

МИТНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

За редакцією П.В. Пашка

У серії “Митна справа в Україні” вийшли друком:

- “Основи митної справи в Україні”
- “Митний контроль та митне оформлення”
- “Таможенное оформление морских грузов”
- “Основы таможенного дела в Украине”
- “Митний контроль на автомобільному транспорті”
- “Митний контроль на залізничному транспорті”
- “Митне оформлення автотранспортних засобів”
- “Митний кодекс України та нормативно-правові акти,
що регулюють його застосування”
- “Митний контроль на повітряному транспорті”
- “Порядок заповнення ВМД”
- “Митне регулювання ЗЕД в Україні”
- “Історія митної справи в Україні”
- “Основи мистецтвознавчої експертизи та вартісної оцінки
культурних цінностей”
- “Таможенный контроль: на пути к международным
стандартам”
- “Таможенный контроль в морских пунктах пропуска”
- “Митне оформлення енергоносіїв”
- “Митна безпека”
- “Святий Матфей. Митар. Апостол. Євангеліст”

У серії “Митна справа в Україні” готуються до друку:

- “Історія митної справи в Україні в особах”
- “Митна політика та митна безпека України”
- “Митні традиції та ритуали”
- “Етика та етикет митника”
- “Митні лабораторії України”
- “Митна класифікація товарів”
- “Робоча книга психолога митного органу”

Серія "МИТНА СПРАВА В УКРАЇНІ"

Серію засновано у 2001 році

Голова редакційної колегії —
доктор економічних наук
П.В. Пашко

МИТНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Навчальний посібник

За редакцією
заступника Голови Державної митної служби України,
доктора економічних наук П.В. Пашка

*Рекомендовано
Міністерством освіти і науки України*



Київ

“ЗНАННЯ”

2011

УДК 339.543+004(075.8)

ББК 65.9(2)8я73

М66

*Рекомендовано Міністерством освіти і науки України
(лист № 1/12-2426 від 9 червня 2010 р.)*

Автори:

О.Ф. Волик, старший викладач кафедри вищої математики та інформатики Академії митної служби України; *О.В. Кащєєва*, старший викладач кафедри вищої математики та інформатики Академії митної служби України; *І.В. Дорда*, старший викладач кафедри державної служби та митної справи Інституту післядипломної освіти Академії митної служби України; *С.А. Копосов*, начальник Регіональної інформаційної митниці Державної митної служби України; *О.О. Ніколайчук*, перший заступник начальника Регіональної інформаційної митниці Державної митної служби України; *П.В. Пашко*, заступник Голови Державної митної служби України; *П.Я. Пісний*, заступник начальника Регіональної інформаційної митниці Державної митної служби України; *В.П. Шуляк*, заступник начальника Регіональної інформаційної митниці Державної митної служби України

Рецензенти:

Г.В. Кузнецов, завідувач кафедри електроніки та обчислювальної техніки Національного гірничого університету, доктор технічних наук, професор; *М.Г. Гуменюк*, начальник відділу інформаційної роботи та митної статистики Дніпропетровської митниці; *О.В. Коваленко*, завідувач кафедри радіоелектроніки Дніпропетровського національного університету імені Олеся Гончара, доктор фізико-математичних наук, професор

Митні інформаційні технології : навч. посіб. / О.Ф. Волик, О.В. Кащєєва, І.В. Дорда та ін. ; за ред. П.В. Пашка ; передмова А.В. Толстоухова. — К. : Знання, 2011. — 391 с. — (Митна справа в Україні).

ISBN 978-966-346-853-2 (серія)

ISBN 978-966-346-661-3

У навчальному посібнику висвітлено основні принципи побудови та вдосконалення Єдиної автоматизованої інформаційної системи Держмитслужби України, її складові, способи формування, збереження та передавання даних. Детально розглядаються програмне забезпечення митного контролю та митного оформлення товарів і транспортних засобів ("Інспектор-2006"), програмне забезпечення обміну даними у відомчій телекомунікаційній мережі. Особливо наведено відомості про програмні продукти та технології, що застосовуються для декларування товарів суб'єктами зовнішньоекономічної діяльності.

Для курсантів, студентів і слухачів навчальних закладів митної служби України, які вивчають сучасні митні інформаційні технології. Книга буде корисною працівникам митної служби, декларантам, керівникам підприємств та організацій, державним службовцям, підприємцям, а також викладачам, які мають справу із застосуванням сучасних інформаційних технологій у митній справі.

УДК 339.543+004(075.8)

ББК 65.9(2)8я73

ISBN 978-966-346-853-2
(серія)

ISBN 978-966-346-661-3

© П.В. Пашко, О.Ф. Волик, О.В. Кащєєва,
І.В. Дорда та ін. автори, 2011
© Видавництво "Знання", 2011

ЗМІСТ

Передмова	9
Частина I. ОСНОВИ ІНФОРМАЦІЙНИХ СИСТЕМ.....	13
Розділ 1. Основні поняття, проблеми і роль інформаційних технологій та інформаційних систем	14
1.1. Інформація і дані	14
1.2. Інформаційні ресурси організації	17
1.3. Інформаційні технології.....	18
Розділ 2. Типова структура і склад інформаційних систем	26
2.1. Інформаційні системи	26
2.2. Типи інформаційних систем	28
2.3. Компоненти інформаційних систем	30
Частина II. ЄДИНА АВТОМАТИЗОВАНА ІНФОРМА- ЦІЙНА СИСТЕМА ДЕРЖАВНОЇ МИТНОЇ СЛУЖБИ УКРАЇНИ	37
Розділ 3. Історія розвитку інформаційної системи митної служби України	38
Розділ 4. Призначення та основні принципи побудови САІС Держмитслужби України	44
Розділ 5. Структура, склад і функції САІС.....	48
Частина III. ТЕХНОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ ІНФОР- МАЦІЙНИХ СИСТЕМ У МИТНІЙ СПРАВІ ...	51
Розділ 6. Класифікація та кодування інформації.....	52
6.1. Вимоги до уніфікованої системи документів...	52

6.2. Системи класифікації та кодування	56
Розділ 7. Електронний обмін інформацією.....	60
7.1. Міжнародні стандарти електронного обміну даними	60
7.2. Міжнародні стандарти систем обробки повідомлень (електронної пошти)	67
7.3. Інтегрована система Lotus Domino та Notes	94
Розділ 8. Захист інформації в інформаційних системах	118
8.1. Захист інформаційних ресурсів від несанкціонованого доступу	118
8.2. Методи і засоби захисту інформації в інформаційних системах	123
8.3. Правове забезпечення режиму електронного цифрового підпису.....	126
8.4. Організаційне забезпечення електронного цифрового підпису.....	138
8.5. Технічне забезпечення режиму електронного цифрового підпису. Поняття електронного цифрового підпису.....	144
Частина IV. ПРИКЛАДНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЄДИНОЇ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЕРЖАВНОЇ МИТНОЇ СЛУЖБИ УКРАЇНИ	163
Розділ 9. Компоненти електронного декларування	164
9.1. Автоматизована система митного оформлення “Інспектор-2006”	167
9.2. Автоматизована система аналізу та управління ризиками.....	198
Розділ 10. Програмно-інформаційні комплекси ЄАІС ДМСУ	214

10.1.	Програмно-інформаційний комплекс “Квитанції МД-1”	214
10.2.	Програмно-інформаційний комплекс “Аналітична та статистична обробка інформації про порушення суб’єктами ЗЕД чинного законодавства”	217
10.3.	Програмно-інформаційний комплекс “Реєстр дозволів на право відкриття складів тимчасового зберігання”	219
10.4.	Програмно-інформаційний комплекс “Контроль за переміщенням вантажів при транзиті”	222
10.5.	Програмно-інформаційний комплекс “Митний контроль та митне оформлення транспортних засобів, що переміщуються громадянами через митний кордон України”	227
10.6.	Власні розробки митних органів	229
Розділ 11.	Системи передачі інформації у митній службі України	234
11.1.	Засоби електронної пошти та їх застосування в ЄАІС Держмитслужби України	234
11.2.	Відомча телекомунікаційна мережа ЄАІС Держмитслужби України	239
Розділ 12.	Захист митної електронної інформації	243
12.1.	Електронна митна інформація. Відпові- дальність за підготовку, використання та по- ширення електронної митної інформації	243
12.2.	Засоби захисту інформації в ЄАІС ДМСУ	246
Розділ 13.	Комерційні програмні продукти митного оформлення	253
13.1.	Програмні комплекси для декларування товарів суб’єктами зовнішньоекономічної діяльності	253

13.2. Програмне забезпечення MD Office	256
13.3. Програмне забезпечення QD Professional	267
13.4. Програмне забезпечення Diamond Bridge	288
13.4.1. Підсистема роботи з нормативними докумен- тами з питань митної справи	289
13.4.2. Робота з класифікаторами та іншою норма- тивно-довідковою інформацією	294
13.4.3. Робота з вантажними митними деклараціями	300
13.4.4. Модуль “Митний облік”	306
13.4.5. Звіти програми Diamond Bridge	308
13.4.6. Адміністрування програми Diamond Bridge...	310
Розділ 14. Створення Електронної митниці — головний напрямок подальшого розвитку ЄАІС ДМСУ	312
14.1. Концепція створення Електронної митниці...	312
14.2. Обґрунтування та мета створення Електронної митниці.....	316
14.3. Основні завдання, які вирішує Електронна митниця	321
14.4. Напрями створення Електронної митниці	322
14.5. Принципи побудови багатофункціональної комплексної системи “Електронна митниця”	325
14.6. Структура та інфраструктура Електронної митниці	327
14.7. Інформаційна безпека Електронної митниці	329
14.8. Етапи впровадження Концепції “Електронна митниця”	333
14.9. Очікувані результати реалізації Концепції...	336
14.10. Шлях інформаційних технологій від e-Customs до i-Customs	337
Додатки.....	345
Література.....	375
Основні поняття і терміни	378
Предметний покажчик	389
Від авторів	391

ПЕРЕДМОВА

У ХХІ столітті відбулися значні зміни в зовнішньоекономічній діяльності як України, так і всього світового суспільства. Ці зміни потребують більш якісного підходу до реалізації державної митної політики.

Стратегія розвитку суспільства однозначно засвідчує, що перемоги досягають ті структури, які накопичують і вміло розпоряджаються наявною інформацією. У наш час збір та обробка великих обсягів інформації можливі лише в результаті застосування інформаційних технологій, що реалізуються шляхом побудови комп'ютерних інформаційних систем.

Тенденції світового розвитку встановлюють нові завдання, зокрема зі спрощення митних процедур та процедур логістики на території будь-якої країни, зменшення ризиків порушення безпеки мешканців, для чого створюються комп'ютерні інформаційні системи, функціонально сумісні між аналогічними системами різних країн, а отже, доступні, керовані, безпечні, об'єднані та контрольовані.

Всесвітня митна організація визначила підходи до прискорення і спрощення митних процедур у своїх програмних документах — Міжнародній конвенції щодо спрощення й гармонізації митних процедур, Рамкових стандартах безпеки і полегшення світової торгівлі. Європейська спільнота вбачає шлях до цього у зменшенні розбіжностей між митними процедурами країн світу, практичним засобом реалізації якого є створення системи “Електронна митниця”.

Цілком очевидно, що прискорення і спрощення митних процедур не можливі за умови використання старих технологій, заснованих на паперових документах. Тут на перший план виходять інформаційні митні технології, основою яких є електронний документообіг. Впровадження електронного документообігу дає змогу значно скоротити час на отримання, опрацювання і прийняття рішення щодо переміщення товарів через митний кордон України, випуску товарів у вільний обіг, зменшити ризики, пов'язані з митними правопорушеннями і контрабандою, що у свою чергу забезпечить зростання товарообігу, а отже, і збільшення надходжень до бюджету держави.

Держави — члени ЄС прийняли рішення діяти в рамках структури “Електронної Європи”, тобто простого і безпаперового середовища стосовно митних адміністрацій та суб'єктів зовнішньоекономічної діяльності.

Виходячи з цього аналогічні завдання щодо втілення новітніх технологій у митну справу ставлять перед собою митні адміністрації багатьох країн СНД, Азії та Америки. Ці завдання відрізняються лише термінами реалізації та окремими деталями. Тому “Електронна митниця” — це не тільки утворення декількох країн, це майбутнє митної спільноти світу.

“Електронна митниця” є багатофункціональною комплексною системою, яка діє в митних органах країни, поєднуючи інформаційно-комунікативні технології та сукупність механізмів їх застосування, що дає можливість підвищити якість митного регулювання і вдосконалити митне адміністрування з метою забезпечення митної безпеки держави шляхом:

- технологічної підтримки безперервного двостороннього потоку електронної інформації від органів державної влади, суб'єктів зовнішньоекономічної діяльності, митних адміністрацій інших держав до митної адміністрації країни, а також її накопичення та обробки;

- впровадження новітніх процедур автоматизації процесів митного контролю та оформлення, їх супроводження;

- створення і технічної підтримки організаційно-технічних систем для функціонування всеохоплюючих автоматизованих процедур оцінювання якості виконання митної справи;

- інформаційного забезпечення правоохоронної діяльності, контролю за переміщенням товарів, а також виконання інших функцій, покладених на митні органи.

Україна поетапно просувається до створення власної інформаційної системи. Постановою Кабінету Міністрів України “Про заходи щодо створення електронної інформаційної системи “Електронний Уряд” від 24 лютого 2003 р. № 208 встановлено, що одним із пріоритетних завдань розвитку інформаційного суспільства є надання громадянам та юридичним особам інформаційних та інших послуг шляхом використання електронної інформаційної системи “Електронний Уряд”, яка забезпечує інформаційну взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій.

Закон України “Про електронні документи та електронний документообіг” від 22 травня 2003 р. № 851-IV встановлює основні організаційно-правові засади електронного документообігу і використання електронних документів.

Митна служба України розпочала втілення новітніх технологій в митну справу ще в 1992 р. У 2005 р. почався новий етап роботи з розробки принципів побудови системи “Електронна митниця” та її часткової реалізації. Однак організація і проведення цієї роботи потребують єдиного підходу та комплексного вирішення.

“Електронна митниця” повинна поєднувати в собі такі підсистеми, як електронне декларування; електронний документообіг; аналіз ризиків і керування ними; контроль за транзитом; єдина міжвідомча автоматизована система збору, збереження й обробки інформації, у тому числі від органів виконавчої влади; автоматизоване здійснення всіх видів державного контролю; уніфікована база нормативних і довідкових документів, які використовуються в митних цілях; інформаційне забезпечення аудита та правоохоронної діяльності. Об’єднуючий стрижень митної служби — інформаційні механізми. У цьому запорука посилення авторитету та могутності митниці. Інші шляхи — це крок назад.

Ця система повинна бути заснована на новітніх інформаційних технологіях і, відповідно, на сучасній матеріальній базі, що дасть можливість створити модернізовану багаторівневу систему із застосуванням телекомунікаційних технологій, забезпечену комплексною системою захисту інформації, однак це потребує тривалого часу та значних капіталовкладень.

Це також важливо для втілення в життя міжнародних стандартів якості, які є міжнародним еталоном для створення та оцінки систем якості, у тому числі якості виконання митної справи. Критерії оцінки якості виконання митної справи можуть і мають стати складовою оцінки роботи митних органів, сприяти підвищенню основних показників їх роботи та повному виконанню завдань, які покладаються державою на митну службу, що зрештою і є основною метою всіх перетворень.

Важко переоцінити роль інформаційних технологій у будь-якій сфері державної діяльності, але у митній справі це особливо очевидно. Необхідно зазначити, що митна служба на сьогодні — один із небагатьох органів державної влади, де застосування інформаційних технологій є пріоритетним завданням.

Створення і функціонування комплексної системи “Електронна митниця” не тільки забезпечить виконання митної справи, а й внесе значний вклад у розвиток та впровадження інформаційного суспільства та “е-урядування”, яке здійснює взаємодію органів державної влади з населенням, що базується на широкому застосуванні інформаційних технологій, у тому числі за допомогою мережі Інтернет, з метою доступності та якості державних послуг, зменшення термінів їх надання, а також зниження адміністративного навантаження на громадян та організації, обумовленого їх отриманням.

Впровадження “е-урядування” забезпечить якісно новий рівень управління державою і суспільством у цілому, зміцнить довіру до держави та її політики, вдосконалив взаємодію між органами державної влади та органами місцевого самоврядування, бізнесом, громадянами і державними службовцями.

Сподіваюся, що ця книга допоможе курсантам Академії митної служби, студентам інших вищих навчальних закладів України, які здійснюють підготовку спеціалістів для роботи в митниці, отримати необхідні знання з побудови та використання Єдиної автоматизованої інформаційної системи Митної служби України, познайомитися з професійними програмними продуктами, що дають змогу вирішувати прикладні завдання в рамках митної справи.

***А.В. Толстоухов,**
доктор філософських наук,
член-кореспондент НАПН України,
міністр Кабінету Міністрів України*

Частина I

ОСНОВИ ІНФОРМАЦІЙНИХ СИСТЕМ

Розділ 1

ОСНОВНІ ПОНЯТТЯ, ПРОБЛЕМИ І РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

1.1. Інформація і дані

Будь-яка діяльність людини базується на інформації. У контексті автоматизованої обробки інформації та інформаційних систем термін “інформація” має надзвичайно важливе значення і від правильної його інтерпретації залежить ефективність людино-машинних систем. У загальному розумінні *інформація* (від лат. *informatio* — роз’яснення) — це незвичайний ресурс, споживання якого не зменшує його кількості та якості. Вартість виробництва разом з витратами на збирання, зберігання, пошук і обробку інформації значна, тому величезну перевагу має колективне використання інформації. Отже, однією з головних цілей розробки інформаційних систем є полегшення колективного використання інформації.

Інформація невіддільна від процесу інформування користувачів, тому відомості стають інформативними, тобто перетворюються на інформацію, лише у разі їх новизни й достовірності, коли вони зменшують невизначеність з того чи іншого питання. На шляху від джерела до користувача інформація зазнає перетворень, в яких змістові аспекти повідомлень відходять на другий план. Інформація — це не будь-які відомості, вона несе щось нове, що зменшує наявну невизначеність. Інформація стає повідомленням, виражається певною мовою у вигляді знаків і може бути записана на матеріальному носії (повідомлення є формою передачі інформації). Інформація передається в каналі суспільної комунікації.

