забезпечення електронного цифрового підпису студентів доцільно ознайомити із законами [3 – 13], відповідно до яких здійснюється функціонування ЕЦП. Це питання можна винести на самостійне вивчення і запропонувати студентам написання рефератів з даної теми.

Засіб електронного цифрового підпису - програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису [4]. Оскільки від алгоритмів, на основі яких функціонують засоби ЕЦП, залежить надійність і стійкість документообігу, до засобів ЕЦП висуваються спеціальні вимоги. В Україні діяльність щодо розробки засобів ЕЦП відноситься до ліцензованих видів діяльності [8]. Обмежено також використання готових засобів ЕЦП. В державних і комерційних установах дозволяється використовувати тільки засоби ЕЦП, які мають сертифікат відповідності або експертний висновок відповідних державних органів [8].

Враховуючи вище зазначене, для ознайомлення студентів із принципами функціонування засобів електронного цифрового підпису доцільно розглянути або ліцензовані, або вільно поширювальні засоби, за допомогою яких можна:

- генерувати ключі;
- накладати ЕЦП на електронні документи;
- перевіряти ЕЦП, який накладено на відповідний електронний документ.

Наприклад, таким вимогам відповідає програмний комплекс *Pretty Good Privacy (PGP).*

Комплекс PGP може функціонувати як під управлінням операційної системи сімейства Windows, так і під управлінням ОС сімейства Linux. Комплекс PGP спочатку розповсюджувався абсолютно безкоштовно. Однак ситуація змінилась, PGP став комерційним продуктом, а безкоштовно розповсюджувана версія має значні обмеження. Проте навіть така FreeWare-версія PGP – є якісним продуктом, за допомогою якого можна достатньо надійно приховати конфіденційні дані від стороннього втручання. Завантажити таку версію можна за адресою

http://www.pgp.com/downloads/freeware/index.html.

PGP функціонує за принципом шифрування з відкритим ключем. Спочатку користувач створює пару ключів – невеликі текстові файли. Один ключ – закритий, інший – відкритий. Коли хтось хоче зашифрувати листа власнику пари ключів, він це робить за допомогою відкритого ключа. З того моменту, як лист зашифровано відкритим ключем, його може прочитати тільки власник закритого ключа. Навіть автор після шифрування листа відкритим ключем не може його переглянути.

Після встановлення комплексу в системному лотку панелі задач з'являється іконка модуля PGP tray. Після встановлення курсора мишки на цю іконку і натиснення на праву клавішу мишки з'являється контекстне меню, з якого можна запустити модуль PGPkeys (рис. 1).

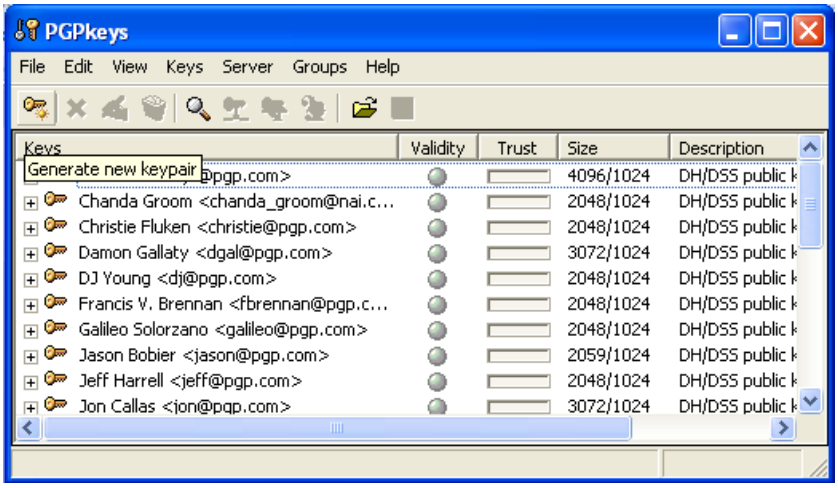

Рис. 1

Для генерації пари ключів потрібно викликати відповідний майстер, вибравши команду *Keys\New key…*

Крок 1 (рис. 2). Виведення повідомлень про призначення даного майстра.

