| | | | | |
|---|---|---|---|---|
| | | | вища середнього | вС |
| | | | висока | В |
| $z_2$ | відстань між матрицею і роликами | 0-1 мм | мала | М |
| | | | нормальна | Н |
| | | | велика | В |
| $z_3$ | температура матриці | 20-120 град. | низька | Н |
| | | | середня | С |
| | | | висока | В |
| $z_4$ | тиск в системі затискання роликів | 150-250 Бар | низький | Н |
| | | | середній | С |
| | | | високий | В |
| $z_5$ | наявність модифікаторів | 0-3 % | відсутні | Ві |
| | | | присутні | Пр |
| $v_2$ | діаметр отворів матриці D | 6-8 | малі | М |
| | | | середні | С |
| | | | великі | В |
| $v_3$ | відношення довжини отвору до діаметра L/D | 3.5-5 | низьке | Н |
| | | | нижче середнього | нС |
| | | | середнє | С |
| | | | вище середнього | вС |
| | | | велике | В |
| $v_4$ | кут зенкування | 20-40 град. | низький | Н |
| | | | середній | С |
| | | | високий | В |
| $v_5$ | швидкість обертання привідного вала | 1.15:1; 1:1; 1:1.15 | низький | Н |
| | | | середній | С |
| | | | високий | В |
| $x_1$ | рівень зношеності матриці | 0-5 у.о | низький | Н |
| | | | середній | С |
| | | | високий | В |
| $x_2$ | рівень зношеності роликів | 0-5 у.о | низький | Н |
| | | | середній | С |
| | | | високий | В |

Для моделювання багатомірної залежності "вхід – вихід" доцільно використовувати ієрархічні системи нечіткого виведення [4]. В таких системах вихід одної бази знань подається на вхід іншої, що має вищий рівень ієрархії. Застосування такого підходу дає змогу уникнути великих розмірностей, та виключає потребу фазифікації – дефазифікації проміжних змінних. Це спрощує побудову експертної системи і робить її прозорою.

Аналіз процесу гранулювання [1] дав змогу побудувати ієрархічну систему нечіткого виведення із кількістю входів на кожному з рівнів, що не перевищує рекомендованого рівня 5 [3]. Внаслідок того отримано дерево логічного виведення (рис. 2). У табл. вказано фактори впливу як лінгвістичні змінні. Дерево логічного виведення, що має у своїй вершині продуктивність гранулятора, містить такі відгалуження, що описують: якість подрібненої сировини; якість налаштувань технологічних параметрів; якість апаратного забезпечення, яка, своєю чергою, містить відгалуження, що описує стан спрацювання основних механічних вузлів – матриці та роликів.





**Висновки**. За результатами експериментальних досліджень процесу гранулювання подрібнених деревинних відходів листяних порід створено базовий варіант експертної системи. Вона спирається на дерево логічного виведення, що описує взаємодію основних компонентів і факторів, які впливають на процес гранулювання. Нагромаджена база знань є необхідною передумовою для створення подалі автоматизованої системи керування процесом гранулювання та оптимізації її основних параметрів.

## Література

1. Бобович Б.Б. Переработка отходов производства и потребления : справ. пособ. / Б.Б. Бобович, В.В. Девятин. – М. : Изд-во "Интернет инженеринг", 2000. – 496 с.

2. Облагораживание твердых материалов путем прессования на прессах с плоской матрицей. [Электронный ресурс]. – Доступный с http://www.amandus-kahl-group.de/kahl_ grupe/ru/home/.

3. Ротштейн А.П. Интелектуальные технологии идентификации: нечеткая логика, генетические алгоритмы, нейронные сети / А.П. Ротштейн. – Винница : Вид-во УНІВЕРСУМ-Вінниця, 199. – 320 с.

4. Штовба С.Д. Проектирование нечетких систем средствами MATLAB / С.Д. Штовба. – М. : Вид-во "Горячая линия – Телеком", 2007. – 288 с.