Інформація — це відомості про навколишній світ (об’єкти, явища, події, процеси тощо), які зменшують міру наявної невизначеності, неповноти знань, відчужені від їх творця та які стали повідомленнями (вираженими певною мовою у вигляді знаків, у тому числі й записаними на матеріальному носії). Їх можна відтворювати шляхом передачі людьми усним, письмовим або іншими способами (за допомогою умовних сигналів, технічних та обчислювальних засобів та ін.).

Обов’язкові атрибути інформації: наявність носія, джерела і приймача, а також каналів зв’язку між ними (рис. 1.1).



Рис. 1.1. Атрибути інформації

Процес насичення виробництва й усіх сфер життя і діяльності людини інформацією називається **інформатизацією**.

Наука, що вивчає властивості інформації, питання її збирання, зберігання, пошуку, опрацювання, перетворення, поширення і використання у різних сферах діяльності людини, називається **інформатикою**.

Говорячи про інформацію, мають на увазі її властивості, а саме:

- 1) інформація *достовірна*, якщо вона відображає істинний стан справ, не містить перекручень;
- 2) інформація *повна*, якщо її достатньо для розуміння і прийняття рішень;
- 3) інформація *чітка й зрозуміла*, якщо вона виражена мовою, якою спілкуються ті, для кого вона призначена;
- 4) *цінність, якість* інформації — це міра розширення, розвитку тезауруса (систематизованого словника понять із зазна-

ченням смислових зв'язків між ними, тобто сукупності відомостей, які має у своєму розпорядженні користувач або система) сприймаючою стороною під час приймання та інтерпретації повідомлення, міра зниження стану невизначеності економічного суб'єкта, міра просування до мети;

5) *адекватність* інформації — це певний рівень відповідності, що створюється за допомогою отриманої інформації, образу реального об'єкта, процесу, явища та ін.

Таким чином, інформація має бути достовірною, переконливою, повною, точною, корисною, новою, оперативною та актуальною.

Дані — це інформація, подана у формалізованому вигляді, прийнятому для опрацювання автоматичними засобами за можливої участі людини (вхідні, вихідні дані, база даних тощо).

Виходячи з наведених визначень, співвідношення понять “інформація” і “дані” можна відобразити такою схемою (рис. 1.2):



Рис. 1.2. Співвідношення інформації та даних

Інформація класифікується за видами.

Наукова інформація найбільш повно відображає об'єктивні закономірності природи, суспільства, мислення. За галузями одержання або користування її поділяють на політичну, технічну, біологічну, фізичну тощо, за призначенням — на масову і спеціальну.

У системах організованого управління виокремлюють *економічну* інформацію, пов'язану з управлінням людьми.

Економічна інформація відображає процеси виробництва, розподілу, обміну і споживання матеріальних благ і послуг. У зв'язку з тим, що економічна інформація пов'язана переважно

із суспільним виробництвом, її часто називають *виробничою інформацією*.

Економічна інформація характеризується великим обсягом, багаторазовим використанням, оновленням і перетворенням, великою кількістю логічних операцій і відносно нескладних математичних розрахунків для отримання багатьох видів *результативної інформації*.

1.2. Інформаційні ресурси організації

Наприкінці XX ст. уперше в історії людства основним предметом праці в суспільному виробництві промислово розвинутих країн стає інформація. Виникли тенденції неухильного перекачування трудових ресурсів зі сфери матеріального виробництва в інформаційну сферу. Національні інформаційні ресурси — це нова економічна категорія. Інформація стає таким самим ресурсом, як матеріал та енергія, тому важливі питання: “Хто ним володіє? Хто в ньому зацікавлений? Наскільки він доступний? Чи можливе його комерційне використання?”.

Ресурс — це запас, джерело чого-небудь. Розглядаючи народне господарство країни, будь-яку галузь, підприємство, тобто організацію будь-якого масштабу, можна виокремити матеріальні, природні, трудові, фінансові, енергетичні ресурси. Ці поняття є економічними категоріями.

Для нормального функціонування організації будь-якого масштабу недостатньо мати матеріальні, фінансові та людські ресурси — необхідно знати, що з цим усім треба робити, знати про технології їх використання. Тому інформація, інформаційні ресурси нині розглядаються як окрема економічна категорія.

Інформаційний ресурс — це особливий вид ресурсу, що ґрунтується на ідеях і знаннях, нагромаджених у результаті науково-технічної діяльності людей і поданих у формі, придатній для збирання, реалізації та відтворення.

Інформаційний ресурс має низку характерних особливостей. Зокрема, на відміну від інших (матеріальних) ресурсів, він практично невичерпний. З розвитком суспільства і зрос-

танням обсягу використовуваних знань цей ресурс не зменшується, а навпаки, зростає. Застосування нового інформаційного ресурсу замість застарілого потенційно може спричинити дії радикального характеру, багаторазово підвищити продуктивність праці, поліпшити використання інших ресурсів тощо.

Як і будь-яким ресурсом, інформаційними ресурсами можна управляти. Хоча ще не розроблено методологію кількісної та якісної оцінки інформаційних ресурсів, а також прогнозування потреби в них, однак на рівні організації можна і треба вивчати інформаційні потреби, планувати й управляти інформаційними ресурсами.

Управління інформаційними ресурсами означає:

1) оцінювання інформаційних потреб на кожному рівні та в межах кожної функції управління;

2) вивчення документообігу організації, його раціоналізацію, стандартизацію типів і форм документів, типізацію інформації і даних;

3) подолання проблеми несумісності типів даних;

4) створення системи управління даними тощо.

З поняттям “інформаційний ресурс” тісно пов’язане поняття “інформаційна технологія” (технологія обробки інформації).

1.3. Інформаційні технології

Поняття інформаційної технології виникло в останнє десятиріччя XX ст. у процесі становлення інформатики. Особливість інформаційних технологій в тому, що в них і предметом, і продуктом праці є інформація, а засобами праці — засоби обчислювальної техніки та зв’язку. Інформаційна технологія як наука про виробництво інформації виникла тому, що інформація стала реальним виробничим ресурсом поряд з іншими матеріальними ресурсами.

Під технологією мають на увазі сукупність методів обробки, виготовлення, зміни стану, властивостей, форми сировини, матеріалу або напівфабрикату, здійснюваних у процесі виробництва продукції. В інформаційних технологіях матеріалом і продуктом є інформація. Але це якісно нова інформація про стан

об'єкта, процесу або явища. Технологія — це методи та способи роботи персоналу і технічних пристроїв з інформацією.

Інформаційна технологія — це система методів і способів збирання, передачі, накопичення, опрацювання, зберігання, подання й використання інформації (далі — ІТ).

Інформаційні технології реалізуються в автоматизованому і традиційному (паперовому) вигляді. Автоматизована інформаційна технологія передбачає існування комплексу відповідних технічних засобів, що забезпечують реалізацію інформаційного процесу, і системи управління цим комплексом технічних засобів.

Автоматизована інформаційна технологія (далі — АІТ) — це комплекс методів і процедур, за допомогою яких реалізуються функції збирання, передавання, обробки, зберігання та доведення до користувача інформації в організаційно-управлінських системах з використанням вибраного комплексу технічних засобів. Тобто це системно організована для виконання завдань управління сукупність методів і засобів збирання, реєстрації, передачі, накопичення, пошуку, опрацювання і захисту інформації на базі застосування розвинутого програмного забезпечення, засобів обчислювальної техніки і зв'язку, а також способів, за допомогою яких інформація пропонується клієнтам.

Мета будь-якої інформаційної технології — отримати потрібну інформацію необхідної якості на заданому носії. При цьому є обмеження на вартість опрацювання даних, трудомісткість процесів використання інформаційного ресурсу, надійність і оперативність процесу опрацювання інформації, якість одержуваної інформації.

Етапи розвитку ІТ

Інформаційна технологія виникла кілька мільйонів років тому разом з виробництвом на Землі. Найпростіші інформаційні технології з'явилися з початком писемності. Це наскельні малюнки, знаки і малюнки на корі, папірусі та ін. Поява книг, виготовлених друкарським способом, стала потужним поштовхом до розвитку інформаційних технологій. У своєму розвитку інформаційна технологія пройшла кілька етапів.

“Ручна” інформаційна технологія панувала до другої половини XIX ст. Уся обробка інформації виконувалася вручну за

допомогою пера, рахівниці, бухгалтерських книг. Зв'язок підтримувався пересиланням пакетів, листів тощо.

“Механічна” інформаційна технологія. Винахід друкарської машинки, телефону, диктофона, модернізація системи поштового зв'язку дали змогу суттєво вдосконалити як окремі операції, так і весь технологічний процес обробки інформації, підвищити продуктивність управлінської праці. Така механізація інформаційної технології стала базою формування організаційних структур в економіці.

“Електрична” технологія. На зміну “механічній” інформаційній технології у 40—50-х роках XX ст. прийшла “електрична”, що ґрунтувалася на широкому використанні електричних друкарських машинок, копіювальних машин, портативних диктофонів. Різко підвищились якість, кількість і швидкість обробки документів.

“Комп'ютерна” інформаційна технологія. Постійне зростання попиту на інформацію та інформаційні послуги зумовило застосування досить широкого спектра технічних засобів, насамперед електронних обчислювальних машин та засобів комунікацій. На їх основі створюються обчислювальні системи і мережі різних конфігурацій не тільки для накопичення, збереження, обробки інформації, а й для максимального наближення термінальних пристроїв до робочого місця фахівця або керівника, що приймає рішення. Це є досягненням багаторічного розвитку АІТ. З появою і широким розвитком електронно-обчислювальних машин (далі — ЕОМ) та периферійної техніки настала ера “комп'ютерної” інформаційної технології, яка у своєму розвитку пройшла три стадії.

Перша стадія (1950—1960) характеризується використанням великих (для того часу) ЕОМ. Вона була зорієнтована на економію машинних ресурсів. Концепція інформаційної технології полягала в такому: все, що можуть зробити люди, вони й мають робити; центральний процесор виконував лише ту частину роботи з обробки інформації, яку люди принципово виконувати не могли, наприклад, масові розрахунки. Основне завдання ІТ можна сформулювати як підвищення ефективності опрацювання даних на підставі використання формалізованих алгоритмів.

Для *другої стадії* (1960—1970) визначальним став широкий випуск малих машин (міні-ЕОМ). Оскільки вартість апаратних засобів (машинних ресурсів) істотно знизилась, то метою інформаційної технології стала економія праці програмістів, тобто необхідно було підвищити ефективність програмування, зокрема за рахунок автоматизації програмних розробок. Докорінно змінилась концептуальна орієнтація — все, що можна запрограмувати, повинні робити машини, а люди зобов'язані виконувати лише те, що не може бути запрограмовано.

Третя стадія інформаційної технології (1970—1990) відома під назвою *нової (сучасної, безпаперової) інформаційної технології*, характеризується масовим випуском персональних електронно-обчислювальних машин (далі — ПЕОМ). Визначальною метою стала економія праці користувачів. Основу нової інформаційної технології становлять розподілена комп'ютерна техніка, “дружнє” програмне забезпечення, розвинуті комунікації. Концепція третьої стадії: автоматизувати можна все, що люди спроможні описати (програмування без програмістів). Тому центральним завданням технології програмування стала розробка інструментальних засобів, які полегшують професіоналам-непрограмістам процес самостійної формалізації індивідуальних знань.

З появою і широким розвитком ЕОМ та периферійної техніки настала ера комп'ютерної інформаційної технології, яка названа *новою (сучасною, безпаперовою) інформаційною технологією*.

Нова інформаційна технологія (комп'ютерна інформаційна технологія) — це інформаційна технологія з “дружнім” інтерфейсом роботи користувача, що використовує персональні комп'ютери і телекомунікаційні засоби. Її інструментарієм є один або декілька взаємопов'язаних програмних продуктів для певного типу комп'ютера, технологія роботи в якому дає змогу досягти поставленої користувачем мети.

Основу нової інформаційної технології (далі — НІТ) становить розподілена комп'ютерна техніка, “дружнє” програмне забезпечення, розвинені комунікації. Користувачеві-непрограмісту надано можливість прямого спілкування з ЕОМ під час роботи в діалоговому режимі. При цьому потужні програмно-апаратні засоби (бази даних, експертні системи та бази знань,

системи підтримки прийняття рішень тощо) створюють комфорт у роботі, дають можливість не лише автоматизувати процес зміни форми та місцезнаходження інформації, а й змінювати її зміст. Завдяки збільшенню обсягів індивідуального виконання робіт комп'ютери допомагають людині підвищувати продуктивність праці, а також ефективність рішень.

Для нової інформаційної технології характерні такі особливості:

- робота користувача в режимі маніпулювання (не програмування) даними. Користувач має бачити (засоби виведення — екран, принтер) і діяти (засоби введення — клавіатура, миша, сканер), а не знати і пам'ятати;
- наскрізна інформаційна підтримка на всіх етапах проходження інформації на основі інтегрованої бази даних, що передбачає одну уніфіковану форму подання, зберігання, пошуку, відображення, відновлення та захисту даних;
- безпаперовий процес обробки документа, під час якого на папері фіксується лише його остаточний варіант, а проміжні версії та необхідні дані, записані на машинні носії, доводяться до користувача через екран дисплея ПК;
- інтерактивний (діалоговий) режим розв'язування задачі з широкими можливостями для користувача;
- можливість колективного виконання документа на основі групи ПК, об'єднаних засобами комунікацій;
- можливість адаптивної перебудови форм і способів подання інформації у процесі розв'язування задачі.

Класифікація ІТ

Нині АІТ можна класифікувати за багатьма ознаками, зокрема за способом реалізації в автоматизованих інформаційних системах (далі — АІС), ступенем охоплення АІТ завдань керування, класами реалізованих технологічних операцій, типом користувацького інтерфейсу, варіантами використання мережі ЕОМ, предметною сферою, що обслуговується (рис. 1.3).

Перспективи розвитку ІТ

Характерними для НІТ є персоналізація засобів обчислювальної техніки, створення локальних мереж ЕОМ і багаторівневих систем обробки даних, організація автоматизованих робочих місць спеціалістів. Арсенал засобів НІТ постійно поповнюється, зокрема значного поширення останніми рока-

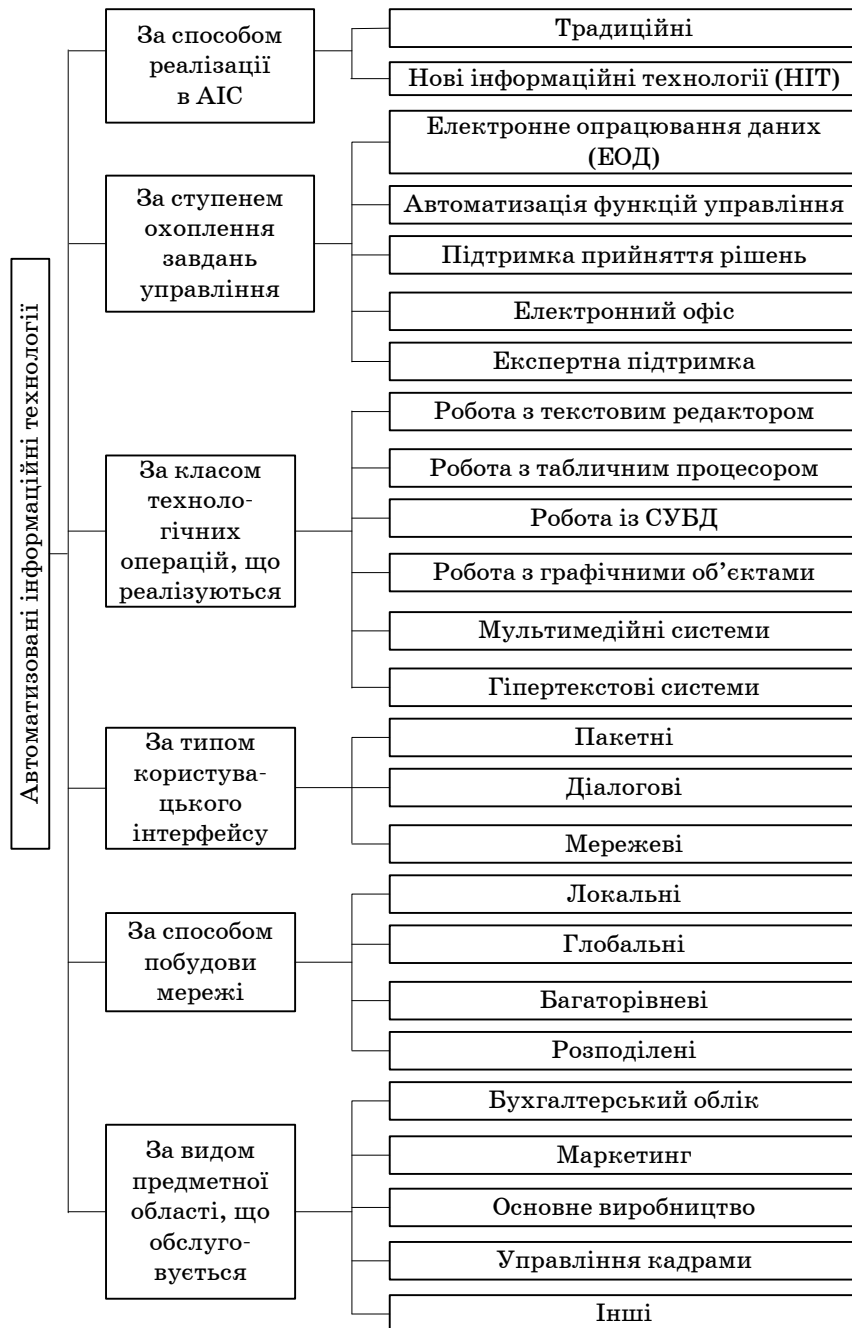


Рис. 1.3. Класифікація інформаційних технологій

ми набули комп'ютерна графіка, мультимедіа, гіпертексти, гіпертекстові технології та системи.

