УДК 621.43:681.3

В.А. Лахно, А.С. Петров*
Луганський національний аграрний університет,
кафедра економічної кібернетики,
*Східноукраїнський національний університет
імені Володимира Даля
кафедра комп'ютерних систем та мереж

ЗАХИСТ ІНФОРМАЦІЇ В КЛІЄНТ-СЕРВЕРНІЙ СИСТЕМІ АВТОМАТИЗАЦІЇ БУХГАЛТЕРСЬКОГО ОБЛІКУ ГОСПОДАРСЬКИХ ОПЕРАЦІЙ ПІДПРИЄМСТВА

Розглянуто досвід розроблення програмного забезпечення для клієнт-серверної системи бухгалтерського обліку господарських операцій. Розглядаються питання, пов'язані з розробленням системи захисту комерційної інформації з бухгалтерських операцій підприємств.

In the article the experience of software development is considered for client-server system of record-keeping of economic operations. Questions are examined the systems related to development and defense of commercial information from book-keeping operations of enterprises.

1. Постановка проблеми

Розвиток комп'ютерної техніки в останнє десятиріччя робить актуальним перехід на новітні інформаційні технології для розв'язання економічних задач.

З розвитком мережевих технологій виникає проблема адаптації як існуючих, так і нових програмних продуктів до платформи клієнт-сервер.

2. Аналіз попередніх досліджень

Як показав аналіз ряду публікацій [1–4], при стрімкому зростанні масштабу підприємств і кількості даних, темпи використання клієнт-серверних технологій зростають значними темпами порівняно з локальними системами автоматизованої обробки інформації. Однією із проблем цього зростання є проблема захисту комерційної інформації, яка може становити інтерес для зловмисників і конкурентів.

3. Цілі статті

Метою статті є раціональна організація роботи фінансових та бухгалтерських служб підприємства – одна з найважливіших задач, що визначає ефективність функціонування його економічних служб. Ми пропонуємо власний досвід реалізації клієнт-серверної технології у галузі бухгалтерського обліку господарських операцій із врахуванням накопиченого нами досвіду щодо захисту корпоративної бази даних.

4. Основний матеріал

Нормативні документи, що використовуються в бухгалтерських облікових операціях, ґрунтуються на розроблених Міністерством фінансів Положеннях (стандартах) бухгалтерського обліку (П(С)БО). Проте під час практичного здійснення обліку підприємство обмежується тільки певним набором проводок найхарактерніших для галузі господарської діяльності підприємства. Водночас, наявні сьогодні на ринку бухгалтерських програм продукти орієнтовані на типове коло задач.

Для організації ефективного й коректного бухгалтерського обліку на підприємстві, на наш погляд, варто використовувати експертну думку (див. рис. 1). Тобто, механізм формування інформаційно-довідкової допомоги ми пропонуємо звести до виконання таких дій:

1. Формування переліку операцій з усіма особливостями (враховуючи супутні операції), які підприємство здійснює під час своєї господарської діяльності.
2. Підбір коректних проводок, які найбільш чітко відображають суть цих операцій (при цьому використовується експертна думка).
3. Внесення проводок в інформаційно-довідковий модуль програми.

Надалі в процесі господарської діяльності інформаційно-довідкову базу можна корегувати або повністю поновлювати.