***Куцик А.С., Курка Р.Р.*** **Экспертная система для реализации нечетких алгоритмов управления технологическим процессом гранулирования**

Рассмотрены проблемы построения автоматизированных систем управления гранулятором с плоской матрицей для переработки отходов деревообрабатывающей промышленности. Предложен вариант экспертной системы с применением нечетких алгоритмов для прогнозирования производительности процесса гранулирования и создания базы знаний о взаимодействии его основных составляющих.

***Ключевые слова:*** гранулятор, топливные гранулы, переделывания отходов, нечеткие множественные числа, экспертная система.

***Kucyk A.S. Kurka R.R.*** **Expert system for the implementation of fuzzy algorithms for granulation process control**

Specific of automatic control system of fuel pellets formation technology of particulate materials is given. Created an expert system for modelling exploitation regimes of pellet press. All conclusions are grounded on fuzzy logic which is popular in the adaptive management systems nowadays.

***Keywords:*** pellet press, fuel pellet, waste disposal, fuzzy logic, expert system.

***УДК 004.056.55***

***Студ. П.Ю. Грицюк – НЛТУ України;***
***проф. Ю.І. Грицюк, д-р техн. наук – Львівський ДУ БЖД***

## ЕЛЕКТРОННІ ГРОШІ – НОВЕ ДОСЯГНЕННЯ КРИПТОГРАФІЇ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Розглянуто особливості впровадження електронних грошей як оперативного, надійного та анонімного засобу платежу в Україні, які є новим досягнення криптографії та сучасних інформаційних технологій. Встановлено, що в системі електронних грошей використовуються два ключі: індивідуальний, призначений для підтвердження вартості купюр, і загальнодоступний – для перевірки їх достовірності при проведенні платежів. Ґрунтуючись на особливостях однонаправлених функцій, які гарантують неможливість відновлення індивідуального ключа підпису за загальнодоступним ключем його перевірки, в електронних грошах використовується схема "сліпого" електронного підпису, яка забезпечує високий рівень їх анонімності.

***Ключові слова:*** готівкові розрахунки, електронні платежі, електронні гроші, криптографічний захист, інформаційні технології, "сліпий" електронний підпис.

**Вступ**. За останнє десятиліття український ринок електронних банківських технологій пройшов помітний шлях від початкової стадії комп'ютеризації, тобто реалізації простих банківських операцій на базі персональних комп'ютерів, до повноцінних автоматизованих банківських систем [2], які відповідають найстрогішим сучасним вимогам [1]. Багато хто з нас вже звик до таких понять як електронні платіжні документи з цифровим підписом, автоматизовані системи клієнт-банк, системи обслуговування клієнтів за допомогою смарт-карт і т.ін., починаємо використовувати можливості електронної торгівлі через мережу Інтернет [4]. Проте в галузі інформаційних технологій, які є сьогодні найбільш перспективними, у нас ще багато не тільки не використаних, але й навіть не завжди чітко усвідомлених нових можливостей. Однією з них є застосування так званих "*електронних грошей*[1]*"* [5].

Хоча сучасні системи безготівкових електронних платежів [4], будь-то електронні міжбанківські розрахунки, електронні платіжні документи в системах клієнт-банк або оплата товарів і послуг приватними особами за дебетними або кредитними картками (вони є основним видом оплати товарів і послуг в західноєвропейських країнах і США), мають очевидні переваги [10], проте готівка і в цих країнах зовсім не вилучена з обігу, а навпаки, становить набагато більшу частку (до 40 %) від загальної грошової маси, ніж в Україні. У чому ж причина такого явища? На це та багато інших запитань спробуємо дати відповіді у цьому дослідженні, що і становить основну його мету.

**1. Переваги готівкових розрахунків**. Головні переваги готівкових розрахунків, які дають змогу їм благополучно співіснувати зі всіма нововведеннями електронних платіжних систем [8] і навіть не сильно втрачати свої позиції, це оперативність, велика надійність і, основне, анонімність [9]. Попри всі переваги сучасних систем електронних платежів, які можуть забезпечити тільки одну з цих властивостей – оперативність, ступінь надійності будь-якого, навіть крупного комерційного банку, все-таки є нижчою, ніж ступінь надійності національної грошової системи загалом.