Комп'ютерна (машинна) графіка — один з важливих напрямів розвитку інформаційної технології в сучасних умовах. Під цим поняттям розуміють сукупність методів і засобів автоматизації процесів підготовки, введення, перетворення, зберігання й відображення графічної інформації за допомогою ЕОМ та графічних пристроїв.

Напрями розвитку комп'ютерної графіки такі:

- графіка для автоматизованого проектування в машинобудуванні, будівництві, електроніці, а також художньому конструюванні;
- програмне керування верстатами, роботами-маніпуляторами і підготовкою автоматизованого виробництва;
- кольорова і напівтонова графіка для формування реалістичних зображень просторових об'єктів, у тому числі для машинної мультиплікації;
- автоматизована обробка зображень, їх зберігання, пересилання, аналіз, розпізнавання образів;
- ілюстративна та ділова графіка, наочне подання інформації в дослідженнях, системах управління, виробництві;
- спеціалізована графіка в поліграфії, видавничій справі, рекламі;
- навчальна та ігрова графіка.

Системами **мультимедіа** є інтерактивні комп'ютерні системи, що забезпечують роботу з багатьма інформаційними середовищами, нерухомим зображенням та рухомим відео, анімованою комп'ютерною графікою, текстом і звуком.

Гіпертекст у загальному випадку — це система інформаційних об'єктів (статей), у якій задані й автоматично підтримуються асоціативні та смислові зв'язки між виділеними об'єктами (елементами, поняттями, термінами або розділами). Це текст, де окремі терміни на екрані дисплея виділені підсвічуванням, а відповідне визначення одразу може бути видано на екран. Сфера застосування гіпертекстових технологій дуже широка: видавнича діяльність, бібліотечна робота, навчальні системи, розробка документації, законів, довідкового управління, баз даних, знань та ін.

Така система містить засоби подання та обробки слів і гіпертекстових структур, інформаційного поєднання документів, а також прокладання і запам'ятовування шляхів у гіпертексті. Під час роботи з гіпертекстовою системою поступово зникає відмінність між автором і читачем, тобто гіпертехнологія стає авторською.

Запитання і завдання для самоконтролю

1. Дайте визначення інформації.
2. Які атрибути інформації ви знаєте?
3. Розкрийте властивості інформації.
4. Розкрийте співвідношення інформації і даних.
5. Які є види інформації?
6. Що таке інформаційний ресурс?
7. Як управляти інформаційним ресурсом?
8. Дайте визначення інформаційним технологіям.
9. Які ви знаєте етапи розвитку ІТ?
10. На чому базується класифікація ІТ?
11. Які перспективи розвитку ІТ?

Розділ 2

ТИПОВА СТРУКТУРА І СКЛАД ІНФОРМАЦІЙНИХ СИСТЕМ

2.1. Інформаційні системи

Розвиток комп'ютерної інформаційної технології нерозривно пов'язаний з розвитком інформаційних систем, які в економіці використовуються для автоматизованого (людино-машинного) розв'язування економічних задач. Для розв'язування будь-якої задачі за допомогою комп'ютера необхідно створити інформаційне (забезпечити розрахунки потрібними даними) і математичне забезпечення (створити математичну модель розв'язування задачі, за якою складається програма для ЕОМ).

Завдання інформаційних систем — це виробництво інформації, яка потрібна організації для забезпечення ефективного управління всіма своїми ресурсами, створення інформаційного і технічного середовища з метою управління організацією.

Інформаційна технологія — це спосіб перетворення інформації, який реалізується в межах інформаційної системи, де можуть використовуватися багато таких технологій. Проте вона ширша за інформаційну систему і може існувати поза нею.

Для успішної роботи інформаційної системи необхідно таке:

- виявлення інформаційних потреб;
- добір джерел інформації;
- збирання інформації;

- введення інформації із зовнішніх або внутрішніх джерел;
- опрацювання інформації;
- виведення інформації для надання її споживачам або передачі в іншу систему;
- організація використання інформації для оцінки тенденцій, розробки прогнозів, оцінки альтернатив рішень і дій, вироблення стратегії;
- організація зворотного зв'язку інформації, переопрацьованої людьми такої організації, корекція вхідної інформації.

В основі будь-якої системи лежить процес, зокрема в основі інформаційної системи — процес виробництва інформації. У цьому розумінні ми можемо розглядати інформаційну систему як систему управління, де цей процес є об'єктом управління.

Зростання обсягів інформації в інформаційній системі організацій, потреба у прискоренні й більш складних способах її переопрацювання зумовлюють необхідність автоматизації роботи інформаційної системи, тобто автоматизації опрацювання інформації.

Автоматизована інформаційна система управління організацією є взаємопов'язаною сукупністю даних, обладнання, програмних засобів, персоналу, стандартів процедур, призначених для збирання, опрацювання, розподілу, зберігання, видачі (надання) інформації відповідно до вимог, що впливають з діяльності організації. Як правило, це система для підтримки прийняття рішень і виробництва інформаційних продуктів, що використовує комп'ютерну інформаційну технологію, і персонал, який взаємодіє з комп'ютерами і телекомунікаціями.

Технологія роботи в комп'ютеризованій інформаційній системі має бути доступна для розуміння фахівцем некомп'ютерної галузі та може бути успішно використана для контролю процесів професійної діяльності й управління ними.

2.2. Типи інформаційних систем

Створенню інформаційних систем у всьому світі приділяється багато уваги. За масштабами, темпами зростання, витратами матеріальних, фінансових і трудових ресурсів, а також за ступенем впливу на процеси управління проблему створення ІС слід розглядати як велике народногосподарське завдання. Інформаційні системи можуть значно різнитися за типами об'єктів управління, характером і обсягом розв'язуваних задач та низкою інших ознак.

Загальноприйнятої класифікації ІС досі немає, тому їх можна класифікувати за різними ознаками. Найбільш поширеними протягом тривалого часу були такі класифікаційні угруповання систем.

1. *За рівнем або сферою діяльності* — державні, територіальні (регіональні), галузеві, об'єднань, підприємств або установ, технологічних процесів.

2. *За рівнем автоматизації процесів управління* — інформаційно-пошукові, інформаційно-довідкові, інформаційно-керівні, системи підтримки прийняття рішень, інтелектуальні ІС тощо.

3. *За ступенем централізації обробки інформації* — централізовані ІС, децентралізовані ІС, інформаційні системи колективного використання.

4. *За ступенем інтеграції функцій* — багаторівневі ІС з інтеграцією за рівнями управління (підприємство — об'єднання, об'єднання — галузь та ін.), багаторівневі ІС з інтеграцією за рівнями планування тощо.

Державні ІС призначені для вирішення найважливіших народногосподарських проблем країни. На базі використання обчислювальних комплексів та економіко-математичних методів у них складають перспективні й поточні плани розвитку країни, ведуть облік результатів і регулюють діяльність окремих ланок народного господарства, розробляють державний бюджет, контролюють його виконання тощо.

Центральне місце в мережі державних ІС належить автоматизованій системі державної статистики (далі — АСДС). Роль

та місце АСДС в ієрархії управління визначається тим, що вона є основним джерелом статистичної інформації, дуже необхідної для функціонування всіх державних і регіональних ІС.

Серед ІС, з якими взаємодіє АСДС, важливе місце посідає автоматизована система планових розрахунків (далі — АСПР). АСПР функціонує при Міністерстві економіки України і є інформаційною системою, призначеною для розробки народно-господарських планів та контролю за їх виконанням в умовах застосування засобів обчислювальної техніки для збирання й обробки інформації.

АСДС взаємодіє також з державною інформаційною автоматизованою системою фінансових розрахунків (АСФР) при Міністерстві фінансів України. АСФР призначена для автоматизації фінансових розрахунків на базі сучасної обчислювальної техніки з формування державного бюджету країни та контролю за його виконанням. При цьому вона використовує статистичну інформацію про випуск і реалізацію продукції, фонди споживання, запаси й витрати фінансових ресурсів та ін.

Відомі й інші державні ІС: автоматизована система обробки інформації з цін (далі — АСОІ цін), автоматизована система управління Національним банком (далі — АСУ банку), автоматизована система обробки науково-технічної інформації (АСО НТІ) тощо.

Територіальні (регіональні) ІС призначені для управління адміністративно-територіальним регіоном. До них належать ІС області, міста, району. Ці системи обробляють інформацію, яка необхідна для реалізації функцій управління регіоном, формування звітності й видачі оперативних даних місцевим і керівним державним та господарським органам.

Галузеві інформаційні системи управління призначені для управління підвідомчими підприємствами та організаціями. Галузеві ІС діють у промисловості та сільському господарстві, будівництві, транспорті тощо. У них вирішуються завдання інформаційного обслуговування апарату управління галузевих міністерств і їх підрозділів. Галузеві ІС різняться за сферами застосування — промислова, непромислова, наукова.

Інформаційні автоматизовані системи управління підприємствами (далі — АСУП) — це системи із застосуванням сучасних засобів автоматизованої обробки даних, економіко-

математичних та інших методів для регулярного розв’язування завдань управління виробничо-господарською діяльністю підприємства.

Інформаційні автоматизовані системи управління технологічними процесами (далі — АСУ ТП) керують станом технологічних процесів (робота верстата, домни тощо). Перша й головна відмінність цих систем від розглянутих раніше полягає, передусім, у характері об’єкта управління: для АСУ ТП — це різноманітні машини, прилади, обладнання, а для державних, територіальних та інших АСУ — колективи людей. Друга відмінність полягає у формі передавання інформації: для АСУ ТП — це сигнал, а для інших АСУ — документи.

Залежно від мети функціонування та завдань, які покладено на ІС на етапах збирання і змістового оброблення даних, розрізняють такі типи ІС: інформаційно-пошукові, інформаційно-довідкові, інформаційно-керівні (управлінські), інтелектуальні інформаційні системи та системи підтримки прийняття рішень.

2.3. Компоненти інформаційних систем

Практично всі розглянуті різновиди інформаційних систем незалежно від сфери застосування включають один і той самий набір компонентів (рис. 2.1):

- функціональні компоненти;
- компоненти системи опрацювання даних;
- організаційні компоненти.

Функціональні компоненти — це система функцій управління, або повний набір (комплекс) взаємопов’язаних у часі й просторі робіт з управління, необхідних для досягнення поставлених перед підприємством цілей.

Будь-яка складна управлінська функція поділяється на низку дрібніших завдань і, зрештою, доводиться до безпосереднього виконавця. Саме від того, як буде виконане те або інше завдання окремим працівником, залежить успіх виконання кінцевих завдань підприємства загалом. Таким чином, уся складна сукупність управлінських впливів повинна мати



Рис. 2.1. Структура інформаційної системи

своїм остаточним результатом доведення загальних завдань, що стоять перед підприємством, до кожного конкретного виконавця незалежно від його службового становища.

Наведені положення підкреслюють не тільки індивідуальний, а й груповий характер функції управління, а діловий (практичний) результат утворюється не епізодично, а постійно.

Весь процес управління підприємством зводиться або до лінійного (наприклад, адміністративного) управління підприємством чи його структурним підрозділом, або до функціонального (матеріально-технічне забезпечення, бухгалтерський облік тощо) управління.

Тому декомпозиція інформаційної системи за функціональною ознакою (рис. 2.1) полягає у виокремленні її окремих частин, які мають назву *функціональних підсистем* (далі — ПС) (функціональні модулі, бізнес-додатки), що реалізують систему функцій управління. Функціональною ознакою зумовлюється призначення підсистеми, тобто те, для якої сфери діяльності вона призначена і які основні цілі, завдання та функції вона виконує. Функціональні підсистеми істотно залежать від предметної області (сфери застосування) інформаційних систем.

Вибір складу функціональних завдань функціональних підсистем управління здійснюється звичайно з урахуванням основних фаз управління: планування; обліку, контролю і аналізу; регулювання (виконання).

Планування — це управлінська функція, що забезпечує формування планів, відповідно до яких буде організовано функціонування об'єкта управління. Традиційно виокремлюють перспективне (5—10 років), річне (1 рік) та оперативне (доба, тиждень, декада, місяць) планування.

Облік, контроль і аналіз — функції, що забезпечують одержання даних про стан керованої системи за певний проміжок часу, визначення факту і причини відхилення стану об'єкта управління від його планованого стану, а також виявлення розмірів цього відхилення. Облік ведеться за показниками плану у вибраному діапазоні планування (оперативний, середньостроковий тощо).

Регулювання (виконання) — це функція, що забезпечує порівняння планованих та фактичних показників функціонування об'єкта управління і реалізацію необхідних керівних впливів за наявності відхилень від запланованих у заданому діапазоні (відрізку). Відповідно до виокремлених функціональних підсистем та з урахуванням вимог управління визначається склад завдань функціональних підсистем. Наприклад, інформаційна система управління персоналом підприємства може містити такі функціональні підсистеми:

- планування чисельності персоналу підприємства;
- розрахунок фонду заробітної плати персоналу;
- планування та організація навчання персоналу;
- управління кадровими переміщеннями;

- статистичний облік і звітність;
- довідки за запитом.

Вибір та обґрунтування складу функціональних завдань є одним із найважливіших елементів створення інформаційних систем. Аналіз функціональних завдань показує, що вони по-різному реалізуються в умовах використання інформаційних систем. Одне й те саме завдання може бути розв'язане (реалізоване) різними математичними методами, моделями й алгоритмами. Іноді цю функціональну підсистему називають підсистемою *математичного забезпечення*.

Серед багатьох варіантів реалізації є, як правило, найкращий, зумовлений можливостями обчислювальної системи і системи опрацювання даних у цілому.

У сучасних системах автоматизації проектування інформаційних систем цей компонент входить до складу так званих банків моделей і алгоритмів, з яких під час розробки інформаційних систем вибираються найефективніші для конкретного об'єкта управління.

Компоненти системи опрацювання даних

Основна функція *системи опрацювання даних* — це реалізація таких типових операцій:

- збирання, реєстрація і перенесення інформації на машинні носії;
- передача інформації в місця її зберігання й опрацювання;
- введення інформації в ЕОМ, контроль введення та компонування інформації в пам'яті комп'ютера;
- створення і ведення внутрішньомашинної інформаційної бази;
- опрацювання інформації на ЕОМ (накопичення, сортування, коригування, вибірка, арифметичне і логічне опрацювання) для виконання функціональних завдань системи (підсистеми) управління об'єктом;
- виведення інформації у вигляді табуляграм, відеограм, сигналів для прямого управління технологічними процесами, інформації для зв'язку з іншими системами;
- організація, управління (адміністрування) обчислювальним процесом (планування, облік, контроль, аналіз обчислень у локальних і глобальних обчислювальних мережах).

Система опрацювання даних (далі — СОД) призначена для інформаційного обслуговування фахівців різних органів управління підприємства, що приймають управлінські рішення.

Виокремлення типових операцій опрацювання даних дало змогу створити спеціалізовані програмно-апаратні комплекси для їх реалізації: різні периферійні пристрої, оргтехніку, стандартні набори програм, у тому числі пакети прикладних програм (ППП). Конфігурація апаратних комплексів утворює так звану топологію обчислювальних систем.

Практично всі системи опрацювання даних інформаційних систем незалежно від сфери їх застосування включають однаковий набір складових (компонентів), що називаються *видами забезпечення* (рис. 2.1). Прийнято виокремлювати інформаційне, програмне, технічне, правове, лінгвістичне забезпечення.

Інформаційне забезпечення — це сукупність методів і засобів розміщення й організації інформації, що включають системи класифікації і кодування, уніфіковані системи документації, раціоналізації документообігу та форми документів, методів створення внутрішньомашинної інформаційної бази інформаційної системи. Від якості розробленого інформаційного забезпечення особливо залежать достовірність і якість прийнятих управлінських рішень.

Програмне забезпечення — сукупність програмних засобів для створення та експлуатації СОД засобами обчислювальної техніки. До складу програмного забезпечення входять базові (загальносистемні) та прикладні (спеціальні) програмні продукти. *Базові програмні засоби* використовують для автоматизації взаємодії людини і комп'ютера, організації типових процедур опрацювання даних, контролю і діагностики функціонування технічних засобів СОД. *Прикладне програмне забезпечення* становить сукупність програмних продуктів, призначених для автоматизованого розв'язування функціональних завдань інформаційної системи. Вони можуть бути розроблені як універсальні засоби (текстові редактори, електронні таблиці, системи управління базами даних) та як спеціалізовані, тобто такі, що реалізують функціональні підсистеми (бізнес-процеси) об'єктів різної природи (економічні, інженерні, технічні тощо).

Технічне забезпечення — це комплекс технічних засобів, що застосовуються для функціонування системи опрацювання даних, і містить пристрої, за допомогою яких виконуються типові операції опрацювання даних як поза ЕОМ (периферійні технічні засоби збирання, реєстрації, первинного опрацювання інформації, оргтехніка різного призначення, засоби телекомунікації і зв'язку), так і на ЕОМ різних класів.

Правове забезпечення — це сукупність правових норм, що регламентують створення і функціонування інформаційної системи. Правове забезпечення розробки інформаційної системи включає нормативні акти договірних взаємовідносин між замовником і розробником ІС, правове регулювання відхилень. Правове забезпечення функціонування СОД включає: умови надання юридичної чинності документам, отриманим із застосуванням обчислювальної техніки; права, обов'язки і відповідальність персоналу, в тому числі за своєчасність і точність опрацювання інформації; правила користування інформацією і порядок вирішення суперечок щодо її достовірності.

Лінгвістичне забезпечення — це сукупність мовних засобів, що використовуються на різних стадіях створення та експлуатації СОД для підвищення ефективності розробки й забезпечення спілкування людини та ЕОМ.

Щодо організаційних компонентів інформаційної системи, то виділення таких компонентів у самостійний напрям зумовлюється особливою важливістю людського чинника (персоналу) в успішному функціонуванні ІС. Перш ніж запроваджувати дорогу систему опрацювання даних, слід провести величезну роботу з упорядкування та вдосконалення організаційної структури об'єкта; в іншому випадку ефективність ІС буде низькою. Головна проблема при цьому полягає у виявленні ступеня відповідності існуючих функцій управління й організаційної структури, що реалізує ці функції і стратегію розвитку підприємства. Засобами досягнення мети — **удосконалення організаційних структур** — є різні методи моделювання.