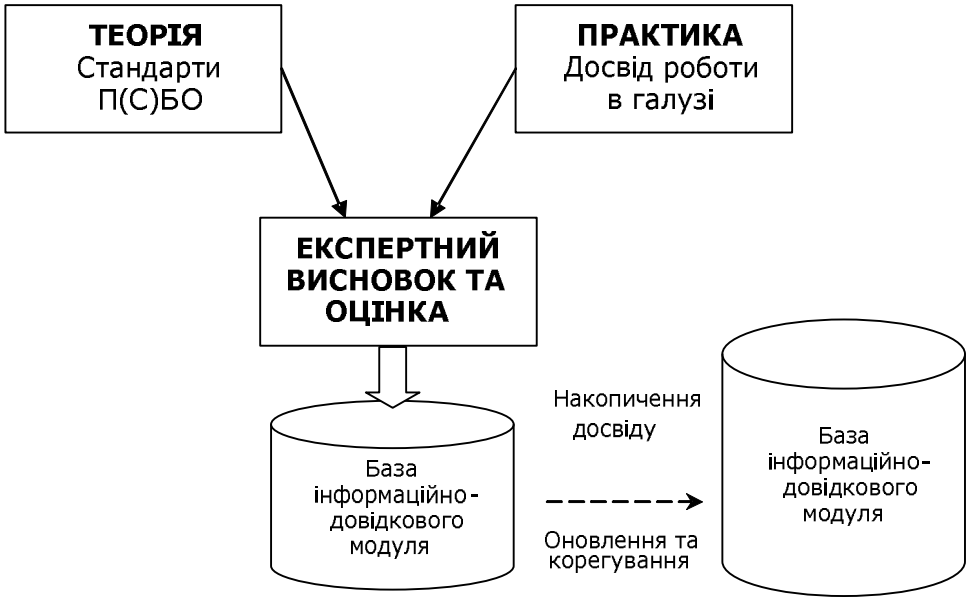

Рис. 1. Використання експертної думки

Отже, розроблений модуль поєднує в собі вимоги, що містяться в наказах Міністерства фінансів, і накопичений досвід обліку господарських операцій. Експертні думки й оцінки повинні гарантувати коректність вибраної схеми обліку.

База даних може містити необмежену кількість потрібної й корисної інформації, яка залишається абсолютно зайвою без зручного механізму маніпулювання нею. Як згадувалося раніше, у будь-якій базі даних інформація зберігається у таблицях, в яких її можна переглядати, і навіть певною мірою керувати нею за допомогою деякого набору універсальних фільтрів. Проте для повсякденної роботи цього дуже мало, особливо у випадках, коли наперед невідома структура інформаційної бази і бізнес-логіка побудови інформаційної системи. Отже, неможливо відповісти на запитання: як отримати потрібну інформацію і чи можна використовувати для цього певне джерело.

Для того, щоб користувачі могли вільно маніпулювати інформацією, в інформаційну систему був вбудований механізм майстрів (система Wizard), призначений для тонкого управління вмістом будь-якої бази даних (див. рис. 2–4).

Механізм майстрів (система Wizard) є найбільш універсальним рішенням, що дає змогу, з одного боку, як завгодно маніпулювати даними – аж до того, що залежно від свого стану додаток вибирав би якісь певні дії, а з іншого – зменшити потребу системи керування базами даних (СКБД) у системних ресурсах взагалі, оскільки активація бази даних (БД) не приводить до проведення всіх запитів та інших автоматичних функцій, що є в БД, як, наприклад, в електронних таблицях. Ті або інші запити виконуються комп'ютером тільки тоді, коли це дійсно необхідно. Правда, медаль має й зворотний бік, оскільки в основу роботи довідника покладені запити. За своєю ідеологією запит

надзвичайно сильно схожий на миттєву фотографію, що відображає поточний стан бази суто на момент виконання цього запиту. Іншими словами, якщо в даних відбулися зміни після того, як запит виконався, то ці зміни в уже створеній вибірці відображені не будуть, оскільки віртуальна таблиця не пов'язана із самими даними. Але цей недолік ліквідують за рахунок чіткого централізованого оновлення даних, яке здійснює експерт-адміністратор.