Звичайно, в країнах із розвиненою банківською системою таких проблем, як проходження грошей з одного міста в інше протягом 2-3 днів, зазвичай, не буває. Тому готівкова валюта, яка емітується національним банком, розглядається в багатьох ситуаціях як більш надійна гарантія збереження капіталу. Найближчі приклади фінансової кризи і навіть закриття великої кількості українських державних і комерційних банків набагато наочніше нам це продемонстрували, ніж декілька повчальних прикладів, підібраних спеціально для нас з історії європейської чи американської банківських систем. Однак головна перевага готівкових розрахунків полягає в їх анонімності.

[1] Електро́нні гро́ші (також відомі як e-money, е-гроші, електронна готівка, електроні обміни, цифрові гроші, цифрова готівка чи цифрові обміни) – означення грошей чи фінансових зобов'язань, обмін і взаєморозрахунки з якими проводяться за допомогою інформаційних технологій. Електронні гроші є важливим концептом електронної комерції та електронного врядування. Для користування ними потрібна інфраструктура – комп'ютерні мережі, мережа Інтернет та електронні платіжні сервіси.





Як би там не стверджували можновладці, що ця властивість готівки необхідна насамперед тіньовому бізнесу і кримінальним структурам, проте навіть для будь-якого легального бізнесу вона є надзвичайно бажаною насамперед для оперативного ведення господарської діяльності.

Відомо, що ринкова економіка, при всій її "відвертості" та "прихильності до споживача", тримається на конкуренції, а точніше – на жорсткій конкурентній боротьбі виробників товарів і надання послуг за свою частку на ринку праці. Найзапеклішою ця боротьба проявляється у конкуренції на фінансових ринках, де переміщення значного обсягу капіталу відбувається деколи майже миттєво. Не даремно ж крупні інвестиційні компанії та фонди рекламують себе перед рядовим виробником у вигляді найгрізніших представників джунглів – тигрів, слонів, левів, горил і т. ін., переконуючи їх у тому, що у фінансових джунглях вони відчувають себе не менше упевнено й гарантують промисловцям виживання у скрутний час.

А в будь-якій боротьбі інформація про подальші ходи суперника і можливість приховати від нього свої наміри часто дає вирішальну перевагу. Анонімність готівкових розрахунків дуже часто використовується і зараз навіть крупними промисловими чи фінансовими компаніями для забезпечення такої переваги в боротьбі на фінансових ринках [9].

**2. Переваги електронних платежів**. У сучасних системах безготівкових розрахунків кредитні картки порівняно з готівкою, яка, здавалося б, мала давно відійти в минуле, мають такі переваги [5]:

- немає потреби мати при собі велику суму грошей і піддаватися загрозам крадіжки або пограбуванню, чи нести великі витрати на охорону;
- пластикові картки зручні у використанні, зберігання та можуть бути легко замінені в разі втрати або псування за незначну суму;
- досить широкий асортимент філіалів банків їх обслуговування та банкоматів, які обслуговують картки більшості міжнародних платіжних систем;
- більшість банків обслуговують платежі за кредитними картками, знімаючи при цьому сповна прийнятні комісійні за надання таких послуг;
- умови видачі кредитних карток приватним особам дедалі лібералізуються практично в усіх країнах світу;
- власникам привілейованих карток надається все більша кількість додаткових послуг у вигляді цінових знижок на проживання в готелях, придбання авіаквитків, оплату товарів у мережі магазинів і т. ін.

Окрім цього, більшість закордонних банків, а також деякі банки України [3] останнім часом широко практикують відкриття рахунку клієнтом через мережу Інтернет і самостійну його роботу з декількома відкритими рахунками в межах дозволених операцій: переказ коштів з рахунку на рахунок з метою отримання вищих відсотків, здійснення поточних платежів і т. ін.