Під **організаційними компонентами ІС** розуміють сукупність методів і засобів, що дають змогу удосконалити організаційну структуру об'єктів і управлінські функції, які виконуються структурними підрозділами; визначити штатний розклад і чисельний склад кожного структурного підрозділу;

розробити посадові інструкції персоналу управління в умовах функціонування СОД.

Упровадження інформаційних систем сприяє вдосконаленню організаційних структур, оскільки передбачає визначення розрахункової, тобто науково обґрунтованої, чисельності апарату управління за структурними підрозділами з обов'язковим вирішенням, зокрема таких проблем:

- достовірне зарахування кожного працівника до відповідного структурного підрозділу (відділу, бюро та ін.);
- установлення чітких службових обов'язків кожного працівника в межах підрозділу. При цьому обов'язки працівників, що обіймають ту чи іншу посаду, не залежать від конкретної особи, яка їх виконує. Сукупність спільних обов'язків має гарантувати їхню несуперечливість і можливість досягнення загального результату;
- визначення нормального завантаження працівника роботою протягом дня і на календарний період;
- розробка посадових інструкцій персоналу в умовах функціонування СОД, зокрема в умовах аварійних ситуацій.

Запитання і завдання для самоконтролю

1. Дайте визначення інформаційним системам.
2. Що таке автоматизовані інформаційні системи?
3. Які є типи ІС?
4. Назвіть складові ІС.
5. З чого складаються функціональні компоненти ІС?
6. Охарактеризуйте компоненти системи опрацювання даних.
7. Дайте визначення інформаційному, програмному, технічному, правовому та лінгвістичному забезпеченню.
8. Що таке організаційні компоненти ІС?

Частина **III**

**ЄДИНА АВТОМАТИЗОВАНА
ІНФОРМАЦІЙНА СИСТЕМА
ДЕРЖАВНОЇ МИТНОЇ СЛУЖБИ
УКРАЇНИ**

Розділ 3

ІСТОРІЯ РОЗВИТКУ ІНФОРМАЦІЙНОЇ СИСТЕМИ МИТНОЇ СЛУЖБИ УКРАЇНИ

Єдина автоматизована інформаційна система Державної митної служби України (далі — ЄАІС Держмитслужби України) почала створюватися ще у 1992 р., коли служба існувала як Державний митний комітет України (до 29 листопада 1996 р.).

На першому етапі (1992—1993) поступово впроваджувалася система збирання й обробки електронних копій вантажних митних декларацій (ВМД), яка містила програмне забезпечення “Інспектор”, розроблене фахівцями інформаційного обчислювального центру Державного митного комітету України (ІОЦ ДМКУ). Учасник зовнішньоекономічної діяльності (ЗЕД) подавав до митного органу паперовий примірник вантажної митної декларації. Інспекторами спеціалізованих підрозділів (митної статистики) інформація вводилася в програму “Інспектор” і таким чином формувалась в електронному вигляді. Інформація, що вводилась до бази даних, записувалась на магнітні носії (дискети) і за допомогою фельд’єгерського зв’язку доставлялася з кожного митного органу в підрозділ статистики інформаційного обчислювального центру (ІОЦ). Після обробки цієї інформації формувалися статистичні звіти

для керівництва Державного митного комітету, а також митна статистика зовнішньої торгівлі України.

Процедура формування електронних копій ВМД з паперових оригіналів була досить трудомісткою і потребувала великої кількості операторів. Термін надання цієї інформації до ІОЦ становив декілька днів.

Відомо, що розробка й упровадження комп'ютерних технологій стають більш ефективними, коли здійснюються на основі єдиного системного проекту. Тому в 1993 р. було розроблено концепцію створення ЄАІС Держмитслужби.

На другому етапі (1994—1995) з метою вдосконалення та прискорення інформаційного обміну в межах митної системи, організації ефективного функціонування автоматизованої системи митного оформлення, поліпшення якості та забезпечення повноти збору даних митної статистики Державний митний комітет України розпочав впровадження в митних органах відомчої системи електронної пошти на базі програмного забезпечення (ПЗ) корпорації Lotus Development Corporation — Lotus cc:Mail. Одночасно в країні почали формуватися брокерські фірми, які надавали допомогу суб'єктам ЗЕД з питань декларування товарів і транспортних засобів та були посередниками між митними органами й учасниками ЗЕД. Зазначені фірми подавали вже разом із заповненим паперовим примірником ВМД її електронну копію. Спеціалізоване програмне забезпечення дало можливість значно скоротити час на перевірку декларації.

Виконуючи обидва завдання, які виникли на першому етапі, фахівці Державного митного комітету, по-перше, перенесли на суб'єкта зовнішньої економічної діяльності та на митного брокера трудомістку процедуру з формування електронної копії ВМД з її подальшою перевіркою в митному органі — було створено програмне забезпечення для декларантів і митних брокерів “Митний брокер”, а також розробки фахівців інформаційного обчислювального центру Державного митного комітету, а по-друге, з використанням системи електронної пошти на базі ПЗ Lotus cc:Mail вирішили питання оперативної передачі інформації безпосередньо з митних органів до ІОЦ за допомогою модемного зв'язку.

З розширенням зовнішньоекономічних відносин України та подальшим збільшенням обсягів зовнішньоекономічних операцій різко зросли потік і масштаби митної інформації.

Уже на другому етапі з'явилися проблеми подальшої автоматизації митного оформлення, контролю ввезення автотранспортних засобів на територію України, контролю за доставкою в митниці призначення підакцизних товарів тощо. Приймається рішення про створення системи оперативного контролю. Надійне функціонування такої системи потребувало створення транспортної мережі супутникового зв'язку.

З січня 1996 р. розпочався *третій етап* упровадження ЄАІС у митних органах.

Однією з найбільших проблем від часу становлення Державної митної служби України був контроль доставки вантажів у митниці призначення. Системи електронного контролю за доставкою вантажів у митниці призначення не існувало, попередньо перевірити зазначені в деклараціях дані було практично неможливо. Цим почали користуватись "нечисті на руку" підприємці для ввезення на територію України високоліквідних товарів без сплати ввізного мита та інших податків і зборів.

Такий стан справ не задовольняв керівництво країни, і в 1996 р. у Держмитслужбі почалася розробка системи "Контроль доставки вантажів у митниці призначення".

У 1997 р. на виконання вимог постанови Кабінету Міністрів України щодо спрощення процедур контролю за ввезенням підакцизних товарів Держмитслужбою розроблено відповідний механізм, а саме: пропуск вантажів на митну територію України митними органами здійснюється виключно за наявності електронної копії вантажної митної декларації типу АД (акцизна декларація) у центральній базі даних.

Водночас нормативними документами Держмитслужби запроваджено пропуск усіх без винятку вантажів на адресу суб'єктів зовнішньоекономічної діяльності (ЗЕД) тільки за наявності відомостей щодо їх акредитації в митниці призначення, у центральній базі даних.

За допомогою сучасних інформаційних технологій побудовано трирівневу систему клієнт-сервер з доступом користувачів до ресурсів серверів центральної бази даних через web-

сервер. Почалася розробка та поетапне впровадження програмно-інформаційних комплексів (ПІК) ЄАІС Держмитслужби.

У 1998 р. почався *четвертий етап* розбудови ЄАІС Держмитслужби. У тому ж році, враховуючи незадовільний розвиток в Україні наземних каналів зв'язку, введено в промислову експлуатацію транспортну мережу супутникового зв'язку (ТМСЗ), яка нараховувала: 246 станцій супутникового зв'язку, 6 радіорелейних станцій, комунікаційне устаткування. Така великомасштабна робота у стислі терміни в межах усієї держави проводилася вперше не тільки в Україні, а й у Східній Європі.

Наприкінці 1998 р. наказом Держмитслужби України затверджено Положення про порядок контролю за доставкою вантажів у митниці призначення. З травня 1999 р. розпочато поетапну розробку та впровадження відповідного програмно-інформаційного комплексу, перший етап якого — контроль за ввезенням вантажів автомобільним транспортом за допомогою ВМД за типами АД, ПД (попередня декларація) та ПП (попереднє повідомлення).

На кожному новому етапі розробки програмно-інформаційного комплексу відповідно до наказу (січень 2000 р. — режим “експорт”, червень — режим “транзит” автомобільним транспортом, листопад — режим “транзит” залізничним транспортом) виникла потреба цілодобового пересилання електронних копій ВМД усіх типів до центральної бази даних безпосередньо з місць митного оформлення (митні пости, пункти пропуску через митний кордон).

Зараз автоматизованою системою охоплено всі митні режими (імпорт, експорт, транзит):

- автомобільним транспортом — у повному обсязі;
- залізничним транспортом — при імпорті, транзиті та експорті (давальницька сировина);
- авіаційним та морським транспортом при імпорті.

Протягом 1998—2000 рр. Державна митна служба України ввела в дію такий важливий елемент Єдиної автоматизованої інформаційної системи митних органів, як центральна база даних. Фактично всі програмно-інформаційні комплекси (ПІК), що розроблялись Держмитслужбою, побудовані з її використанням. Це дало можливість акумулювати в одному місці прак-

тично всю інформацію щодо митного оформлення товарів і транспортних засобів та контролю за їх доставкою, ведення баз даних про порушників митних правил, спеціальних санкцій Міністерства економіки до учасників ЗЕД тощо.

За допомогою використання центральної бази даних ДМСУ будь-яка митниця в реальному часі з використанням каналів зв'язку може звірити інформацію з паперовими документами, які подаються під час митного контролю та митного оформлення.

У 2000 р. базу даних статистики зовнішньої торгівлі переведено на СУБД Oracle і вся статистична звітність почала базуватись саме на цьому, що дало можливість отримувати детальну інформацію у будь-яких розрізах, застосовуючи дані з електронних копій ВМД.

У 2005 р. почався *п'ятий етап* розбудови ЄАІС ДМСУ в рамках створення багатофункціональної комплексної системи “Електронна митниця”.

Постановою Кабінету Міністрів України від 24 лютого 2003 р. № 208 встановлено, що одним з пріоритетних завдань розвитку інформаційного суспільства є надання громадянам та юридичним особам інформаційних та інших послуг шляхом використання електронної інформаційної системи “Електронний Уряд”, яка забезпечує інформаційну взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій.

Держави — члени ЄС протягом 2005—2006 рр. прийняли рішення діяти в рамках структури “Електронної Європи” та затвердили Рішення Ради щодо простого та безпаперового середовища для митниці й торгівлі.

Враховуючи завдання, покладені Президентом і урядом України на митну службу, які спрямовані на наближення митних правил України до світових норм і стандартів, у 2006 р. Держмитслужбою України розроблено Концепцію створення системи “Електронна митниця”. Метою Концепції є визначення стратегії створення багатофункціональної комплексної системи “Електронна митниця” на базі Єдиної автоматизованої інформаційної системи ДМСУ як одного з механізмів забезпечення митної безпеки України. Концепція передбачає визначення принципів побудови Електронної митниці, основних по-

ложень з формування її інформаційно-телекомунікаційного забезпечення, етапів упровадження, а також створення передумов до інтеграції України у світову інформаційну спільноту. Впровадження багатофункціональної комплексної системи “Електронна митниця” розраховано до 2013 р.

Запитання і завдання для самоконтролю

1. Що стало причиною створення ЄАІС ДМСУ?
2. Які програми використовувалися для збирання й обробки електронних копій ВМД на першому та другому етапах розвитку ЄАІС ДМСУ?
3. Обґрунтуйте необхідність упровадження системи “Контролю доставки вантажів у митниці призначення”.
4. Які інформаційні технології забезпечують швидкий та зручний обмін інформацією в електронному вигляді?
5. Проаналізуйте етапи розвитку й упровадження системи “Контролю доставки вантажів у митниці призначення”.
6. Назвіть ПІКи, які безпосередньо використовуються під час митного оформлення.
7. Вкажіть ПІКи, які призначені для роботи з довідковою інформацією.

Розділ 4

ПРИЗНАЧЕННЯ ТА ОСНОВНІ ПРИНЦИПИ ПОБУДОВИ ЄАІС ДЕРЖМИТСЛУЖБИ УКРАЇНИ

У сучасних умовах економічного розвитку України та виходу її на широку міжнародну арену особливе значення в системі органів державного управління має митна служба. Здійснення митної справи й ефективна діяльність Державної митної служби України можливі лише за умови забезпечення митних органів сучасною комп'ютерною технікою та використання сучасних телекомунікаційних мереж для організації автоматизованого інформаційного обміну, як у межах митної служби, так і з іншими міністерствами і відомствами України, а також з організаціями закордонних держав.

З часу створення митної служби України велика увага приділяється розробці й впровадженню Єдиної автоматизованої інформаційної системи (ЄАІС) митних органів, призначення якої — виконання функціональних завдань митних органів з використанням передових технологій передачі й обробки інформації за допомогою засобів обчислювальної техніки та зв'язку.

27 липня 1993 р. прийнято концепцію створення Єдиної автоматизованої інформаційної системи митних органів України і план її реалізації. Метою створення Єдиної автоматизованої

інформаційної системи є підвищення ефективності формування і здійснення єдиної митної політики держави і діяльності митних органів під час виконання основних і допоміжних функцій за допомогою сучасних засобів комп'ютерної техніки, засобів передачі даних, математичних методів, перспективних комп'ютерних технологій.

Створення ЄАІС має такі основні завдання:

- формування об'єктивної митної статистики з максимальним часом затримки інформації не більше ніж півдоби;
- забезпечення оперативної та ефективної інформаційної взаємодії відповідних підрозділів митної служби з питань боротьби з контрабандою та порушенням митних правил, доведення регламентуючих документів до виконавців і контроль за їх виконанням, підтримка в актуальному стані нормативно-довідкової і звітної інформації як у центральному апараті ДМСУ, так і в підпорядкованих митницях та спеціалізованих митних установах;
- глибока і всебічна автоматизація процесів митного оформлення, обліку митних платежів; обліку кадрового складу; бухгалтерського обліку; фінансового забезпечення; обліку розподілу і поповнення матеріальних ресурсів; обліку й оптимізації контролю виконання на усіх рівнях системи;
- забезпечення автоматизованого інформаційного обміну Державної митної служби з іншими міністерствами і відомствами України, а також з організаціями закордонних держав;
- перехід ЄАІС ДМСУ на сучасні інформаційні технології і міжнародні стандарти, а також розробка матеріальної бази для ефективного використання митних експертних систем.

Єдина автоматизована інформаційна система митної служби України за короткий час перетворилася на унікальний інструмент реалізації основних митних інформаційних технологій на всіх рівнях: від митного поста до центрального апарату Держмитслужби України.

Аналогічні системи створені та створюються за кордоном практично в усіх митних службах розвинутих країн. Наприклад, у США, Англії, Франції, Німеччині такі системи створювалися понад 20 років відповідно до національних митних правил.

Для організації виконання програми поетапної розробки ЄАІС Державної митної служби України на базі інформаційного обчислювального центру Держмитслужби України було створено Інформаційно-аналітичне митне управління (ІАМУ) Держмитслужби України як спеціалізовану митну установу щодо розробки, впровадження, супроводження та експлуатації ЄАІС Держмитслужби. На сьогодні це Регіональна інформаційна митниця, на яку відповідно до Митного кодексу України, Положення про Державну митну службу України, Концепції створення Єдиної автоматизованої інформаційної системи Державної митної служби України покладено виконання таких завдань:

- упровадження і розвиток інформаційних технологій Держмитслужби України;
- забезпечення розвитку й модернізації ЄАІС, інформаційного, технічного, телекомунікаційного, програмного забезпечення функціонування Держмитслужби України;
- управління функціонуванням ЄАІС у цілому та її складових;
- ведення центральної бази даних ЄАІС;
- організаційно-технічне, методичне супроводження та розвиток відомчої телекомунікаційної мережі Держмитслужби України, розподілених інформаційно-телекомунікаційних комплексів, локально-обчислювальної мережі центрального органу виконавчої влади в галузі митної справи та митних органів;
- організаційне забезпечення завдань керування системою захисту інформації в автоматизованих системах та ЄАІС;
- своєчасне, повне та об'єктивне інформування керівництва Держмитслужби України про стан автоматизації процесів управління в ЄАІС, розроблення пропозицій щодо їх поліпшення;
- розроблення, впровадження та супроводження програмного забезпечення з питань, що належать до компетенції митної служби України;
- збирання, узагальнення та проведення аналізу пропозицій митних органів України та сторонніх організацій щодо тематики науково-дослідних та дослідно-конструкторських ро-

біт, спрямованих на вирішення актуальних проблем науково-технічного розвитку Держмитслужби України.

Реалізація ЄАІС складається з поетапного процесу розробки й упровадження основних автоматизованих митних інформаційних технологій, поєднаних в технічному, програмному і телекомунікаційному середовищі.

Запитання і завдання для самоконтролю

1. Які положення покладено в основу концепції створення ЄАІС ДМСУ?
2. На який митний орган покладено розробку й упровадження новітніх інформаційних технологій у митній службі України?
3. Чому впровадження ЄАІС виконується поетапно?

Розділ 5

СТРУКТУРА, СКЛАД І ФУНКЦІЇ ЄАІС

Пріоритетні інформаційні митні технології реалізовані за допомогою ЄАІС у митних органах усіх рівнів (центральный апарат Держмитслужби, регіональні митниці, митниці, митні пости, підрозділи митного оформлення тощо), центром якої є Регіональна інформаційна митниця. ЄАІС складається з 5 основних підсистем:

- 1) автоматизована підсистема митного оформлення;
- 2) митна адміністративно-правова підсистема;
- 3) митна підсистема інформаційної безпеки;
- 4) митна зовнішня інформаційна підсистема;
- 5) митна телекомунікаційна підсистема.

Автоматизована підсистема митного оформлення охоплює безпосередньо діяльність митних органів у двох основних напрямках — торгового й неторгового обігу, вирішуючи завдання автоматизації процесів:

- оформлення ВМД;
- обліку і контролю транзитного переміщення вантажів територією України;
- обліку й контролю перебування товарів на ліцензійних і митних складах;
- обліку й контролю зворотного ввезення-вивезення майна інофірм, представництв і виставок;

- обліку й контролю поштових відправлень;
- обліку автомобілів і засобів власного транспорту;
- обліку й контролю несупроводжуваного багажу;
- обробки даних комерційних доповнень (електронний обмін інформацією з учасниками зовнішньоекономічної діяльності).