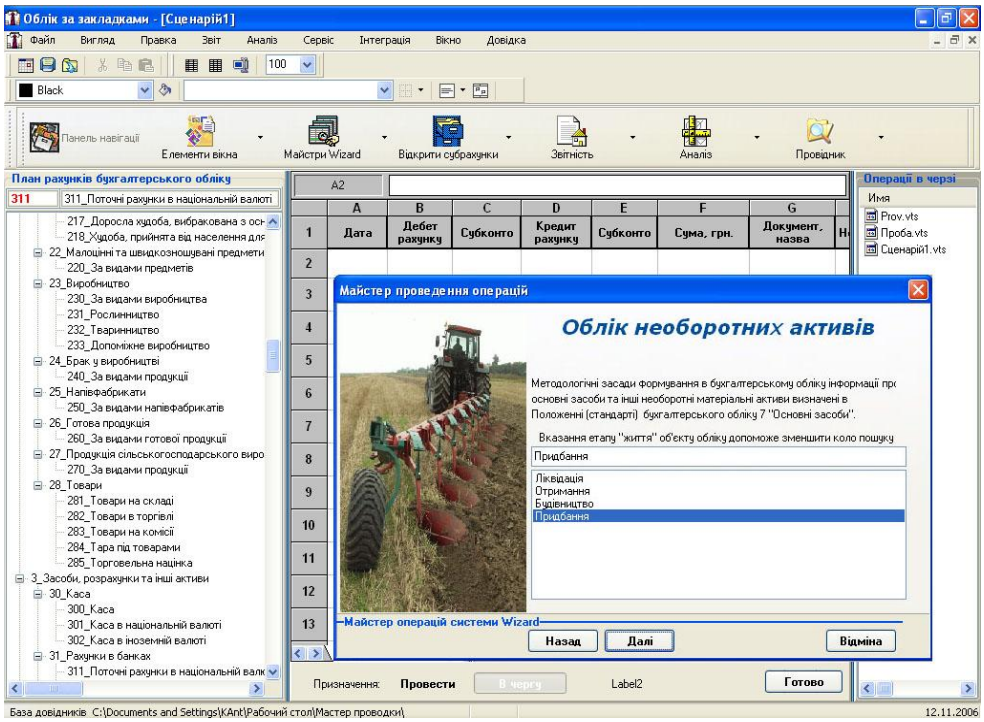

Рис. 2. Сторінка інтерфейсу Майстра

У сфері бухгалтерського обліку цей інформаційно-довідковий додаток реалізує принцип централізованого контролю коректності обліку операцій, а саме, їхнього проведення; вироблення рекомендацій стосується організації ефективного й достовірного обліку інформації (рис. 5).

Ділянки обліку (склад, відділ оплати праці) при цьому виконують функцію генерації протоколів проведення з використанням сформованої експертами інформаційно-довідкової бази. Результатом роботи на ділянках обліку є протоколи проведення – файли, що мають розширення *.vts – список проводок, призначених для подальшого проведення, які характеризують здійснення операції. Далі ці протоколи передаються різними способами (локальна мережа, гнучкі диски і т. п.) на комп'ютер відповідального за проведення операцій, компетентного у цьому питанні (експерт). Він перевіряє правильність віддзеркалення інформації та записує в базу проведені операції (база проводок). У разі виявлення яких-небудь недоліків, таких як не повний зміст або оновлення інформаційно-довідкової бази, на комп'ютер ділянки обліку передаються відповідні вказівки.

Щоб уникнути ненавмисних дій із даними, які не можна скасувати, розробники спроектували систему так, що будь-який створюваний запит автоматично вважається запитом-вибіркою. У випадку, коли користувачу потрібно отримати запит-дію, системі потрібно про це "сказати" окремо, за це й відповідає майстер налагодження інформаційної системи (Wizard), див. рис. 3, 4.

Однією з технічних задач, що розв'язувалися під час створення інформаційної системи, була задача захисту інформації.

Найширші можливості для проведення атаки на корпоративну інформаційну систему підприємства (КІС) мають законні користувачі, які технологічно залучені в процес роботи КІС і які можуть неправильно використовувати надані права доступу. У загальному плані складність захисту інформації на технологічному рівні полягає в необхідності надати операторам певні права доступу і

водночас перешкодити несанкціонованому використанню повноважень. Одним із найефективніших і гнучких механізмів захисту є криптографічні перетворення [7, 8].