**3. Перспективи впровадження електронних платежів в Україні**. Останнім часом ті переваги електронних платіжних систем [3, 9, 10], про які йшлося вище, помітно покращили свої позиції. В основному це сталося завдяки новим досягненням в області інформаційних технологій і, зокрема, неабияким здобуткам телекомунікаційних систем і криптографії[1], які загалом

[1] Криптогра́фія (від грецького kryptós – прихований і graphein – писати) – наука про математичні методи забезпечення конфіденційності (неможливості читання інформації стороннім) і автентичності (цілісності та

дали змогу проводити розрахунки практично без затримок (у режимі on-line) і з гарантією юридичної значущості передаваних каналами зв'язку електронних документів: виписок про стан рахунків, чеків, квитанцій і т. ін. Дійсно, з появою сучасної комп'ютерної техніки стало можливим практичне застосування технології електронного цифрового підпису[1] відправлених документів, а сама вона з'явилася внаслідок того, що криптографи розробили надійні алгоритми його перевірки [6], які не дають змоги зловмисникам цей підпис підробити за реальний проміжок часу. У сукупності це дає змогу застосовувати його як законний засіб підтвердження достовірності електронного документа та автентифікації[2] особи, відповідальної за його вміст.

Аналогічні криптологічні ідеї дали змогу побудувати системи забезпечення конфіденційності електронних повідомлень, які передаються відкритими каналами зв'язку. Як наслідок, у рядового користувача персонального комп'ютера без застосування всяких дорогих "шифрувальних засобів" з'явилася можливість захистити свою інформацію при її передачі не менш надійно, ніж при міжбанківських платежах у сотні мільйонів доларів у системі SWIFT[3]. В Україні так сталося, що всі конкретні проблеми сучасних взаємин невеликих фірм-розробників у цій області знань з урядовими організаціями породжені саме цим парадоксом. Навіть тепер деякі державні чиновники ніяк не можуть змиритися з тим, що зараз маленькі компанії або навіть окремий програміст може легко розробити програму захисту даних для пересічного користувача з таким же рівнем безпеки, який раніше був доступний тільки для систем засекреченого каналу урядового зв'язку.

Вочевидь, ситуація абсолютно аналогічна тій, коли персональний комп'ютер, обчислювальна потужність та надійність роботи якого у стократ перевершує величезні обчислювальні машини 80-90-х років вартістю у багато сотень тисяч доларів, зараз може зібрати в своєму підсобному приміщенні яке-небудь ТзОВ "Винники, Лтд." чисельністю в два працівника і коштує він менше тисячі доларів. Але до цього факту вже всі звикли, позаяк технологія складання таких комп'ютерів стала масовою. Те ж саме відбувається зараз на наших очах і з новими технологіями захисту інформації. Особливо наочно це виявилося з масовим впровадженням мережі Інтернет [4].

**4. Поєднання електронних платежів і готівкових розрахунків**. Зрозуміло, що у пересічного читача може виникнути зовсім природне запитання: "А чи не можна поєднати всі переваги систем електронних платежів з основною перевагою готівки – анонімністю?". Виявляється – можна [9]. Вперше ідею так званих "електронних грошей" або "електронної готівки" (E-cash) запропонував американський фахівець з теорії складності та відомий бізнесмен Девід Чоум (David Chaum) [6] ще наприкінці 70-х років на хвилі ейфорії довкола перших систем цифрового підпису і цифрових конвертів на основі перетворень з двома ключами (паролями): "відкритим" або загальнодоступним (public) і "закритим" або індивідуальним (private). На цих самих принципах можна домогтися також і анонімності операцій, які проводяться між банками і клієнтами, зберігаючи при цьому можливість доведення їх правомірності в подальших податкових звітах. Як і в звичайних системах цифрового підпису, в системі електронних грошей використовуються ключі двох видів: індивідуальні ключі призначені для підтвердження вартості купюр, а загальнодоступні – для перевірки їх достовірності при проведенні платежів.