Крок 2 (рис. 3). Введення параметрів: *Ім'я, Адреса електронної пошти.*

Задаючи *Ім'я* пари ключів, що створюються, необхідно правильно вказувати своє власне ім'я, щоб в подальшому користувачам було простіше знаходити ключі відповідних партнерів.

В полі *Адреса електронної пошти* вводиться e-mail, з якою буде встановлено відповідність для даної пари ключів.

Крок 3 (рис. 4). Встановлення розміру ключів.

Для визначення розміру ключів потрібно задати параметр *Key Pair Size* (розмір ключів), встановивши перемикач на відповідному значенні. Чим більший розмір ключів, тим складніше їх пошкодити. З іншого боку, при роботі з ключами великого розміру потрібно більше часу.

Крок 4 (рис. 5). Введення терміну дії ключа.

За допомогою параметра *Key expiration* (термін придатності ключа) можна ввести термін дії ключа, вказавши будь-яку дату, після якої ключ стане недійсним. Користувачі, які використовують цей ключ, будуть бачити термін закінчення його дії так само, як і власник ключа. Якщо виникає необхідність продовжити зашифроване листування із власником «простроченого» ключа, їм буде потрібно запросити у нього або розшукати на спеціалізованому сервері нову версію ключа.

Рис. 2

Рис. 3

Рис. 4

Рис. 5

Рис. 6

Рис. 7

Крок 5 (рис. 6). Введення пароля. На рисунку 6 не встановлено прапорець *Hide Typing* (приховувати пароль), тому відображається послідовність символів, яка є паролем в даному прикладі. Це було зроблено навмисно для того, щоб показати, як можна ускладнити пароль. В наведеному прикладі

набрано послідовність символів «Київ на Дніпрі столиця України» української розкладки клавіатури при встановленій англійській.

Потрібно ввести і підтвердити пароль, за допомогою якого можна буде здійснювати доступ для використання цих ключів. При введенні пароля показується індикатор його якості: чим довше пароль і чим більший набір в ньому символів, тим важче буде такий пароль зламати.

Після виконання наведених кроків генерується пара ключів.

Крок 6 (рис. 7). Процес створення ключів.

Далі потрібно «роздати» відкриті ключі тим, з ким буде вестись приховане листування. Це можна зробити кількома шляхами:

- зберегти ключі у вигляді файлу і відправити його кореспонденту на електронному носієві або за допомогою електронної пошти;
- розмістити його на спеціалізованому сервері. Всі користувачі PGP мають доступ до цього сервера. Потрібний ключ можна знайти за допомогою системи пошуку, яка вбудована в PGPkeys, і додати його до власної "зв'язки".

Таким чином, з кожним користувачем, чий відкритий ключ додано до "зв'язки", можна починати таємне листування

Для роботи з листами призначено модуль PGPtools.

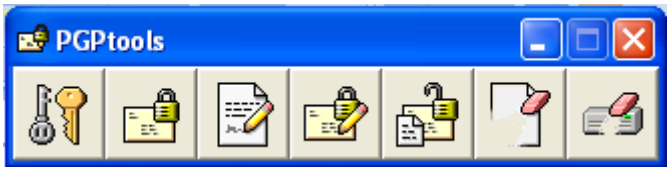

Рис. 8

Основні команди цього модуля:


PGPkeys – командна кнопка виклику PGPkeys.


Encrypt (зашифрувати). Для того, щоб зашифрувати файл або вміст буферу обміну, потрібно вибрати відповідний відкритий ключ із списку і здійснити шифрування. Зашифрований файл має те саме розширення, але піктограма інша  і його можна відправити будь-яким способом одержувачу.


Sign (підписати). Для накладання ЕЦП на електронний документ потрібно вибрати відповідний файл і потрібний власний електронний підпис. Після накладання підпису створюється новий файл з тим самим розширенням, наприклад, .doc, але має іншу піктограму  .


Encrypt and Sign (зашифрувати і підписати). З назви командної кнопки зрозуміло, що її використовують для здійснення двох операцій, які описано вище.


Decript/Verify (розшифрувати та\або перевірити підпис). За допомогою цієї кнопки здійснюється розшифрування отриманого повідомлення з використанням закритого ключа, а також перевіряється відповідність підпису.