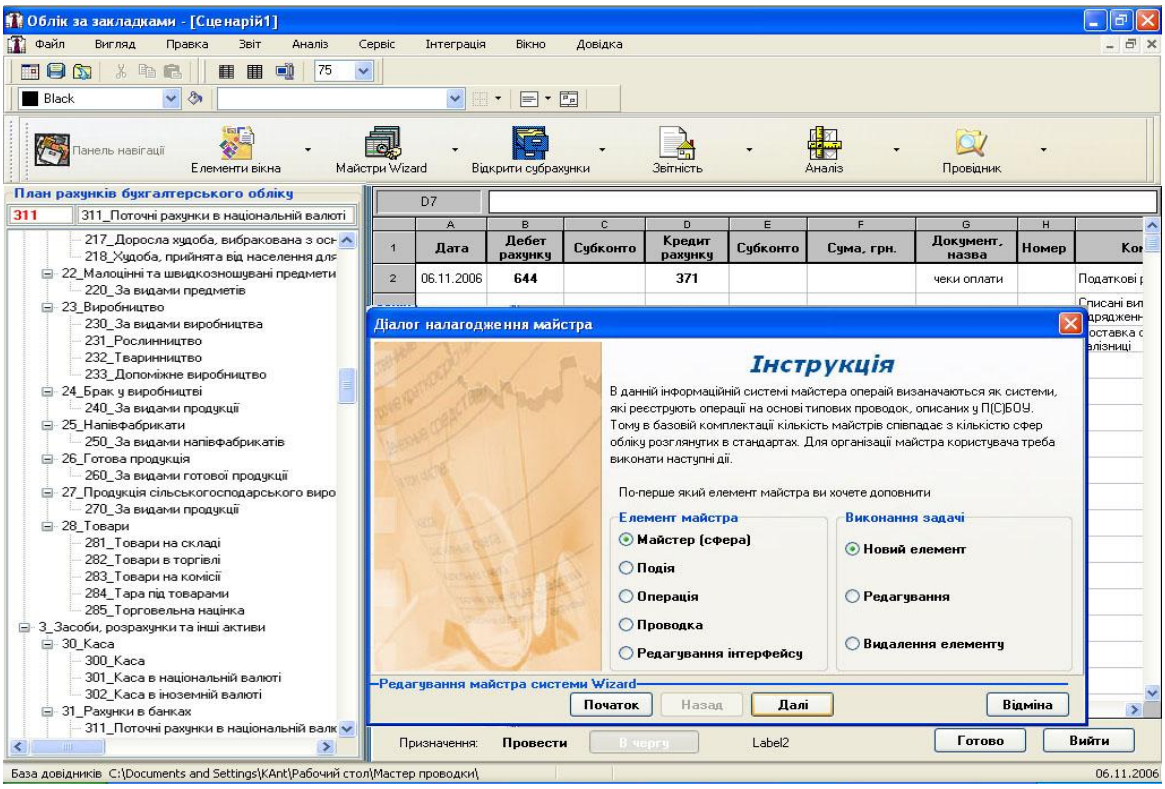

Рис. 3. Налагодження системи Wizard

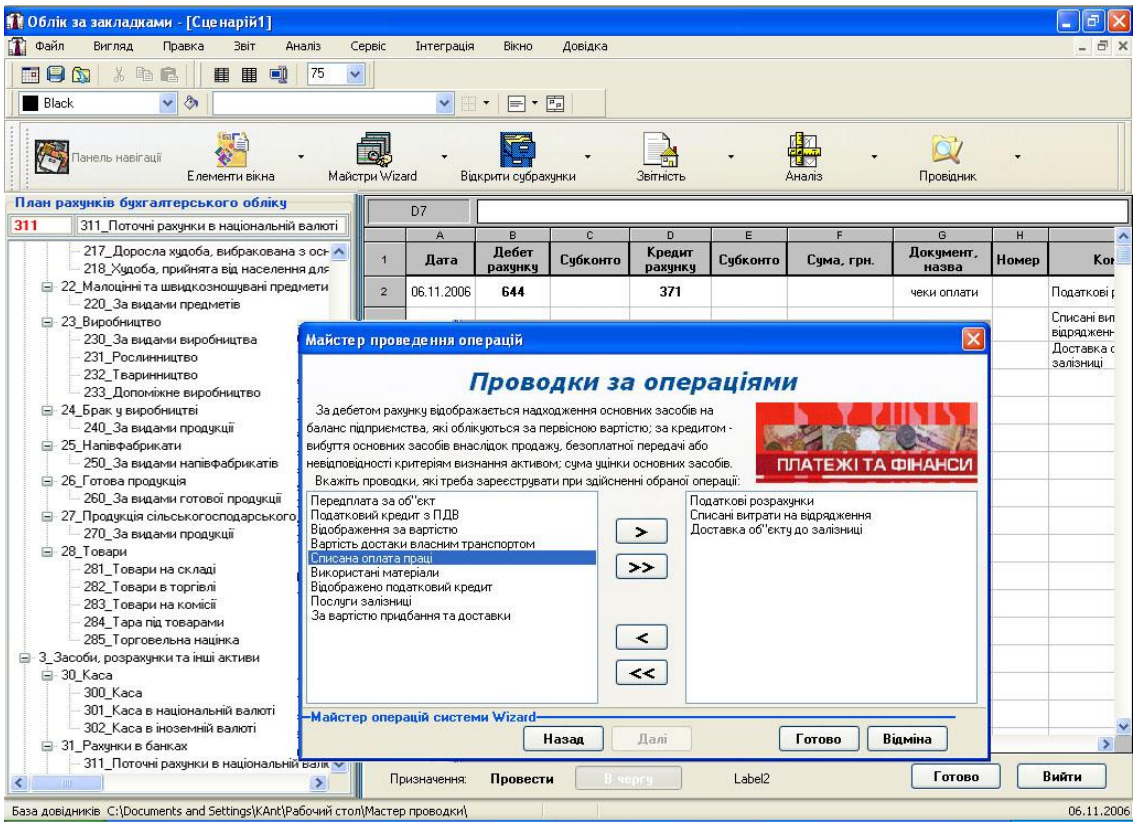

Рис. 4. Результат роботи системи Wizard

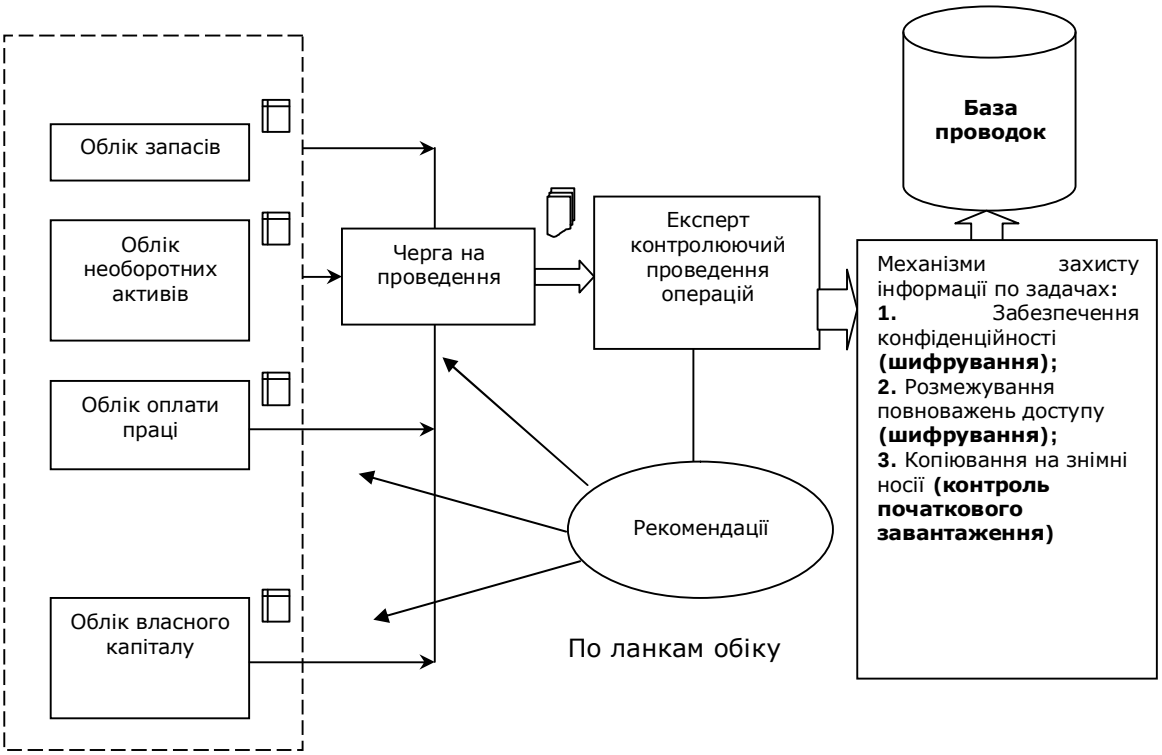

Рис. 5. Централізація обліку операцій

Для розробленого модуля, що працює у складі КІС, розв'язувалися такі задачі захисту від загроз на технологічному рівні:

- розподіл повноважень у правах доступу до ресурсів КІС;
- забезпечення конфіденційності під час роботи в мережі;
- безпечне копіювання на зовнішні носії.

Наша інформаційно-довідкова система програмно реалізована у середовищі програмування С ++ Builder 6 з використанням СКБД InterBase 7.0.

Як головний механізм захисту було вибрано шифрування даних [8]. Як алгоритм шифрування використовувався RSA [7,8]. Як блок безпеки при вході в систему (додаток) застосовувалася функція, що використовує дві динамічні змінні – *key_l, secret*.