Митна адміністративно-правова підсистема забезпечує управління митними органами на всіх рівнях, контроль і дотримання законності під час автоматизованого митного оформлення.

Основними завданнями підсистеми є автоматизація процесів:

- боротьби з контрабандою та порушеннями митних правил;
- тарифного регулювання й управління;
- експортно-імпортного контролю;
- антидемпінгового й антимонопольного контролю;
- фінансово-валютного контролю;
- оперативної служби;
- бюджетного фінансування;
- збирання коштів у бюджет;
- кадрової служби;
- статистичної служби;
- правової та нормативної служби;
- канцелярії та контролю документопотоку;
- матеріально-технічного забезпечення.

Митна підсистема інформаційної безпеки забезпечує контроль і оперативне управління функціонуванням системи в цілому. Її основними завданнями є:

- забезпечення безпеки ЄАІС;
- поділ рівня привілеїв і доступу до системи;
- доступ до системи за паролем;
- контроль доступу до системи;
- контроль логічного стану системи;
- контроль і управління цілісністю системи;
- статистика роботи системи.

Митна зовнішня інформаційна підсистема забезпечує обмін необхідною інформацією з іншими організаціями України, іноземними державами і міждержавними організаціями, встановлює необхідний рівень повноважень доступу та підтримує його.

Митна телекомунікаційна підсистема є базовою транспортною системою і складається з Відомчої телекомунікацій-

ної мережі (ВТМ) ЄАІС Держмитслужби України та Інформаційно-телекомунікаційного комплексу Держмитслужби України “Електронна пошта”.

Митна телекомунікаційна підсистема також є базовою транспортною системою і контролює маршрутизацію й роботу запитів (отримання повідомлень у глобальній мережі в он-лайн режимі та передачу повідомлень в оф-лайн режимі електронної пошти).

Підсистема забезпечує:

- роботу і взаємозв’язок усіх підсистем ЄАІС Держмитслужби України, об’єднує всі митні органи, спеціалізовані митні установи, організації та їх підрозділи;
- цілодобову роботу головного інформаційно-телекомунікаційного комплексу;
- з’єднання головного інформаційно-телекомунікаційного комплексу, регіональних інформаційно-телекомунікаційних комплексів та їх користувачів через наземні цифрові, супутникові, низькошвидкісні комутовані та радіоканали зв’язку;
- цілодобову адресацію, маршрутизацію й доставку повідомлень у відомчій телекомунікаційній мережі митної служби в режимі реального часу;
- підтримку поштових функцій з використанням наявних стандартних протоколів обміну (експлуатується система електронної пошти Lotus Domino/Notes);
- транспортний рівень для підсистем автоматизованого митного оформлення, митної адміністративно-правової підсистеми, митної зовнішньої інформаційної підсистеми;
- можливість підключення до міжнародних обчислювальних мереж (Інтернет та ін.).

Запитання і завдання для самоконтролю

1. Поясніть, чому ЄАІС складається саме з 5 підсистем.
2. Які процеси автоматизуються кожною з підсистем ЄАІС ДМСУ?
3. Що таке митна телекомунікаційна підсистема?
4. Дайте характеристику митних підсистем ЄАІС Держмитслужби України.

Частина III

**ТЕХНОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ
ІНФОРМАЦІЙНИХ СИСТЕМ
У МИТНІЙ СПРАВІ**

Розділ 6

КЛАСИФІКАЦІЯ ТА КОДУВАННЯ ІНФОРМАЦІЇ

6.1. Вимоги до уніфікованої системи документів

Інформація, що циркулює в системі управління, об'єднується у смислові групи і фіксується на будь-якому матеріальному носії. Таке об'єднання називається документуванням, а сам носій інформації, призначений для використання в ІС, відповідно визначається як документ.

Документообіг — процес проходження документів усередині інформаційної системи: від джерела формування до використання в управлінні.

Система документообігу має надавати можливість підготовки документів, вхідного та вихідного контролю, обліку проходження документів, ведення архівів і перетворення форматів. Документи є головним засобом подання юридично оформлених відомостей про об'єкт управління, вони становлять основну частину інформаційних потоків у системі управління.

Нині функціонує уніфікована система документації (УСД), що включає 16 уніфікованих систем документації з 4500 уніфікованих форм документів (планової, звітно-статистичної, первинно-облікової, організаційно-розпорядчої, розрахунково-грошової документації та ін.). Призначення УСД полягає у сприянні виконанню основних функцій управління економікою. *Уніфікована система документації* — це комплекс

взаємопов'язаних документів, кожному з яких присвоєно код відповідно до класифікатора управлінської документації.

Під час виконання економічних завдань необхідно забезпечити їх порівнянність. Забезпечується це шляхом створення єдиних систем групувань, отриманих за єдиними класифікаційними ознаками, — Єдиної системи класифікації та кодування техніко-економічної інформації (ЄСКК ТЕІ).

Використання УСД та ЄСКК дає змогу забезпечити інформаційну, термінологічну, ідентифікаційну єдність показників і взаємозв'язок АІС різних сфер та рівнів управління.

З 1 червня 1999 р. набрав чинності державний класифікатор управлінської документації ДК 010-98.

Державний класифікатор управлінської документації (ДКУД) є складовою державної системи класифікації і кодування техніко-економічної та соціальної інформації (табл. 6.1). ДКУД розроблено у зв'язку зі змінами у складі та змісті організаційно-розпорядчої, первинно-облікової, банківської і звітно-статистичної документації внаслідок реорганізації системи державного управління в Україні.

Система документації — сукупність взаємопов'язаних документів, що застосовуються у певній сфері діяльності.

Уніфікована система документації (УСД) — це система документації, що створена за єдиними правилами та вимогами і містить інформацію, необхідну для управління у певній сфері діяльності.

Уніфікована система зовнішньоторговельної документації — це система документації, що використовується для виконання завдань зовнішньоторговельної діяльності.

Уніфікована форма документа (УФД) — це сукупність реквізитів, установлених відповідно до завдань у певній сфері діяльності та розташованих у певному порядку на носії інформації.

ДКУД є номенклатурним переліком назв уніфікованих форм документів з унікальними кодовими позначеннями. ДКУД використовується під час збирання й оброблення документів за відповідними уніфікованими формами всіма органами державного і господарського управління та підвідомчими підприємствами й організаціями в процесі виконання відповідних управлінських функцій згідно з чинним законодавством.

Класифікатор орієнтований на однозначне визначення (ідентифікацію) УФД, їх облік і систематизацію, контроль складу та змісту УФД у кожному класі документації, організацію ведення відповідних класів документації, забезпечення автоматизованого пошуку потрібних УФД. Кожному класу документації відповідає певна уніфікована система документації (УСД).

Об'єктом класифікації є безпосередньо УФД, які використовуються під час виконання управлінських функцій згідно з чинним законодавством.

ДКУД орієнтовано на забезпечення оброблення інформації із застосуванням засобів комп'ютерної техніки та прогресивних інформаційних технологій. ДКУД складається з таких класів:

- 1) організаційно-розпорядча документація (код 02);
- 2) первинно-облікова документація (код 03);
- 3) банківська документація (код 04);
- 4) фінансова документація (код 05);
- 5) звітно-статистична документація (код 06);
- 6) планова документація (код 07);
- 7) ресурсна документація (код 08);
- 8) торговельна документація (код 09);
- 9) зовнішньоторговельна документація (код 10);
- 10) цінова документація (код 13);
- 11) документація з праці, соціальних питань і соціального захисту населення (код 15);
- 12) документація з побутового обслуговування населення (код 17);
- 13) бухгалтерсько-облікова документація (код 18);
- 14) документація з Пенсійного фонду (код 20);
- 15) словниково-довідкова документація (код 21).

Ідентифікація УФД здійснюється за допомогою ієрархічної класифікації з трьома ступенями. Кодове позначення складається з семи цифрових десяткових знаків. У кодовому позначенні УФД відображено: перший та другий знаки (клас) — належність УФД до відповідної УСД; третій та четвертий знаки (підклас) — належність УФД у межах класу до відповідного підкласу; п'ятий, шостий і сьомий знаки — реєстраційний номер УФД підкласу (табл. 6.1).

Таблиця 6.1. Класифікація державної управлінської документації. Уніфікована система управлінської документації

Код	Назва	
10	ЗОВНІШНЬОТОРГОВЕЛЬНА ДОКУМЕНТАЦІЯ	
1001	Оперативно-комерційна документація	
1001101	Контракт (експорт)	КЕ
1001102	Контракт (імпорт)	КІ
1001111	Специфікація на сировинні товари та машинне устаткування	ССМУ
1001112	Специфікація на запасні частини	СЗЧ
1001113	Специфікація типового переліку запасних частин (1)	СТПЗЧ-1
1001114	Специфікація типового переліку запасних частин (2)	СТПЗЧ-2
1001121	Додаток до контракту (експорт)	КЕ дод.
1001122	Додаток до контракту (імпорт)	КІ дод.
1001131	Повідомлення про укладення контракту (експорт)	ПК-експ
1001132	Повідомлення про укладення контракту (імпорт)	ПК-імп
1001140	Замовлення-наряд	ЗН
1001200	Доручення на імпорт	ДІ
1001201	Контракт із зовнішньоекономічних операцій з давальницькою сировиною	КЗОДС
1001202	Свідоцтво про реєстрацію міжнародних торгів	СРМТ
1001203	Форма № 2-контракт “Інформація про хід виконання державного контракту уповноваженими зовнішньоторговельними організаціями (ЗТО)”	2-контракт
1002	Транспортна зовнішньоторговельна документація	
1002010	Експортне повідомлення	ЕП
1002020	Імпортне повідомлення	ІП
1002041	Коносамент	Коносамент
1002042	Таблиця № 61.10-ТР “Підсумки індексів тарифів на перевезення вантажів”	Таблиця 61.10-ТР

Закінчення табл. 6.1

Код	Назва	
1002043	Зовнішня торгівля України товарами народного споживання	ЗТ
1003	Товаросупровідна документація	
1003001	Відвантажувальна специфікація	ВС
1003002	Пакувальний лист	ПЛ
1003003	Комплектувальна відомість	КВ
1003004	Сертифікат якості	СЯ
1003005	Товаросупровідний документ	ТД
1003006	Типова форма основного товаросупровідного документа	ТФОТД
1004	Розрахункова зовнішньоторговельна документація	
1004 010	Рахунок	Р
1004 011	Специфікація до звіту	СЗ
1005	Страхова зовнішньоторговельна документація	
1005100	Типова форма страхових документів	ТФСД
1006	Ветеринарна зовнішньоторговельна документація	
1006100	Типова форма ветеринарних документів (тендерів)	ТФВД

Ведення ДКУД здійснює Державний науково-дослідний інститут інформатизації та моделювання економіки Національного агентства з питань інформатизації при Президентіві України. ДКУД актуалізується один раз на рік.

6.2. Системи класифікації та кодування

Під *класифікацією* розуміють поділ множини об'єктів на частини за їх подібністю чи розбіжністю відповідно до прийнятих методів. Є два методи класифікації: ієрархічний і фасетний.

Ієрархічний метод класифікації — це послідовний поділ множини (об'єктів) на підпорядковані класифікаційні угруповання. Множину, яка класифікується, поділяють на підпоряд-

ковані підмножини спочатку за деякою ознакою (основою поділу) великі угруповання, потім кожен з них — на низку наступних угруповань, які, у свою чергу, поділяються на дрібніші, поступово конкретизуючи об'єкт класифікації. Між цими угрупованнями встановлюються відношення підпорядкованості (ієрархії).

Фасетний метод класифікації — це паралельний поділ множини об'єктів на незалежні класифікаційні угруповання. При цьому множина об'єктів, що характеризується деяким набором однакових для всіх об'єктів ознак (фасет), значення яких відповідають конкретним виразам зазначених ознак, може поділятися багаторазово і незалежно. Такий метод класифікації однорівневий, оскільки вхідна множина об'єктів поділяється на підмножини відповідно до значень ознак окремих фасетів.

Кодування — процес створення кодів (набору цифр, букв та цифр і букв) і присвоєння їх підмножинам об'єктів, отриманих у процесі класифікації. Особливістю кодування техніко-економічної інформації є те, що коди мають відображати її структуру, ідентифікувати об'єкти й описувати зв'язки між ними. Основне завдання кодування — забезпечення ідентифікації елементів множин, що класифікуються, та їхніх класифікаційних ознак.

Розрізняють два методи кодування: *реєстраційний* і *класифікаційний*.

До реєстраційних належать порядковий і серійно-порядковий методи, а до класифікаційних — послідовний і паралельний.

Порядковий метод кодування — це створення коду з чисел натурального ряду і його присвоєння. Він є найбільш простим, повним і однозначним.

Серійно-порядковий метод кодування — це створення коду з чисел натурального ряду, закріплення окремих серій чи діапазонів цих чисел за об'єктами класифікації з однаковими ознаками його присвоєння; використовується для двознакових номенклатур.

Послідовний метод кодування — це створення коду класифікаційного групування і (чи) об'єкта класифікації з використанням кодів послідовно розміщених підпорядкованих угру-

повань, що були отримані при ієрархічному методі класифікації, та його присвоєння.

Паралельний метод кодування — це створення коду класифікаційного групування і (чи) об'єкта класифікації з використанням кодів незалежних угруповань, що були отримані за факетного методу класифікації, та його присвоєння.

Результати класифікації і кодування фіксуються в документах, що отримали назву класифікаторів. Класифікатор становить документ із систематизованим переліком назв і кодів класифікаційних угруповань або об'єктів класифікації.

Процес створення інформаційних систем для міжнародного бізнесу пов'язаний з проектуванням та розробленням різних видів забезпечень, зокрема інформаційного забезпечення.

Оскільки конкретний зміст інформаційної бази залежить від виду економічних завдань, що розв'язуються автоматизовано в межах ЄІС, зосередимо увагу на системах класифікації та кодування.

Класифікація і кодування — це дві невід'ємні частини одного процесу: переведення різноманітної інформації з природної мови на стандартизовану, тобто впорядкування й узгодження різних інформаційних повідомлень.

Результат діяльності з класифікації і кодування інформації відображається у класифікаторі відповідного рівня, якому після прийняття і затвердження надається статус нормативно-технічного документа з обов'язковим застосуванням усіма учасниками інформаційного процесу обміну різноманітними даними. Прикладом міжнародного класифікатора може бути Товарна номенклатура зовнішньоекономічної діяльності.

Нові міждержавні класифікатори. Чинним законодавством України встановлено, що вантажі переміщуються через митний кордон України під митним контролем і підлягають обов'язковому декларуванню митними органами, які проводять митний контроль і оформлення таких вантажів. Декларування здійснюється шляхом заяви за встановленою формою точних даних про мету переміщення через митний кордон України товарів та інших предметів і про самі товари і предмети, а також інших відомостей, які необхідні для митного оформлення. Уніфікованим документом, який містить необхідні відомості про товари та інші предмети, які переміщують-

ся через митний кордон України в рамках експортно-імпортних операцій, є вантажна митна декларація.

Під час заповнення ВМД та ведення митної статистики зовнішньої торгівлі, а також для спрощення процедур обміну відповідною інформацією на міжнародному рівні в Україні з 1 березня 1995 р. (наказ Державного митного комітету України від 16 лютого 1995 р. № 57) застосовуються класифікатори (дод. 2, табл. 2—9), розроблені на основі міжнародних документів.

Запитання і завдання для самоконтролю

1. Дайте визначення документообігу.
2. Для чого потрібен державний класифікатор управлінської документації?
3. Розкрийте поняття уніфікованої системи документації, уніфікованої системи зовнішньоторговельної документації та уніфікованої форми документа.
4. Які класи містить ДКУД?
5. Для чого необхідні системи класифікації та кодування?
6. Які є методи класифікації?
7. Які методи кодування ви знаєте?
8. Яке призначення нових міжнародних класифікаторів?

Розділ 7

ЕЛЕКТРОННИЙ ОБМІН ІНФОРМАЦІЄЮ

7.1. Міжнародні стандарти електронного обміну даними

Електронний обмін даними — це міжкомп'ютерний обмін діловими, комерційними та фінансовими електронними документами, наприклад, замовленнями, платіжними інструкціями, контрактними пропозиціями, накладними, квитанціями.

Такий обмін даними забезпечує оперативну взаємодію торговельних партнерів (клієнтів, постачальників, торговельних посередників, експедиторів та ін.) на всіх етапах підготовки торговельної угоди, укладення контракту і реалізації постачання.

На етапі оплати контракту і переказу грошових коштів електронний обмін даними для комерційних цілей може взаємодіяти зі службою електронного обміну фінансовими документами. Така взаємодія створює для покупців (клієнтів) ефективне середовище під час виконання всіх торговельно-платіжних операцій, а саме:

- он-лайн-перегляд каталогів торговельних пропозицій, товарів і послуг на ринку;
- вибір в інтерактивному режимі потрібного товару/послуги, уточнення умов (вартості й термінів постачання, торговельних знижок, гарантійних і сервісних зобов'язань);

- он-лайн-замовлення товару/послуги або запит контрактної пропозиції, погодження й укладення контракту;
- оперативний контроль постачання товару;
- одержання за допомогою електронної пошти супровідних документів (накладних, фактур, комплектуючих відомостей та ін.);
- підтвердження завершення постачання товару/послуги, виставлення й оплата рахунків;
- виконання банківсько-кредитних і платіжних операцій.

Виконуючи ці операції, користувачі служби електронного обміну даними мають використовувати відповідне телекомунікаційне обладнання, програмне забезпечення та канали зв'язку.

Історія виникнення і розвитку електронного обміну даними починається у 60-х роках, коли несумісність окремих фірмових технологій обробки комерційних даних не давала змоги інтегрувати їх в єдину систему, яка б забезпечила комплексну автоматизацію міжнародних торговельних операцій.

Так, якщо дві компанії використовують національні стандарти для подання електронних документів, то під час обміну інформацією їм буде потрібне подвійне перетворення форматів повідомлень (рис. 7.1).

