Для оцінювання фінансової ефективності проекту важливо враховувати фактор часу, який впливає на дисконтування грошових потоків, які утворюються в ході реалізації проекту.

Як вже було зазначено вище, в процесі керування рівнями ризиків у інвестиційній діяльності основною метою є утримання оптимального співвідношення “фінансова ефективність – ступінь ризику”. З цією метою до мого проекту створення експертної системи керування ризиками в інвестиційній діяльності застосований алгоритм Воронова-Максимова для визначення комплексного показника оцінки ступіня ризику [3]. Цей показник дозволяє отримати кількісну оцінку ступіня ризику проекту, враховуючи наступні кількісні похідні критерії інвестиційного проекту з урахуванням фактору часу:

1) загальна тривалість проекту;
2) об′єм стартових інвестицій;
3) діапазон варіації ставки дисконтування;
4) крайові значення чистого грошового потоку.

Алгоритм базується на теорії нечітких множин Лотфі Заде. В рамках виконання алгоритму вираховуються значення чистої поточної вартості (NPV_{min}, NPV_{avg}, NPV_{max}) та будується тріангулярна нечітка змінна, за якою обчислюється значення комплексного показника ступіня ризику [3].

Список літератури: 1. *Волков А.* Инвестиционные проекты: от моделирования до реализации. http://www.businessproekt.ru/articles/ **2.** *Ковалев В.В.* Методы оценки инвестиционных проектов. – М.: Финансы и статистика, 2000. **3.** *Недосекин А.О., Максимов О.Б.* Новый комплексный показатель оценки финансового состояния предприятия. http://www.vmgroup.sp.ru

УДК 004.056

ВАРЛИГІНА А.Ю., ПОШТАРЕНКО В.М., канд. техн. наук

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО БІЗНЕСУ З РОЗРОБКОЮ ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ СТАНДАРТУ ДСТУ 4145-2002

Бурхливий розвиток комп’ютерних технологій, використання Інтернету в бізнесі змінює сталі способи ведення бізнесу. Крім уже звичних задач по

захисту переданої інформації від прочитання й перекручування, електронний документообіг породив і нові задачі, що раніше вирішувалися тільки в «паперових» технологіях – приміром, формування підпису під документом, одержання квитанції про його вручення. Тепер ці задачі стало необхідно вирішувати й у рамках електронного документообігу[1].

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 підписувала [2].

Розглянемо схему електронного цифрового підпису, запропоновану [3]:

1) параметр безпеки n, яким може бути довжина підпису, довжина блоків даних, що підписуються тощо;

2) простір вихідних повідомлень;

3) максимальне число підписів, які можуть бути отримані в даній схемі без заміни секретної інформації;

4) алгоритм G генерації ключів, що формує по заданому параметрі n пари $\{SK_A, PK_A\}$, де SK_A – секретний ключ відправника (абонент А) повідомлення, а PK_A – відповідний відкритий ключ перевіряючої сторони (абонент В);

5) алгоритм S формування електронного цифрового підпису, що виробляє по заданому вихідному повідомленню М и секретному ключу SK_A підпис sign для повідомлення М;

6) алгоритм V перевірки, що дає на виході при заданих повідомленню М, відкритому ключу PK_A й можливому підпису sign або значення 1, коли підпис вірний, або 0, коли підпис відхилено.

В класичній схемі електронного цифрового підпису передбачається, що підписуючий (абонент А) знає зміст повідомлення документу М, який підписує. Перевіряючий (абонент В), знаючи відкритий ключ перевірки підпису, може будь-коли перевірити правильність підпису без дозволу або участі відправника А. При створенні електронного цифрового підпису згідно до класичної схеми претендент А виконує наступні дії:

1) застосовує до вихідного повідомлення М хеш-функцию Н і формує хеш-образ Н(М) (хеш-образ – це функція Н всіх бітів повідомлення, що одержує на вхід повідомлення М довільної довжини, а на вихід видає хеш-образ Н(М) фіксованого розміру);

2) обчислює електронний цифровий підпис sign із використання несиметричного криптоалгоритму D і секретного ключа SK_A створення електронного цифрового підпису: sign={H(M)}SK_A.

Послідовність дій абонента B, що отримав повідомлення:

1) верифікатор B застосовує до тексту отриманого повідомлення M хеш-функцію H і отримує хеш-образ H(M) повідомлення;

2) застосовує до отриманого підпису sign асиметричний криптоалгоритм E з використанням відкритого ключа перевірки електронного цифрового підпису PK_A і зрівнює отримане значення PK_A {sign} із обчисленим на попередньому етапі хеш-образом, при позитивному результаті порівняння підпис приймається, інакше відхиляється.

Національний стандарт України [4] електронного підпису ґрунтуються на еліптичних кривих. Схема електронного цифрового підпису при цьому відповідає зазначеній вище, але як числа, використаються еліптичні числа – рішення рівняння еліптичних кривих над зазначеними скінченими полями [5]. Цей стандарт установлює механізми цифрового підписування, що ґрунтуються на властивостях груп точок еліптичних кривих над полями $GF(2^m)$ [6, 7], та правила застосування цього механізму до повідомлень, що їх пересилають каналами зв'язку та/ або обробляють у комп'ютеризованих системах загального призначення.

Список літератури: ***1.*** *Брод М.* Криптозащита и электронная подпись. http://www.trusted.ru/company/pressroom/infobez/03/ **2.** Закон України "Про електронний цифровий підпис" **3.** Деднев М.А., Дыльнов Д.В., Иванов М.А. Защита информации в банковском деле и электронном би знесе. – М.: Кудиц-Образ, 2004. – 512с. **4.** ДСТУ 4145-2002 Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. **5.** *Винокуров А.* Стандарты аутентификации и ЭЦП России и США. http://www.trusted.ru/company/pressroom/infobez/09/ **6.** *Лидл Р., Нидеррайтер Г.* Конечные поля: Т.1. – М.:Мир, 1988. – 430с. **7.** *Биркгоф Г., Барти Т.* Современная прикладная алгебра. – М.:Мир, 1976. – 400с.