Найпростіший варіант блоку безпеки, реалізований на С++, виглядатиме так [8]:

```
int dostup(CLINT n_l)
{CLINT key_l;
USHORT secret;
/*Записуємо дані */
secret=0;
memset(key_l,0,sizeof(key_l));
return 0; }
```

Для підвищення ефективності коду ми використовували асемблерну вставку для відповідних змінних – *key_l, secret.*

```
void main()
{
EXTRN _ purgevars_l:Near;

 _ key_l$=-516;
 _ secret_$=-520;
 _asm
{
 sub esp, 520
```

```
lea eax, DWORD PTR_key_I$[esp+532]
PUSH EAX
lea ecx, DWORD PTR_secret_$[esp+536]
PUSH 514
PUSH ECX
PUSH 2
PUSH 2
}
call _purgevars_l
….
```

Для розробленої нами системи ми також запропонували один із найефективніших і гнучких механізмів захисту – криптографічні перетворення [4,5].

Поняття часу й складності реалізації алгоритму шифрування нерозривно пов'язані з теорією складності обчислень, основоположником якої був Клод Шеннон [9], який довів важливість булевої алгебри для аналізу й синтезу релейних схем перемикачів. Моделювання обчислювальних процесів часто виконується у вигляді логічних (комбінаційних) схем, для реалізації яких використовується деякий базис найпростіших логічних елементів (вентилів), що реалізовують логічні операції.

Необхідно зазначити, що комбінаційна складність істотним чином залежить від базису *W={&,Ú,–}*. Крім того, одна й та ж логічна схема може мати різні реалізації. У статті оцінка складності даних комбінаційних схем дана для базису "*I*". Цей варіант представлений на рис. 6.

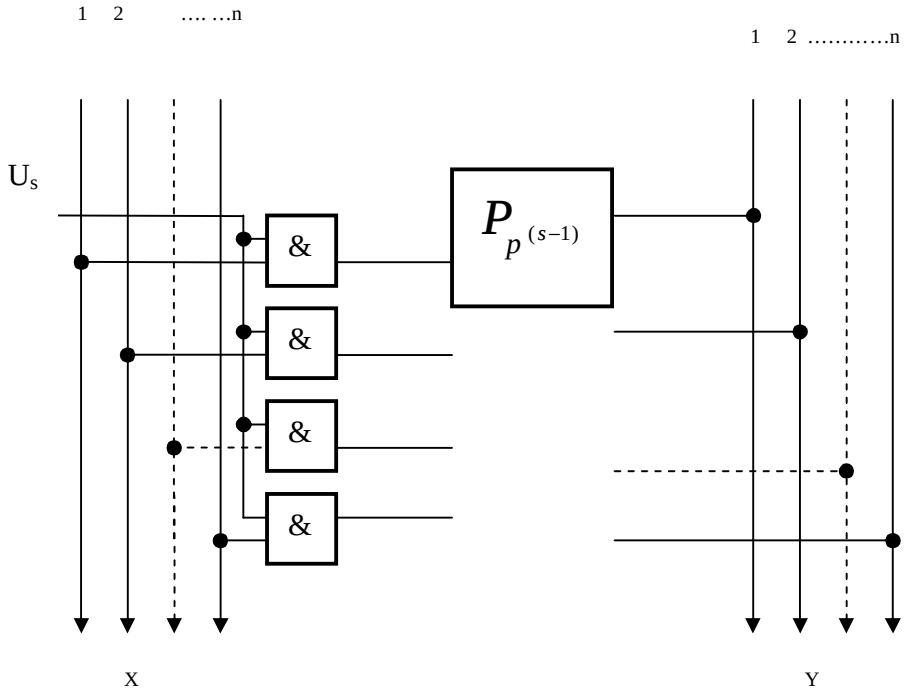

Рис. 6. Схема реалізації керованого вибору

Схема працює так. Двійковий дешифратор D_m, на вхід якого надходить m розрядний керуючий вектор $V=(v_1, v_2, \ldots, v_m)$, формує двійковий керуючий вектор $U=D_m(V)$ завдовжки 2^m з вагою Хеммінга $WH(U)=1$, тобто значення 1 виробляється тільки в одному розряді, а саме:

$$u_s = \begin{cases} 1, & якщо \quad s = 1 + v_1 + v_2 2 + \ldots + v_m 2^{m-1} \\ 0, & в \quad інших \quad випадках \end{cases}$$

Комутація розрядів входу й розрядів виходу за заданою фіксованою перестановкою $p^{(s-1)}$ реалізується відповідно до схеми, яка наведена на рис. 6, у якій розряди вектора X надходять на вхід n логічних елементів "*I*" при керуючому сигналі U_s.