Ідею системи "сліпого" цифрового підпису запропонував вчений-криптограф Девід Чоум [5]. Сутність його ідеї полягала в тому, що підписувач (платильник) інформації бачить її тільки в необхідній йому частині, але своїм цифровим підписом завіряє достовірність всієї інформації. Водночас банк-емітент бачить номінал купюр, але не знає їх серійних номерів, які знає тільки їх власник. При цьому криптографічно доводиться, що таким "сліпим" підписом гарантується достовірність всього вмісту купюри з тією ж надійністю, що і звичайним цифровим підписом, який є засобом підтвердження достовірності електронних документів.

Комп'ютерних систем "сліпого" цифрового підпису за минулі три десятиліття було винайдено небагато. Найбільш відомі з них запатентував сам Девід Чоум. Зараз він очолює голландську компанію DigiCash, яка реалізує близько двох десятків конкретних пілотних проектів у області електронних грошей для західноєвропейських і американських банків, а також різних фінансових компаній. Ґрунтуючись на своєму know-how[1] в області однонаправлених функцій, тобто функцій, які гарантують неможливість відновлення індивідуального ключа підпису за загальнодоступним ключем його перевірки, у роботі [3] запропоновано схему роботи "сліпого" підпису (рис.).

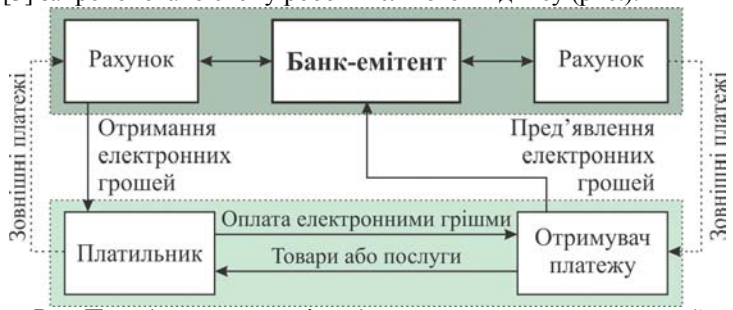


***Рис. Проведення платежів за допомогою електронних грошей***

справжності авторства) інформації. Розвинулась з практичної потреби найнадійніше передавати важливі відомості. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри.

[1] Електронний цифровий підпис (ЕЦП) (англ. digital signature) – 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.

[2] Автентифікація (з грец. αυθεντικός – реальний або істинний) – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора. З позицій інформаційної безпеки, автентифікація є частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації і передує авторизації.

[3] Платіжна система SWIFT – провідна міжнародна система у сфері фінансових телекомунікацій, яка забезпечує оперативну, безпечну і абсолютно надійну передачу фінансових повідомлень в усьому світі.

[1] Ноу-хау (від англ. know how – знаю як) або секрет виробництва – це відомості будь-якого характеру (винаходи, оригінальні технології, знання, уміння і т. п.), які охороняються режимом комерційної таємниці й можуть бути предметом купівлі-продажу або використовуватися для досягнення конкурентної переваги над іншими суб'єктами підприємницької діяльності.

При емісії електронних грошей ця система забезпечує той самий рівень анонімності, що і схема Чоума, але може бути реалізована значно ефективніше і компактніше за рахунок дещо повнішого використання можливостей комп'ютера. Це дає змогу реалізовувати систему обігу електронних грошей еквівалентно найбільш стійкому з відомих алгоритмів, не порушуючи при цьому чужих патентних прав на поширеній зараз в українських банках комп'ютерній техніці [1].