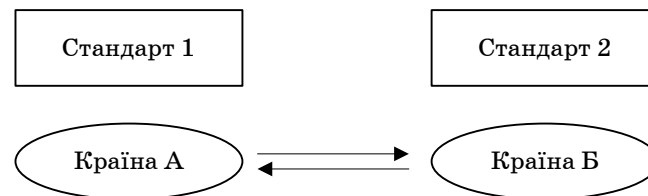


Рис. 7.1. Схема перетворення форматів для двох підприємств у різних країнах

У разі збільшення кількості партнерів, які беруть участь в інформаційній взаємодії, кількість перетворень зростає згідно з формулою

$$C = N (N - 1),$$

де C — кількість необхідних перетворень під час використання різних стандартів партнерами;

N — кількість партнерів, які беруть участь в інформаційній взаємодії.

Міжнародний стандарт електронного обміну даними для адміністрації, торгівлі і транспорту (EDIFACT)

У 1983—1985 рр. міжнародні організації ООН (UN/ECE та ISO) почали розробку процедур, форматів даних і міжнародних кодових систем для електронного обміну даними. У 1988 р. оприлюднено першу версію міжнародного стандарту United National Electronic Data Interchange for Administration, Commerce and Transport — UN/EDIFACT (ООН / Електронний обмін даними для адміністрації, торгівлі і транспорту).

В EDIFACT виокремлено чотири основні компоненти, які підлягають стандартизації під час підготовки документів для передачі каналами телекомунікацій:

- 1) елементи даних (data elements);
- 2) стандартні групи елементів даних (standard data segments);
- 3) стандартні повідомлення (standard message);
- 4) правила створення форматів документів (syntax rules).

Таким чином, розроблено набір синтаксичних правил і комерційних елементів, який отримав назву EDIFACT і був оформлений у вигляді двох стандартів ISO:

ISO 7372 — *Trade Data Elements Directory* (Довідник комерційних елементів даних);

ISO 9735 — *Application Level Syntax Rules* (Правила синтаксису на рівні користувача).

Стандарти EDIFACT розроблялись для глобальних комп'ютерних мереж з широким колом користувачів: державних установ, виробників товарів, виробів і послуг, дистриб'юторів, брокерів, транспортних експедиторів, банків, страхових компаній та ін. По суті вони є універсальною мовою електронного спілкування на міжнародному рівні, тобто лінгвістичним забезпеченням для інформаційних систем у міжнародному бізнесі.

Головними цілями створення і використання EDIFACT визнано:

- визначення стандартних щодо синтаксису і семантики повідомлень, які відповідають міжнародним стандартам;
- заміну звичайних паперових форм і документів електронними документами та відповідними методами їх обробки;
- прискорення документообігу і відповідно оперативності обробки комерційних і фінансових трансакцій;
- створення для малих, середніх і великих фірм більш сприятливих і рівних умов ринкової конкуренції;
- покращання умов для підготовки і здійснення торговельних угод;
- більш широке та масове використання клієнтами сучасних комп'ютерних мереж і послуг.

На базі стандарту EDIFACT інтенсивно розвивається інфраструктура електронного обміну даними. Інформаційні й телекомунікаційні системи забезпечують для своїх користувачів комплекс послуг з обробки і видачі довідкових даних, комерційних звітів, замовлень і торговельних пропозицій, розрахунків і платіжних квитанцій.

Усі ці послуги надаються як прикладні служби, які створюються технологіями електронного обміну даними. На сучасному етапі розрізняють такі основні види прикладних служб.

1. *Онлайнові бази даних* — бази даних, які доступні в оперативному режимі з терміналів користувачів. Онлайнові бази даних цілодобово відкриті для діалогового пошуку інформації і видачі довідок та різних статистичних звітів. Користувачами онлайнових баз даних можуть бути спеціалісти комерційних і фінансових організацій, економісти, дилери, постачальники, агенти фінансових і торговельних організацій.

2. *Електронна пошта* — система обміну й обробки повідомлень (сукупність електронних поштових скриньок, програмних засобів обробки, збереження і передачі повідомлень, термінальних станцій для підготовки і виведення повідомлень). Користувачі електронної пошти можуть проводити міжперсональний обмін повідомленнями, розсилання повідомлення за списками адрес, зажадати свої повідомлення з поштових скриньок, організувати проблемні телеконференції і виконувати інші функції обробки повідомлень (електронних документів).

3. *Електронна передача грошових коштів (EFT — Electronic Funds Transfer)* — система передачі фінансових (кредитних, платіжних) документів між клієнтами і банками, між банками, між банками та іншими фінансовими і комерційними організаціями. Міжнародна мережа обміну фінансовою інформацією SWIFT забезпечує багато функцій EFT.

4. *Електронний обмін даними (EDI — Electronic Data Interchange)* — багатоцільова система обміну документами, які мають розвинуту структуру даних. Як правило, реалізується на базі стандартних програмних і технічних засобів електронної пошти.

5. *Керівні мережні служби (Managed Network Services)* виконують різні виробничі, адміністративні та службові функції управління об'єктами, технологічними лініями, транспортними системами і службовцями підприємств. Реалізуються на базі внутрішньофірмових мереж ЕОМ, розподілених між підрозділами фірми.

6. *Телеметричні служби* — система оперативного спостереження, дистанційного виміру і контролю за нерухомими та рухомими об'єктами.

Бізнесмени, торговельні агенти, транспортні службовці, банківські спеціалісти, адміністратори, економісти і бухгалтери переважно використовують перші чотири служби електронного обміну даними.

На сучасному етапі електронний обмін даними діє або впроваджується практично в усіх країнах. Міжнародний статус стандарту EDIFACT спонукає до того, що його використання є обов'язковою умовою адекватного обміну даними із закордонними партнерами для всіх без винятку підприємств і організацій України, які здійснюють зовнішньоекономічну діяльність.

Міжнародний стандарт відкритої торгівлі через Інтернет (OBI)

Стандарт OBI (Open Buying on Internet) — це відкритий гнучкий стандарт для вирішення питань ділової співпраці за допомогою Інтернету. Початковою метою під час створення OBI була автоматизація великих за обсягом, але незначних за

вартістю угод між торговельними партнерами, які становлять близько 80 % усіх операцій приватних фірм.

За розвитком стандартів ОВІ наглядає ОВІ-консорціум, використовуючи групу розвитку. Участь у консорціумі та групі розвитку відкрита для торговельних і збутових організацій, технологічних компаній, фінансових інституцій, інших зацікавлених осіб на основі щорічної плати.

Мета роботи над ОВІ — впровадження стандартної моделі для безпечного та інтерактивного проведення операцій для інтернет-комерції.

У рамках стандарту ОВІ виокремлюються чотири сторони: особа, що формує запит, продавець, покупець, центр платежу (банк). Архітектура ОВІ передбачає, що замовник за допомогою web-браузера взаємодіє зі спеціалізованим каталогом продавців. Якщо замовник розміщує замовлення, то продавець відсилає запит, що потребує підтвердження замовником та/або додаткової інформації. Замовник має можливість погодитися із запитом або відкинути його, можливий варіант перероблення або зміни цього запиту, який у формі завершеного повідомлення надсилається продавцю.

Технічна специфікація стандарту ОВІ (версія 2.1) фокусує свою увагу на тих аспектах розглянутого вище процесу, які є найважливішими для інтерактивної взаємодії торговельних партнерів:

- 1) стандартна процедура доступу до спеціалізованих каталогів продавця;
- 2) стандартний формат інформації, якою обмінюються партнери;
- 3) стандартні методи передачі інформації між організаціями і стандартні механізми захисту інформації, авторизації доступу та підтвердження згоди.

Міжнародний стандарт електронного обміну даними EANCOM

Стандарт EANCOM є практичним підстандартом стандарту UN/EDIFACT і нині вже прийнятий як національний і міжнародний майже в 50 країнах світу.

Характерна особливість EANCOM у тому, що він є однією зі складових всеохопного пакета міжнародних стандартів для

ідентифікації товарів, послуг і розташування, автоматизованої ідентифікації на основі штрихових кодів та електронного обміну даними EAN (Electronic Data Interchange), у комбінації з якими забезпечує засоби для побудови ефективної системи створення, передачі й обробки інформації на основі автоматизованої ідентифікації (рис. 7.2).

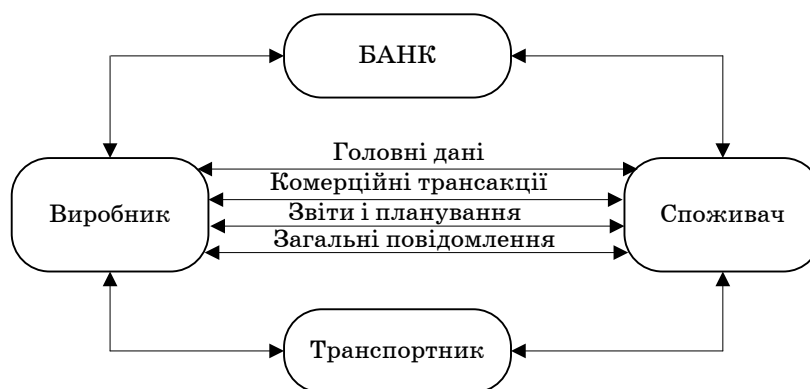


Рис. 7.2. Схема використання стандарту EANCOM

Стандарт EANCOM доступний для організацій будь-яких розмірів, необхідно лише мати комп'ютер, телефонну лінію, модем і конвертор (спеціальне програмне забезпечення).

Електронний обмін даними в найближчому майбутньому, очевидно, стане єдиною можливою формою господарської діяльності, оскільки участь і конкурентоспроможність на ринку буде неможливою без автоматизованого подання інформації і негайної відповіді на потреби клієнтів.

7.2. Міжнародні стандарти систем обробки повідомлень (електронної пошти)

Загальна характеристика електронної пошти

Із середини 70-х років комп'ютерні системи почали використовуватися як середовище для зв'язку між людьми. Попередниками сучасних систем обробки повідомлень і комп'ютерних систем телеконференцій були мережі типу ARPANET та Електронна інформаційна система обміну, які забезпечували обмін текстовою інформацією між людьми у межах локальної модемної структури. З часом з'явилась необхідність взаємодії із зовнішніми системами обробки повідомлень.

Перші спроби показали, що для індивідуальних систем цю проблему можна вирішити за допомогою шлюзів. Проте велика різноманітність систем обробки потребувала створення великої кількості шлюзів. Тому постало питання кардинального розв'язання цієї проблеми шляхом розробки універсальних стандартів для комп'ютерних систем опрацювання повідомлень. Роботи в цьому напрямі розпочато в 1979 р. Міжнародною федерацією обробки інформації (IFIP) і підтримано Міжнародною координаційною комісією з телеграфії і телефонії (МККТТ) та паралельно Міжнародною організацією зі стандартизації (МОО).

Системи транспортування повідомлень між людьми за допомогою комп'ютерів називають електронною поштою. Далі будемо враховувати, що термін "електронна пошта" (ЕП) належить до прикладного рівня систем обробки повідомлень. В електронній пошті транспортна служба має справу з файлами, які обробляються комп'ютерами, а не з паперами, які транспортуються за допомогою різних технічних засобів (машин, потягів, літаків), як це відбувається в класичних поштових системах. Тому електронну пошту визначили як службу поштового зв'язку, в якій доставка повідомлень здійснюється електронними методами за допомогою комп'ютерів.

Для користувачів електронна пошта — цілком нова служба зв'язку, яка забезпечує більш надійне та якісне обслуговування порівняно зі звичайною поштовою службою.

У контексті проблем систем обробки повідомлень можна виокремити три групи завдань: *транспортування, переприймання й адресацію*.

Однією з головних особливостей більшості систем обробки повідомлень (СОП) є асинхронна природа зв'язку між користувачами. Ця особливість забезпечує низку переваг:

- *асинхронний зв'язок не потребує присутності учасників*. Це дуже важливо для користувачів, які перебувають у різних часових поясах, коли зв'язок за допомогою телефону неможливий або незручний;

- з технічного погляду *асинхронна передача дає змогу використовувати принцип комутації повідомлень (КП) до найвищих протокольних рівнів семирівневої моделі*. Переваги методу комутації повідомлень — високий ступінь використання ресурсів і можливість перетворення форматів, кодів та ін. Ці властивості дають змогу забезпечити функціонування систем опрацювання повідомлень за високого рівня неоднорідності систем на нижніх рівнях протоколів.

Другою особливістю систем опрацювання повідомлень є можливість ефективних двосторонніх (1 : 1) і багатосторонніх (1 : N, N : N) зв'язків. Передача повідомлень одночасно до багатьох користувачів забезпечується за допомогою спеціальних механізмів — формування адреси на конверті або служби розподільних листів.

Третя важлива особливість полягає в тому, що система опрацювання даних — це одна з головних складових системи автоматизації установ, яка забезпечує обмін повідомленнями, що генеруються, обробляються, передаються, приймаються та архівуються за допомогою електронних систем.

Описуючи системи опрацювання даних, використовують базові терміни. Враховуючи специфічну функцію, розглянемо більш докладно поняття шлюз.

Шлюз — це устаткування, необхідне для з'єднання двох мереж, що помітне їх користувачам (на відміну від мосту, наявність якого, як правило, непомітна). Введення шлюзу доцільне, коли необхідно врахувати одну або декілька перелічених нижче розбіжностей між мережами, які він з'єднує.

- Відмінність адресації. Якщо адресація в мережах, що з'єднуються, визначається різними організаціями, тоді шлюз може бути потрібним для перетворення адрес повідомлень, які через нього проходять.

- Відмінність способів оплати. Якщо в мережах, що з'єднуються, реалізовано різні способи оплати (наприклад, локальна мережа, в якій оплата не проводиться, може з'єднуватися з глобальною мережею, в якій оплачується передача кожного пакета), тоді шлюз може використовуватись для перевірки повноважень користувачів та обліку використання ресурсів.

- Відмінність протоколів. Якщо в мережах реалізовано різні протоколи, тоді в шлюзі можна здійснити необхідні перетворення протоколів (якщо це можливо) або запобігти спробам користувача однієї мережі скористатись засобами, які недоступні в другій мережі, і видати відповідні повідомлення.

Розрізняють три типи шлюзів, що становлять систему для з'єднання різнорідних мереж.

1. *Адресний шлюз* з'єднує мережі з різними просторами адрес/імен. Зазвичай такі шлюзи використовуються між мережами з однаковими протоколами нижніх рівнів (починаючи з транспортного), але з різними правилами адресації та присвоєння імен.

2. *Протокольний шлюз*, з'єднуючи мережі з різними протоколами на всіх рівнях, забезпечує перетворення сервісних елементів однієї мережі в сервісні елементи другої. Елементи, які не можуть бути перетворені, ігноруються.

3. *Шлюз форматів* забезпечує перетворення форматів різних стандартів систем електронної пошти, первинних кодів (ASCII, EBDIC) тощо. Вони мають бути повністю прозорими для користувачів.

У деяких випадках шлюзи підтримують комбінацію перелічених вище служб.

Інші терміни стосуються питань, пов'язаних з адресацією.

Ім'я (ідентифікатор) однозначно визначає ресурс (хто, що), який належить до специфічної системи координат, що формується певним простором імен. Наприклад, ім'я користувача "Коваленко" однозначно ідентифікує персону, яка пов'язана з простором імен у певній обчислювальній системі.

Простір імен може бути плоским або ієрархічним. *Плоский простір імен* потребує наявності центральної системи для того, щоб уникнути конфліктів під час використання імен, тоді як в *ієрархічному іменному просторі* управління може бути розподіленим. Ієрархічний простір імен можна використовувати для відображення організаційної або топологічної структури систем.

Адреса визначає місце розташування ресурсу (де) у деякій системі координат, що формується певним адресним простором. Аналогічно до простору імен адресний простір може бути плоским або ієрархічним.

Шлях указує на те, як знайти ресурс. У системі обробки повідомлень використовуються два різних методи маршрутизації:

- *маршрутизація від джерела* — відправник визначає весь шлях проходження повідомлення від одержувача (при цьому він використовує інформацію про структуру мережі та лінії між вузлами);

- *внутрішня маршрутизація* — відправник не визначає маршрут доставки повідомлення одержувачу. Разом з тим має діяти система відображення “адресного маршруту”, для того щоб у кожному проміжному вузлі шлях до наступного вузла визначався автоматично.

Міжнародний стандарт електронної пошти X.400

Стандарт X.400 становить набір рекомендацій щодо побудови системи передачі електронних повідомлень, яка не залежить від операційних систем та апаратних засобів, що використовуються. Рекомендації X.400 — це результат діяльності Міжнародного комітету із засобів телекомунікації (СІТТ у французькій транскрипції або ІТУ в англійській), створеного при Організації Об’єднаних Націй. Вони охоплюють усі аспекти побудови середовища управління повідомленнями: термінологію, компоненти і схеми їхньої взаємодії, протоколи керування та передачі, формати повідомлень і правила їхнього перетворення. У рекомендаціях X.400 найбільш повно відображається накопичений в індустрії комп’ютерів і телекомунікацій досвід створення та застосування інформаційних систем.

На сьогодні є три редакції рекомендацій:

- рекомендації 1984 р., відомі як “Червона книга” (Red Book);
- рекомендації 1988 р., відомі під назвою “Блакитна книга” (Blue Book);
- рекомендації 1992 р., відомі як “Біла книга” (White Book).

Рекомендації, надані пізніше, описують додаткові протоколи і формати передачі даних, коригують неточності або змінюють трактування більш ранніх. Виправлення і доповнення до зазначених специфікацій випускаються щорічно, однак наявні системи переважно підтримують рекомендації 1984 і/чи 1988 рр. На жаль, ці специфікації не є вільно доступними і поширюються за досить високу плату.

Рекомендації X.400 спираються на семирівневу модель і родину протоколів *OSI (Open System Interconnect)* Міжнародної організації зі стандартів (*ISO*) (рис. 7.3). Відповідно до цієї моделі кожний з рівнів використовує сервіси тільки того рівня, що знаходиться безпосередньо під ним, і надає сервіси тільки тому рівню, що знаходиться безпосередньо над ним. Це забезпечує системам, побудованим на основі такої моделі, високий ступінь незалежності від середовища передачі даних. Оскільки рекомендації X.400 визначають набір специфікацій для найвищого рівня (Application), то додатки, що відповідають цим рекомендаціям, мають вільно взаємодіяти один з одним незалежно від операційних систем, апаратури і мережних протоколів.