Комутація виконується тільки в тому випадку, якщо значення однорозрядного керуючого сигналу $U_s=1$ Наприклад, у блоці керованих перестановок вектору відповідає модифікація

$$p^{(7)} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Властивості блоку керованих перестановок з матричною структурою залежать від конкретного набору заданих перестановок, а також від їх взаємного розташування. Дослідження цього напрямку наразі тривають, тому не розглядаються у цій статті.

Висновки

Отже, у роботі обґрунтована необхідність використання в економічних інформаційних системах таких елементів, як:

- майстер побудови протоколів проводок, що полегшує навчання персоналу і відображає практичні особливості обліку на підприємстві, а також дає змогу накопичувати і передавати досвід роботи;
- централізована обробка даних, яка дає змогу ефективно використовувати робочий час висококваліфікованих фахівців;
- генерація протоколів проведення у вигляді окремих файлів, що значно спрощує процес передачі даних від рядових службовців до кваліфікованих фахівців;
- автоматизований процес консультацій фахівців підприємства експертами з приводу правильності віддзеркалення в обліку операції, що дає змогу знижувати витрати на здійснення технологічних процесів та операцій бухгалтерського обліку;
- криптографічний механізм захисту інформації для збереження конфіденційності комерційної таємниці підприємства.

При реалізації нашої розробки в середовищі програмування С ++ Builder 6 та СКБД InterBase 7.0 було розв’язано такі задачі:

- розроблено відповідне програмне забезпечення для клієнт-серверної системи бухгалтерського обліку господарських операцій підприємства;
- розроблені зручні інтерфейси, орієнтовані навіть на недосвідченого користувача системи;
- розпочато роботу з криптографічного захисту розробленого додатка, зокрема, шляхом використання блоку безпеки, реалізованого на С++, а також блоку керованих перестановок із матричною структурою.

Інтерфейс розробленої програми є інтуїтивно зрозумілим і простим у використанні, що дає змогу навіть недосвідченому бухгалтеру або працівнику економічних служб підприємства, який не володіє спеціальними знаннями з комп’ютерної техніки, працювати з нею без додаткової допомоги.

1. Архангельский А.Я. Приёмы программирования в C++ Builder. – 2-е изд., перераб. и доп. – М.: ООО “Бином-Пресс”, 2006. – 848 с. 2. Барановский Н.Т. Автоматизированная обработка экономической информации: Учебник. – М.: Финансы и статистика, 1991. – 304 с. 3. Вендров А.М. Проектирование программного обеспечения экономических информационных систем. – М.: Финансы, 2002. – 254 с. 4. Дудка К.П., Жук В.М., Жук Н.Л., Канцуров О.О., Кірейцев Г.Г., Кононенко Г.Г., Михайлов М.Г., Мосаковський В.Б., Паригін К.О., Томчук О.Ф. Облік в сільськогосподарських підприємствах за національними стандартами: Посібник. – К.: Інститут аграрної економіки УААН, 2000. – 218 с. 5. Перов В. Н. Информационные системы. – СПб.: Питер, 2002. – 688 с. 6. Лишиленко О.В. Бухгалтерський фінансовий облік. Навчальний посібник. – Київ: Вид-во “Центр навчальної літератури”, 2004. – 528 с. 7. Молдовян А.А. Криптография: скоростные шифры. - СПб.: БХВ-Петербург, 2002. – 496 с. 8. Вельшенбах М. Криптография на Си и С++ в действии. – М.: Триумф, 2004. – 464 с. 9. Шеннон К.Э. Синтез двухполюсных переключательных схем // В кн. Работы по теории информации и кибернетике. – М.: Иностранная литература, 1963. – С. 9–45. 10. Пирогов В.Ю. MS SQL Server 2000 управление и программирование. – СПб.: БХВ, 2005. – 608 с. 11. Пирогов В.Ю. Программирование на Visual C++. – СПб.: БХВ, 2003. - 424 с.