Опишемо на понятійному рівні (без використання математичних формул) основні процедури обігу електронних грошей [5]:

1) Покупець генерує на своєму комп'ютері так звані "електронні банкноти" (звичні рядки букв і цифр), які містять їх номінал, наприклад 10, 20, 50 чи 100 грн, і для кожної з них – індивідуальні серійні номери, які тільки знає він і "ховає" ту частину кожної купюри, що містить серійний номер, у спеціальний "цифровий конверт" (зрозуміло, поки що такі купюри не мають вартості).
2) Тільки банк-емітент може присвоїти вартість конкретним купюрам електронних грошей. Він перевіряє номінали направлених покупцем купюр, але не може визначити їх закриті серійні номери.
3) Банк-емітент підписує своїм "сліпим" цифровим підписом купюри, знаючи їх номінали, але не знаючи серійних номерів, і повертає їх покупцеві вже завіреними. Звичайно, банк зажадає для цього від покупця завчасно депонувати відповідні суми звичайних грошей або оформити кредитний договір.
4) Покупець "виймає" з цифрових конвертів "заховані" купюри і може ними розплачуватися за товари чи послуги, позаяк це законні засоби платежу. Отже, у покупця є електронні гроші, які мають визначену і підтверджену банком вартість, якими він може користуватися, як йому заманеться. При цьому ніхто не зможе встановити, за що саме покупець ними розплатився з кимось конкретно, але якщо він збережете (запам'ятає) копію купюри, то зможете при потребі довести, на що її витратив.
5) Продавець, отримавши від покупця електронні банкноти, пред'являє їх банку, який перевіряє їх достовірність, дезавуює їх серійні номери і проводить зарахування відповідних сум на рахунок продавця або оформляє йому нові електронні банкноти на відповідну суму.
6) Цикл обігу електронних грошей завершений.

Звичайно, без точного математичного опису наведена вище схема обігу електронних грошей виглядає не настільки переконливою, яка вона є насправді, але основні ідеї її реалізації все ж таки зрозумілі. Технічно всі операції можуть бути практично реалізовані на будь-якій офісній техніці, що реально використовується зараз багатьма банками. Найскладніший момент полягає в тому, аби забезпечити онлайновий доступ продавцям до банківської системи оброблення електронних банкнот, але це сповна реально вже зараз для багатьох банків. При цьому є можливість розділити дрібні банкноти, середні та великі, що дає змогу дуже точно регулювати ступінь ризику при емісії електронних грошей.

**5. Практична можливість обігу електронних грошей**. Отже, криптографія та інформаційні технології забезпечують практичну можливість обігу електронних грошей в Україні вже зараз і без великих витрат на реалізацію такого проекту [3, 9, 10]. Тепер на перший план виходять питання економічні, політичні та моральні. З економічної точки зору, вигоди для банку-емітента електронних грошей очевидні:

- по-перше, він отримує на депонент реальні безготівкові або готівкові гроші, якими забезпечується емісія електронних грошей;
- по-друге, він отримує відсотки за обслуговування;
- по-третє, він отримує можливість працювати з "залишками" сум електронних грошей, не пред'явлених до оплати.

Загалом, це додаткові і, здебільшого, гарантовані фінансові ресурси: засоби, що депонують клієнти, банк може пустити в обіг повністю і відразу, а з їх залишками – працювати як із звичайними залишками грошей на рахунках клієнтів. Контроль з боку Центрального банку України за обсягом емісії електронних грошей конкретним банком-емітентом або всіма банками-емітентами також досягається звичайними методами банківського контролю та регулювання.

Економічні інтереси клієнта тут також зрозумілі – на додаток до всіх переваг повсякденних платежів за допомогою електронної картки він отримує можливість проводити їх анонімно, не маючи при собі великих сум реальних фізичних банкнот. Також він має змогу оперативно оплачувати товари і послуги, не розкриваючи перед банком або іншими особами, кому і за що він провів оплату, але за потреби може точно довести навіть в суді, що провів оплату певного товару або послуги конкретному продавцеві.