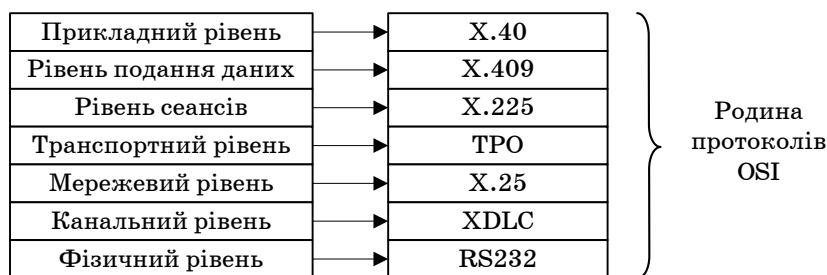


Рис. 7.3. Семирівнева модель OSI та приклади протоколів, що відповідають кожному рівню

Нижні чотири рівні — від фізичного до транспортного — відповідають за організацію середовища передачі даних. Реалізуються частково на апаратному рівні або як сервіси-послуги ядра операційної системи. Верхні три рівні призначені для використання операційною системою і прикладними програмами.

Для поділу вхідного потоку даних між додатками на кожному з рівнів — транспортному (*Transport*), сеансовому (*Session*) та подання (*Presentation*) — використовується механізм так званих точок доступу (*access point*). Кожна така точка має унікальний ідентифікатор чи селектор (*selector*), що може бути або символьним рядком, або послідовністю шістнадцяткових цифр. Довжина селектора транспортного рівня — 32 символи (64 цифри), рівня сеансів — 16 символів (32 цифри), а рівня подання даних — 8 символів (16 цифр). Щоб два додатки в мережі могли взаємодіяти, кожен з них має знати набір селекторів іншого.

Розглянемо, як у термінах X.400 визначаються компоненти системи передачі електронних повідомлень. На рис. 7.4 наведено схему побудови середовища управління повідомленнями (*Messaging Handling Environment* — *MHE*).

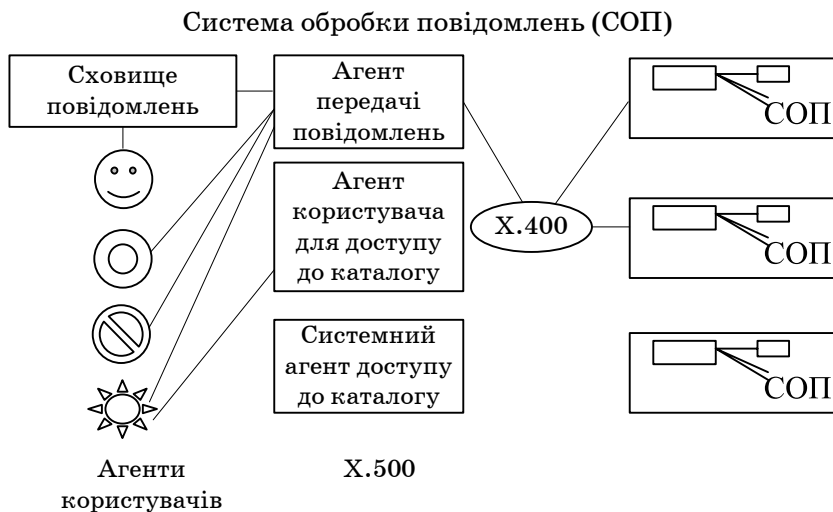


Рис. 7.4. Схема побудови середовища управління повідомленнями

Ця схема класична і в її термінах можуть бути описані структура і принципи функціонування будь-якої наявної поштової системи на будь-якій платформі. Як видно з ілюстрації, середовище управління повідомленнями — це об'єднання систем управління повідомленнями (*Messaging Handling Systems* — *MHS*), що можуть бути довільно пов'язані між собою за допомогою шлюзів або публічних інформаційних мереж. Кожна з систем управління повідомленнями, у свою чергу, складається з таких компонентів:

- *агент користувача (АК) (User Agent — UA)* — підсистема, що є клієнтом у процесі обміну поштовими повідомленнями; клієнт, у свою чергу, може бути як реальним користувачем, так і процесом, що використовує сервісні послуги електронної пошти;

- *агенти передачі повідомлень (АПП) (Message Transfer Agent — MTA)* — підсистема, до обов'язків якої входить обмін повідомленнями з агентами користувачів і/або зовнішніми та локальними агентами передачі повідомлень. Слід зазначити, що кожен агент передачі повідомлень може мати ім'я і пароль доступу;

- *системи передачі повідомлень (СПП) (Message Transfer System — MTS)* — підсистема, що складається з одного чи декількох *MTA* і виконує функції приймання, доставки і проміжного збереження повідомлень;

- *сховища повідомлень (СП) (Message Store — MS)* — підсистема, до функцій якої входять відсилання, приймання і збереження повідомлень від агентів користувачів та агентів передачі повідомлень; у складі *MHS* може бути більше одного сховища.

З усієї різноманітності описаних у рекомендаціях X.400 способів взаємодії між агентом користувача, агентом передачі повідомлень та системою передачі повідомлень розглянемо такі.

- *Відправлення повідомлення агентом користувача через сховище.* Користувач, використовуючи свого агента (АК), розміщує повідомлення, призначене для доставки іншому користувачу, безпосередньо у сховище повідомлень; звідти воно ви-

бирається локальним агентом передачі повідомлень і передається далі.

- *Відправлення повідомлення агентом користувача через агента передачі повідомлень.* Повідомлення передається прямо від агента користувача до агента передачі повідомлень і далі доставляється його засобами.

- *Одержання повідомлення агентом користувача зі сховища.* Агент передачі повідомлень здійснює доставку повідомлення у сховище (поштова скринька користувача) для подальшої обробки агентом користувача.

- *Одержання повідомлення агентом користувача від агента передачі повідомлень.* Агент користувача не має безпосереднього доступу до сховища, а для одержання повідомлень звертається до агента передачі.

Кожна з нині відомих поштових систем використовує один з перелічених способів відправлення і приймання повідомлень.

Додатково до складу систем обробки повідомлень можуть входити такі компоненти, що не є специфічними для X.400 і визначені в окремій специфікації X.500:

- *агент користувача для доступу до каталогу (АКДК) (Directory User Agent — DUA)* — підсистема, що є клієнтом при доступі до каталогу;

- *системний агент доступу до каталогу (САДК) (Directory System Agent — DSA)* — підсистема, яка є частиною каталогу і надає доступ до АКДК інформації, що зберігається в ньому, локальним і зовнішнім АКДК та САДК.

Не менш важливими компонентами специфікації X.400 є такі компоненти (рис. 7.5):

- *списки розсилання (CP) (Distribution Lists — DL)*, що містять перелік членів, кожний з яких може бути або користувачем системи управління повідомленнями, або іншим списком розсилання. Відправлене на адресу списку розсилання повідомлення буде доставлено всім його членам, включаючи вкладені списки користувачів;

- *блок доступу (БД) (Access Units — AU)*, більш відомий як шлюз (Gateway), — пристрій, що забезпечує сполучення із зовнішнім середовищем передачі даних, наприклад, з телексом чи телетайпом;

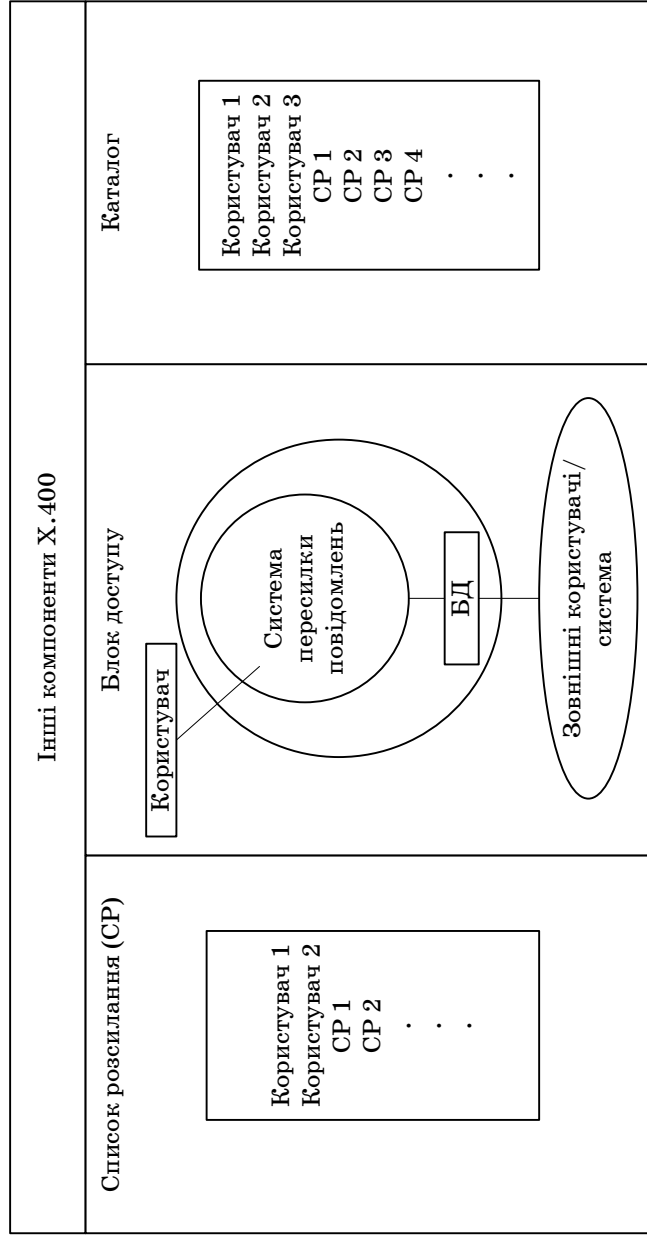


Рис. 7.5. Додаткові компоненти середовища управління повідомленнями

— *каталог (K) (Directory)*, призначенням якого є збереження інформації про об'єкти, що входять до складу системи управління повідомленнями. Поняття каталогу введено вперше у 1988 р. і реалізація цієї частини в системі X.400 не обов'язкова.

Структура електронної пошти X.400

Розглянемо ще одне базове поняття — *поштове повідомлення* і його складові. Для опису формату повідомлення в рекомендаціях X.400 прийнято парадигму *конверта (envelope)* і *змісту (content)*, характерну для традиційних поштових систем. Конверт містить вичерпну інформацію про те, куди і кому має бути доставлено листа, зворотну адресу відправника і позначку про терміновість доставки. При цьому системі не потрібно знати зміст листа. На основі інформації, зазначеної на конверті, середовище доставки виконує необхідну маршрутизацію і передачу з можливим проміжним збереженням (*store and forward*). Роль перевалочних пунктів і засобів транспортування виконують агенти передачі повідомлень. Конверт може мати спеціальну позначку про необхідність установки на ньому електронного “штампа” (*trace information*) кожним агентом передачі повідомлень, через який проходить повідомлення на шляху до адресата. Це, зокрема, дає змогу системі автоматично відстежувати виникнення поштових петель. Формат конверта X.400 визначає специфікація Р1, що є загальною для рекомендацій 1984 і 1988 рр. Формат *змісту* визначається його функціональним навантаженням. Оскільки основною функцією систем передачі повідомлень є передача повідомлень між людьми (персонами), для цього є спеціальний тип змісту, що має назву міжперсонального повідомлення (*МПП*) (*Interpersonal Message — IPM*). Міжперсональне повідомлення — це складний об'єкт. На рис. 7.6 наведено схему, що пояснює структуру електронного листа і міжперсонального повідомлення.

Міжперсональне повідомлення складається із заголовка (*header*) і тіла (*body*). Заголовок зазвичай містить копію інформації, зазначеної на конверті, і копію додаткових полів, що визначають розширені властивості повідомлення. Тіло може бути складним і включати різні типи інформації, такі як плоский текст, графіка, документи різних форматів, вкладення повідом-

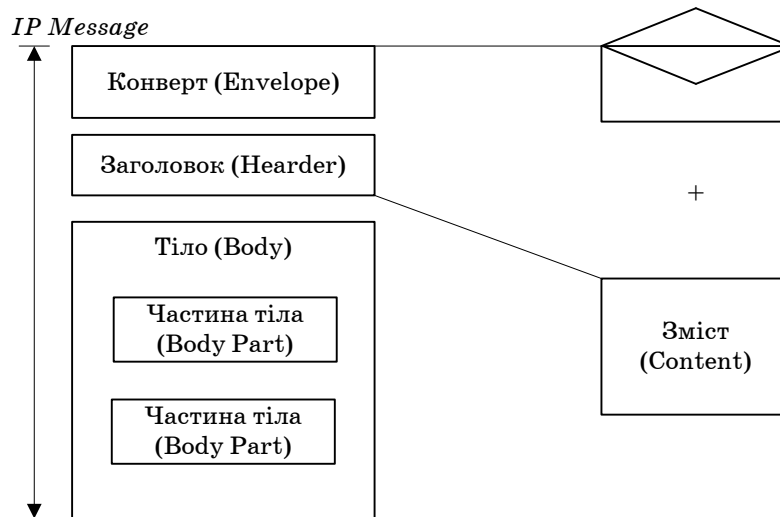


Рис. 7.6. Структура повідомлення X.400

лення тощо. Окремі частини повідомлення іменуються як *body parts*. Зараз використовуються два формати міжперсонального повідомлення, що розрізняються набором типів даних та правил кодування тексту, який містить символи національних алфавітів: P2, що використовується в системах X.400 1984 р., та P22, що використовується в системах X.400 1988 р. Ці формати сумісні знизу догори, тобто системи 1988 р. можуть працювати зі змістом як у форматі P2, так і P22.

Ще один тип змісту повідомлень X.400 — це міжперсональна нотифікація (МПН; Interpersonal Notification). Вона використовується для автоматичного повідомлення відправника про факт доставки і/або прочитання надісланого ним повідомлення. Міжперсональна нотифікація — це плоский текст довільного змісту у форматі US-ASCII, інші типи змісту несуть службове навантаження і використовуються виключно для взаємодії систем.

Архітектура X.400-систем

Рекомендації Міжнародної координаційної комісії з телеграфії і телефонії (МККТТ) X.400 визначають структуру функ-

ціональної моделі системи обробки повідомлень, описують основні співвідношення між її компонентами, служби і протоколи. Модель має багат шарову структуру. На рис. 7.7 подано модель системи обробки повідомлень, яка відповідає рекомендаціям МККТТ Х.400 (1984 р.). Внутрішня частина системи, яка отримала назву системи пересилання повідомлень (СПП), складається з вузлів — агентів пересилання повідомлень (АПП).

Наступний шар складається із систем, які одержали назву агентів користувачів (АК). Ці системи є сполучним процесом між користувачем і системою обробки повідомлень. Вони виконують функції введення повідомлення від відправника в таку систему, а далі його доставку користувачеві, а також ряд функцій, пов'язаних з обробкою повідомлень. Сукупність шарів агентів пересилання повідомлень і агентів користувачів становить систему обробки повідомлень (СОП).

Зовнішній шар системи обробки повідомлень утворюється самими користувачами (К), які застосовують цю систему для обміну повідомленнями.

У рекомендаціях МККТТ Х.400 1988 р. попередню модель розширено, і в складі системи обробки повідомлень з'явилися нові об'єкти — блоки доступу для так званих непрямих користувачів у сховище повідомлень. Модель 1988 р. наведено на рис. 7.8.

Непрямі користувачі зазвичай входять до складу інших телематичних служб (телекс, телетекс, факс та ін.). За допомогою блоків доступу (БД) ці користувачі тепер отримують доступ до системи обробки повідомлень. Спеціальний блок БД — блок доступу фізичної доставки (БДФД) — установлює зв'язок системи обробки повідомлень з традиційною системою поштового зв'язку. Рекомендації МККТТ Х.400 1988 р., визначаючи перехід від системи обробки повідомлень до класичної поштової служби, враховують специфічні види поштового сервісу, такі як рекомендовані листи, спеціальні режими доставки тощо. Перехід від електронної системи обробки повідомлень до поштової системи здійснюється шляхом одержання твердої копії повідомлення.

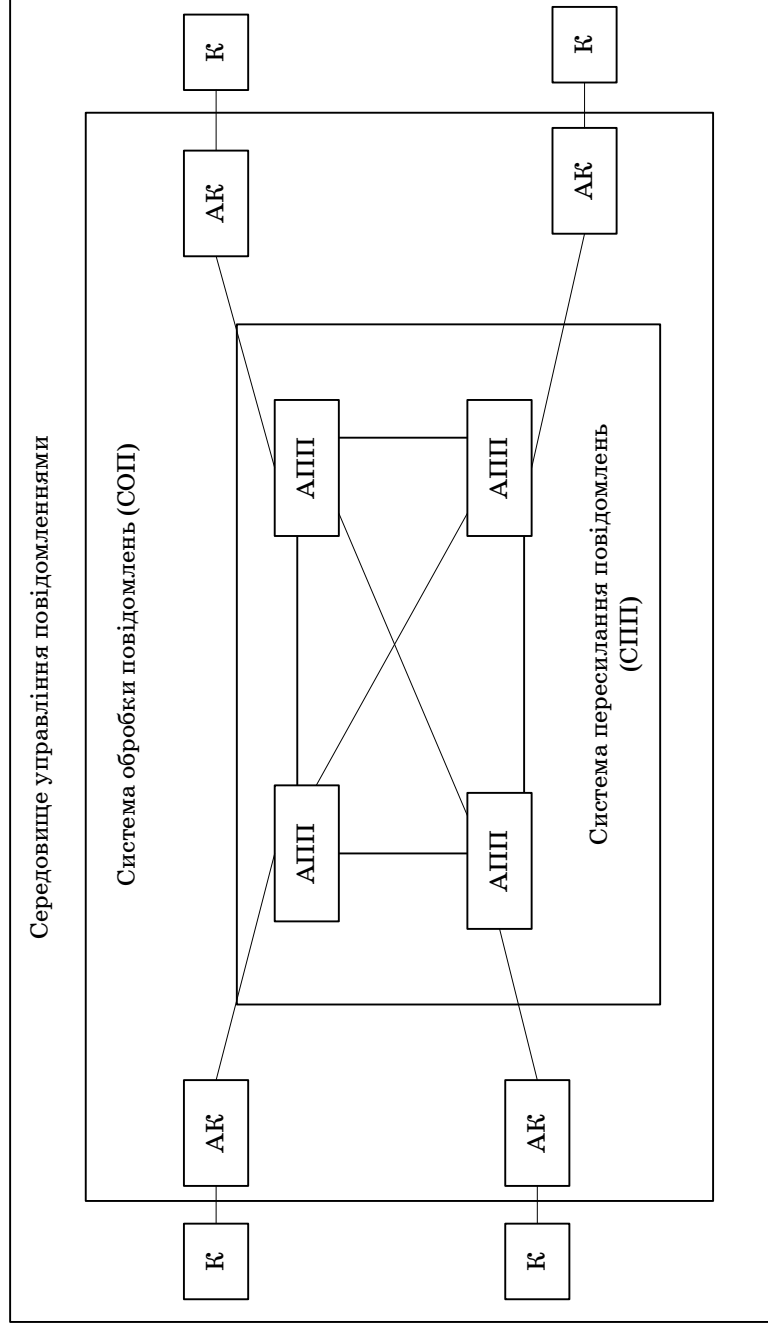


Рис. 7.7. Модель системи обробки повідомлень відповідно до рекомендацій МКСТТ Х.400 (1984 р.)