Wipe («зачистити»). Після вилучення файлів засобами операційної системи на жорсткому диску залишаються «сліди», за допомогою яких можна поновити вилучені файли. За допомогою операції «зачистки» вилучаються з жорсткого диску не тільки вказані користувачем файли, але й і всі їх «сліди» так, що їх не можна відновити. Це здійснюється шляхом багатократного запису різних повідомлень без смислу на місце вилученого файлу.


Freespace Wipe ("зачистити" вільний простір). Ця операція доповнює попередню, її застосування унеможливлює поновлення вилучених файлів. Під час роботи з файлами його вміст дуже часто записується до різних тимчасових файлів, про які користувач може не знати. При коректному закритті документу тимчасовий файл вилучається, але його вміст може ще довго зберігатись на диску, поки на його місце не буде записано новий файл. Таким чином, вилучення файлу і навіть «зачистка» місця, де він зберігався, не дають гарантії, що дані не будуть відновлені хоча б частково. За допомогою команди *Freespace Wipe* на всі вільні місця на диску здійснюється кілька разів перезапис випадкових даних. Після такої операції неможливо відновити будь-які вилучені з диска дані.

Модуль PGPtools призначено для роботи з файлами і вмістом буферу обміну. Зашифровані або підписані файли чи вміст буферу обміну можна вставити до листа і відправити адресату. Також PGP-шифрування здійснюється за допомогою модулів підтримки PGP, які вбудовані до різних поштових програм. В цьому випадку спочатку потрібно створити в поштовій програмі лист і дати команду зашифрувати та\або підписати його і після цього відправити адресату.

Використання команд контекстного меню PGPtray дозволяє:

- запускати модулі PGP;

- зашифровувати і підписувати або, навпаки, розшифровувати і перевіряти підпис вмісту відкритого вікна або буферу обміну;
- очистити або відредагувати вміст буферу обміну.

Слід зазначити, що пункт PGPdisk контекстного меню PGPtray можуть використовувати лише власники ліцензійної версії.

Таким чином, під час ознайомлення з програмою PGP і розгляду можливостей її використання у студентів формуються вміння і навички роботи з засобом ЕЦП.

Література

1. Молоткова Н.В., Соседов Г.А. Основы коммерческой деятельности: Учеб. Пособие. Тамбов: Из-во Тамб. гос. техн. ун-та, 2004. – 152 с.
2. Информатика для юристов и экономистов / Под редакцией С.В. Симоновича. – СПб.: Питер, 2007. – 688 с.: ил.
3. Закон України «Про електронний цифровий підпис» від 22.05.2003 р.
4. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р.
5. Правила посиленої сертифікації. Затверджені наказом ДСТСЗІ СБ України №3 від 13.01.2005 р. та зареєстровані в Міністерстві юстиції України за №104/10384 від 27.01.2005 р. (зі змінами згідно Наказу № 50 від 10.05.2006 «Про внесення змін до Правил посиленої сертифікації»).
6. Наказ № 50 від 10.05.2006 «Про внесення змін до Правил посиленої сертифікації» Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.
7. Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису. Затверджено наказом ДСТСЗІ СБ України №31 від 30.04.2004 р. Зареєстровано в Міністерстві юстиції України за №592/9191 від 12.05.2004 р.
8. Постанова Кабінету Міністрів України від 26.05.2004 р. №680 «Про затвердження Порядку наявності електронного документу (електронних даних) на певний момент часу».
9. Постанова Кабінету Міністрів України від 13.06.2004 р. №903 «Про затвердження Порядку акредитації центру сертифікації ключів».
10. Постанова Кабінету Міністрів України від 28.10.2004 р. №1451 «Про затвердження Положення про Центральний засвідчувальний орган».
11. Постанова Кабінету Міністрів України від 28.10.2004 р. №1452 «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності».
12. Постанова Кабінету Міністрів України від 28.10.2004 р. №1453 «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади».
13. Постанова Кабінету Міністрів України від 28.10.2004 р. №1454 «Про затвердження Порядку обов'язкової передачі документованої інформації».
14. http://www.pgp.com