Залишаються економічні, а з ними, як наслідок, ще й політичні інтереси держави, а саме [10]:

1) Держава звільняється від потреби підтримувати й оновлювати велику масу готівки, забезпечувати їх надійний захист від підроблення сучасними вельми дорогими засобами, здійснювати надійну охорону при друкуванні, зберіганні в ЦБ і розподілі регіонами. При емісії електронних грошей всі ці проблеми вирішуються набагато простіше і ефективніше. Витрати на обслуговування клієнтів при цьому банки перекладають на самих клієнтів, забезпечуючи їм додаткові зручності, про які вже було сказано вище.
2) Наявність електронних грошей практично зменшить можливість зловживань з боку виконавців правоохоронних органів при проведенні юридично правочинних дій з накладання арешту на майно, конфіскацію, обшуки і т.д. Відомо, що скористатися незаконно привласненими електронними грошима значно складніше, ніж звичайною готівкою.
3) Обіг електронних грошей стимулює фіскальні органи держави і законодавців до швидшого введення прийнятої у всьому цивілізованому світі нормальної системи контролю за податками законними методами з боку витрат платника податків, а не шляхом "вибивання" з кожного платника хто скільки зможе будь-якими методами.

У сукупності усе це сприяє будь-якому уряду держави в досягненні його головної мети – організації такого суспільства, у якому б економіка, яка динамічно розвивається, гарантувала дохід її громадян, достатній не тільки для виживання як нації, але й для підтримки нормального функціонування

оборонної структури і органів правопорядку, а також науки, мистецтва, культури, освіти, охорони здоров'я і т. ін.

**Висновки:**

1. З'ясовано, що сучасні системи безготівкових електронних платежів, які широко використовуються в більшості країн світу, маючи очевидні переваги перед готівковими розрахунками, призвели до того, що готівка в цих країнах зовсім не вилучена з обігу, а навпаки, становить значну частку (до 40 %) від загальної грошової маси.

2. Виявлено, що основні переваги готівкових розрахунків, які дають змогу їм благополучно співіснувати зі всіма нововведеннями електронних платіжних систем, це оперативність, велика надійність і анонімність, що навіть для будь-якого легального бізнесу є надзвичайно бажаними властивостями насамперед для оперативного ведення господарської діяльності.

3. Встановлено, що з появою сучасної комп'ютерної техніки стало можливим практичне застосування технології електронного цифрового підпису відправлених документів, а сама вона з'явилася внаслідок того, що криптографи розробили надійні алгоритми його перевірки, які не дають змоги зловмисникам цей підпис підробити за реальний проміжок часу.

4. З'ясовано, що як і в системі електронного цифрового підпису, так і в системі електронних грошей використовуються ключі двох видів: індивідуальні ключі призначені для підтвердження вартості купюр, а загальнодоступні – для перевірки їх достовірності при проведенні платежів.

5. Грунтуючись на особливостях однонаправлених функцій, які гарантують неможливість відновлення індивідуального ключа підпису за загальнодоступним ключем його перевірки, в електронних грошах використовується схема "сліпого" електронного підпису, яка забезпечує надзвичайно високий рівень їх анонімності, а також може бути реалізована на звичайних комп'ютерах, які широко використовуються в торгівлі та банківській системі України.

## Література


1. Автоматизовані банківські системи та їх структура. [Електронний ресурс]. – Доступний з http://ru.osvita.ua/vnz/reports/bank/20377/
2. Автоматизована банківська система Б2. [Електронний ресурс]. – Доступний з http://www.csltd.com.ua/uk/products-ua/for-banking/abs-b2.html
3. Електронні гроші як засіб платежу в Україні. [Електронний ресурс]. – Доступний з http://ua.prostobiz.ua/biznes/upravlinnya_biznesom/statti/elektronni_groshi_yak_zasib_platezhu_v_ukrayini
4. Електронні платіжні системи Інтернету. [Електронний ресурс]. – Доступний з http://www.blogs.biz.ua/blog.php?user=judin&note=189
5. Лебедев А.Н. Электронные деньги: миф или реальность / А.Н. Лебедев. [Электронный ресурс]. – Доступный с http://citcity.ru/13128/
6. Панасенко С.П. Основы криптографии для экономистов : учебн. пособ. / под ред. Л.Г. Гагариной / С.П. Панасенко, В.П. Батура. – М. : Изд-во "Финансы и статистика", 2005. – 176 с.
7. Савчук Дмитро. Електронні гроші – не гроші? / Дмитро Савчук. [Електронний ресурс]. – Доступний з http://www.kyivpost.ua/opinion/op-ed/elektronni-groshi-ne-groshi-35984.html
8. Скорпіо Л. Електронні платіжні системи в Україні / Л. Скорпіо. [Електронний ресурс]. – Доступний з http://international-site.net/uk-ua/zakazchiku/100/elektronn-plat-zhn-sistemi-v-ukra-n
9. Хімич Роман. Електронні гроші: загрози вигадані і реальні / Роман Хімич. [Електронний ресурс]. – Доступний з http://news.finance.ua/ua/~/2/2013/01/15/294769







10. Цвєткова Н. Електронні гроші, їх переваги та недоліки / Н. Цвєткова. [Електронний ресурс]. – Доступний з http://www.ufin.com.ua/analit_mat/poradnyk/105.htm


***Грыцюк П.Ю., Грыцюк Ю.И.*** **Электронные деньги – новое достижение криптографии и информационных технологий**


Рассмотрены особенности введения электронных денег как оперативного, надежного и анонимного средства платежей в Украине, являющихся новым достижение криптографии и современной информационной технологии. Установлено, что в системе электронных денег используются два ключа: индивидуальный, предназначенный для подтверждения стоимости купюры, и общедоступный – для проверки их достоверности при проведении платежей. Основываясь на особенности однонаправленной функции, которая гарантирует невозможность возобновления индивидуального ключа подписи по общедоступному ключу его проверки, в электронных деньгах используется схема "слепой" электронной подписи, обеспечивающая высокий уровень их анонимности.



***Ключевые слова:*** наличные расчеты, электронные платежи, электронные деньги, криптографическая защита, информационная технология, "слепая" электронная подпись.


***Grycyuk P.Yu., Grycyuk Yu.I.*** **Electronic money – new achievements of cryptography and information technologies**


The features of the introduction of electronic money as a prompt, reliable and anonymous means of payment in Ukraine, which is a new achievement of cryptography and information technologies. Found that the system of electronic money uses two keys: individual, intended to confirm the value of banknotes and public – to check their validity when making payments. Based on the features unidirectional functions that guarantee the impossibility of restoring individual signing key for public key to his check, electronic cash scheme used of "blind" signature, which provides a high level of anonymity.



***Keywords:*** cash payments, electronic payments, electronic money, cryptographic protection, information technology, "blind" electronic signature.



***УДК 519.83:004.942:658.5***



***Ст. викл. О.М. Васьків – Львівська ДФА;***
***проф. В.В. Здрок, канд. техн. наук – Львівський НУ ім. Івана Франка***


# АВТОМАТИЗАЦІЯ ПРОЦЕСУ ВИБОРУ ОПТИМАЛЬНОЇ СТРАТЕГІЇ РОЗВИТКУ ПІДПРИЄМСТВА В УМОВАХ РИНКУ ТА НЕВИЗНАЧЕНОСТІ


Досліджено процес розроблення оптимальної стратегії розвитку підприємства в умовах ринкової конкуренції, запропоновано підхід до його автоматизації з використанням теоретико-ігрової моделі задачі вибору стратегії випуску продукції підприємства, описано структуру інформаційного та програмного забезпечення реалізації задачі.



***Ключові слова:*** автоматизація, теоретико-ігрова модель, задача вибору стратегії випуску продукції, підприємство.


**Постановка проблеми.** Створення стратегії розвитку підприємства передбачає використання різноманітних математичних моделей для досягнення конкретних цілей. Процес вибору оптимальної стратегії є ітераційним і потребує проведення комп'ютерного експерименту, аналізу його результатів і внесення поправок. Без використання сучасних інформаційних технологій, програмного забезпечення до них та пакетів прикладних програм для прове-