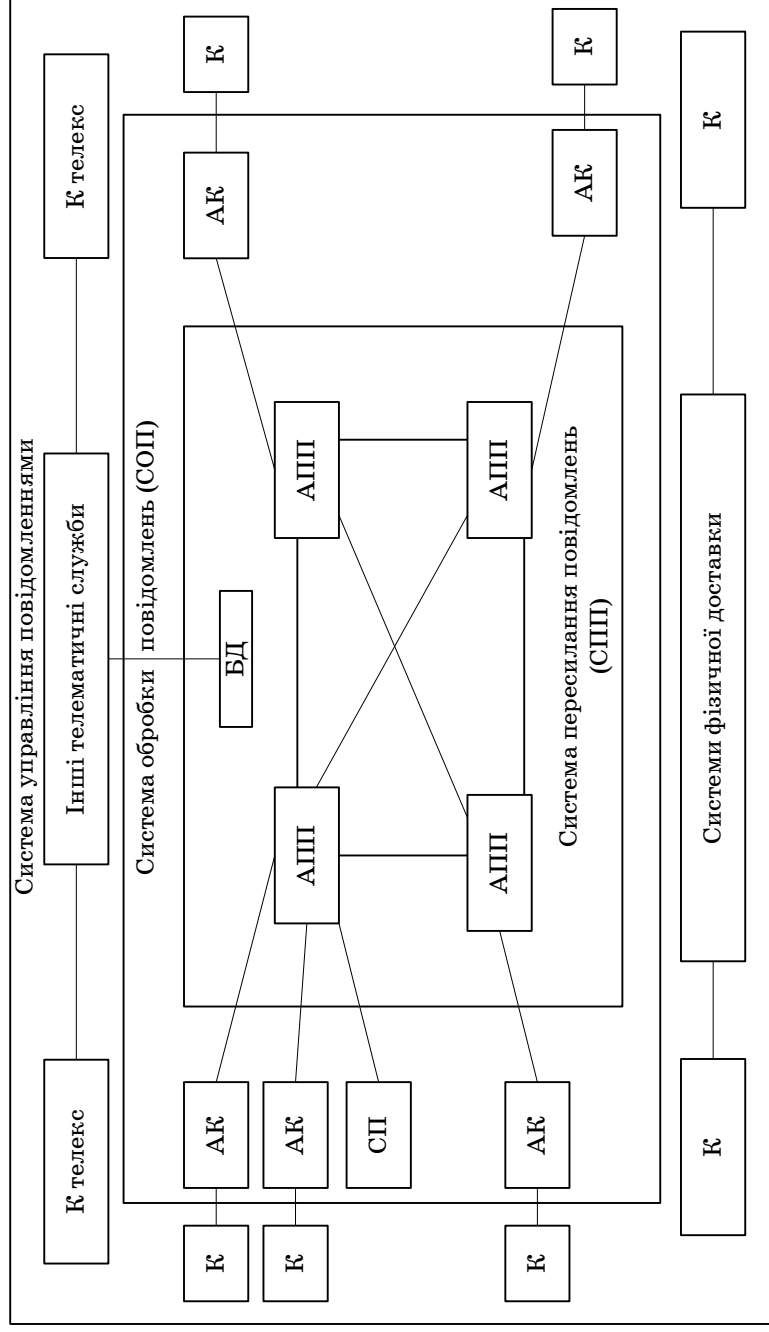


Рис. 7.8. Модель системи обробки повідомлень відповідно до рекомендацій МЄКТТ X.400 (1988 р.)

Особливу роль для користувача мають сховища повідомлень (СП). Ураховуючи те, що персональний комп'ютер широко використовується користувачами як робоча станція, має обмежену пам'ять, а також те, що він може використовуватись для реалізації агента користувача або агента пересилання повідомлень, виникає необхідність у створенні буферних накопичувачів достатньої місткості, роль яких відіграють сховища повідомлень.

Схеми фізичної реалізації електронної пошти X.400

Багатошарова модель не містить жодних припущень про спосіб фізичної реалізації різних об'єктів систем обробки повідомлень.

На рис. 7.9, а відображено варіант реалізації агента пересилання повідомлень і двох агентів користувачів в одному комп'ютері. У цьому разі користувачі можуть застосовувати дуже прості термінали, які мають тільки клавіатуру і дисплей.

На рис. 7.9, б наведено систему обробки повідомлень для двох комп'ютерів, які розподіляють функції цієї системи. У першій частині знову агенти користувачів і агенти пересилання повідомлень суміщені в одному комп'ютері, що дає змогу користувачу застосовувати простий термінал. Ліворуч система містить агента пересилання повідомлень і одне або декілька сховищ повідомлень. У цьому разі функції агента користувача будуть реалізовані в терміналі користувача (ТК), який має виконувати функції обробки повідомлень. Для реалізації цих функцій необхідно використовувати персональний комп'ютер (ПК).

На рис. 7.9, в відображено варіант системи обробки повідомлень, коли комп'ютерна система лівої частини системи обробки повідомлень реалізує тільки функції агента користувача (можливо, більше одного). Система у правій частині містить усі компоненти системи обробки повідомлень: агент пересилання повідомлень, сховище повідомлень і агент користувача. Такий варіант дає можливість підключити до системи обробки повідомлень різні класи терміналів.

Наведені на рис. 7.9 варіанти не охоплюють усі можливі конфігурації систем обробки повідомлень. Відображені струк-

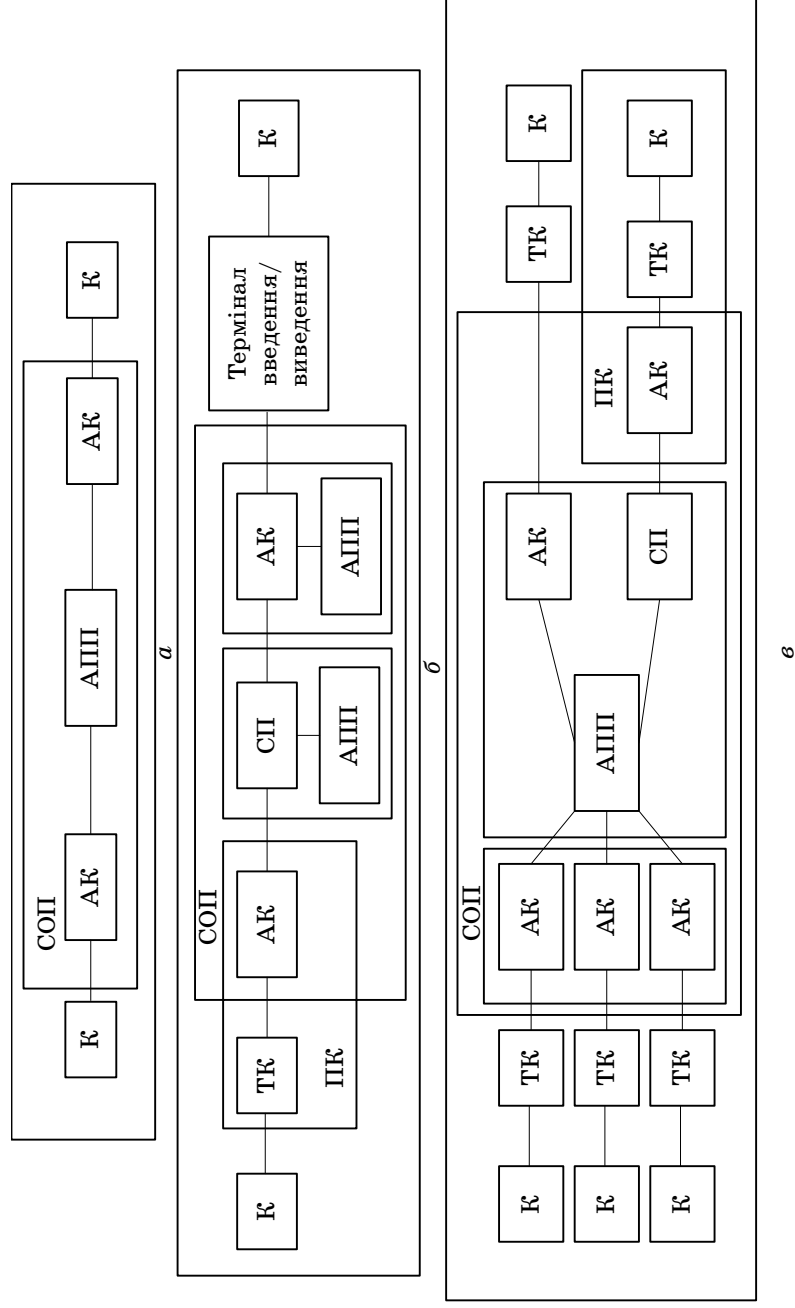


Рис. 7.9. Способы физической реализации системы обработки повідомлень

тури є тільки ілюстрацією до необмеженої кількості варіантів організації системи обробки повідомлень.

X.400-система і довідкова X.500-служба

Процес доставки повідомлення потребує відомостей про адреси одержувача, а за великих обсягів мережі запам'ятати всі адреси дуже складно і необхідно мати довідкову службу, яка б допомагала отримати адреси відправника/отримувача. Рекомендації МККТТ X.500 можна розглядати як стандарт для подібної довідкової служби.

Мета довідкової X.500-системи — забезпечення глобальної довідкової служби. Всі користувачі потенційно мають право входу в цей довідник, використовуючи певний набір атрибутів. Входи в інформаційну базу довідника розподілено за так званим інформаційно-довідковим номером. Вершини дерева є входами: більш високі вершини — це країни, далі йдуть організації тощо.

Якщо користувач не знає адреси відправника/одержувача, а знає тільки його довідкове ім'я, то функції присвоєння виконує найближчий X.400 агент пересилання повідомлень. Агент пересилання повідомлень також може перевіряти правильність адреси відправника/одержувача, присвоєної на попередніх етапах пересилання.

Взагалі, довідкова X.500-служба повинна забезпечувати користувача інформацією щодо своїх потенційних партнерів.

Протокол SMTP

SMTP (Simple Message Transfer Protocol), або, в дослівному перекладі, *простий протокол передачі повідомлень*, був створений у середовищі UNIX і призначався винятково для спілкування поштових серверів між собою. У термінах моделі OSI протокол SMTP перебуває на рівні додатків.

Нині SMTP став стандартом де-факто. Багато в чому така популярність пояснюється порівняною простотою реалізації та широкими можливостями розширюваності без шкоди для зворотної сумісності з наявними версіями поштових систем. Важливим фактором є також широка доступність специфікацій і відсутність необхідності відраховувати кошти за їхнє використання. SMTP-системи останнім часом активно розвиваються у напрямках:

- розширення протоколу спілкування сервер — сервер (власне SMTP);
- створення й поліпшення протоколу спілкування клієнт — сервер (POP3, IMAP4);
- впровадження й розширення нового формату повідомлень (MIME).

Початкова версія протоколу SMTP підтримувала обмежений набір команд і сервісів для прийому і передачі повідомлень. Останнім часом був розроблений його розширений варіант (*Extended* або *ESMTP*), що забезпечує стандартну можливість подальшого розширення і підтримку таких функцій, як підтвердження доставки (*Delivery Notification Request*, або *DNR*), узгодження максимально допустимого розміру повідомлень, переданих між серверами та примусовою ініціацією передачі накопиченої пошти (*dequeue*). Однак однією зі слабких сторін SMTP були і є неможливість аутентифікації вхідних з'єднань, шифрування діалогу й потоку передачі даних між серверами.

Відсутність засобів аутентифікації вхідних з'єднань не дозволила використовувати SMTP для обслуговування клієнтського доступу. Класична поштова SMTP-система вимагає наявності файлового доступу клієнта до своєї поштової скриньки для одержання та роботи з повідомленнями. Для реалізації роботи в режимі клієнт-сервер був створений протокол обслуговування поштового офісу (*Post Office Protocol*, або *POP*). Найбільш вдалою виявилася версія POP3, що широко використовується в сучасних SMTP-системах. Найбільш розвинені реалізації підтримують аутентифікацію із шифруванням імені і пароля та трафіку за протоколом *Secure Socket Layer* (SSL). Однак під час використання протоколу POP3 немає можливості перегляду характеристик повідомлення без попереднього завантаження його на станцію клієнта. Для рішення проблеми перегляду й маніпуляції властивостями поштового повідомлення безпосередньо на сервері, а також для подолання низки інших функціональних обмежень був розроблений протокол IMAP4, його підтримка в більшості комерційних систем очікується у найближчому майбутньому. Варто зазначити, що як для випадку використання класичного клієнта (команда *mail*), так і для випадку застосування POP3 або IMAP4, відправлення

підготовлених клієнтом повідомлень вимагає наявності сервера SMTP.

Спочатку SMTP-системи розраховували на передачу інформації винятково в текстовому вигляді й не були орієнтовані на передачу символів національних алфавітів, тобто використовували 7-бітний набір символів. Для рішення проблеми передачі двійкових файлів був розроблений стандарт UUENCODE, що дає змогу приймати попередньо перетворені з бінарного у текстовий вигляд довільні дані безпосередньо в текст повідомлення. Однак всеосяжним такий підхід назвати було важко, тому що в загальному випадку ніякої інформації про природу вкладення (типу переданих даних і програму, що їх створила) приймаюча сторона не мала. У міру розширення мережі Інтернет, ускладнення програмного забезпечення й активного впровадження мультимедіа назріла необхідність створення універсального формату типізації й подання двійкових даних і тексту, що містить національні символи. Таким універсальним форматом стали багатофункціональні розширення пошти (Multipurpose Internet Mail Extensions, або MIME). Формат MIME виявився надзвичайно вдалим, оскільки в нього були закладені можливості необмеженого розширення, як підтримуваних типів даних, так і національних кодувань.

Повідомлення SMTP, подібно повідомленню X.400, використовує поняття *конверту* та *вмісту*, що, у свою чергу, має *заголовок* і *тіло*. Функціональне призначення їх повністю ідентичне. Склад полів у заголовку визначається форматом тіла повідомлення (UUENCODE або MIME). Жодне поле не є обов'язковим, але, як правило, вказуються такі поля, як *кому* (To:), *від кого* (From:) і *тема* (Subject:). У випадку використання формату MIME, у заголовку обов'язково повинен бути рядок "MIME-Version: 1.0". Повний перелік можливих полів у заголовку повідомлення SMTP знаходиться в RFC 2076.

Відмінною рисою SMTP-систем є те, що в них, як правило, забезпечується фактична незалежність процесу передачі від формату *вмісту*. За інтерпретацію вмісту їм повинна відповідати тільки клієнтська програма (mail reader). Однак платою за сумісність на рівні МТА у цьому випадку є неефективність передачі будь-яких нетекстових даних або повідомлень, що ви-

користовують символи національних алфавітів, внаслідок попередньої трансляції інформації в текстове подання. Залежно від використовуваного алгоритму перетворення розмір фактично переданих даних може зрости на 30—100 %.

Важливою проблемою у процесі передачі даних за допомогою SMTP-систем є забезпечення конфіденційності. Оскільки повідомлення передаються в текстовому вигляді, вони можуть бути легко перехоплені і в довільній формі змінені. Для вирішення проблем щодо захисту інформації був створений стандарт на шифрування тіла повідомлення, так звані засекречені багатофункціональні розширення пошти (*Secure MIME*, або *S/MIME*). Однак цей протокол не в змозі захистити від перехоплення заголовки повідомлень.

Simple Mail Transfer Protocol не залежить від транспортного середовища й може використовуватися для доставки пошти в мережах із протоколами, відмінними від TCP/IP і X.25. Досягається це за рахунок концепції *IPCE* (*Interprocess Communication Environment*). IPCE дає змогу взаємодіяти процесам, що підтримують SMTP в інтерактивному режимі, а не в режимі “STOP-GO”.

Модель протоколу

Взаємодія в рамках SMTP будується за принципом двостороннього зв'язку, що встановлюється між відправником і одержувачем поштового повідомлення. При цьому відправник ініціює з'єднання й посилає запити на обслуговування, а одержувач на ці запити відповідає. Фактично, відправник є клієнтом, а одержувач — сервером (рис. 7.10).

Канал зв'язку встановлюється безпосередньо між відправником і одержувачем повідомлення. За такої взаємодії пошта досягає абонента протягом декількох секунд після відправлення.

Формат поштового повідомлення (RFC-822)

Формат поштового повідомлення Internet визначений у документі RFC-822 (Standard for ARPA Internet Text Message). Це досить великий документ обсягом у 47 сторінок машинописного тексту, тому розглянемо формат повідомлення на прикладах. Поштове повідомлення складається із трьох частин: конверта, заголовка й тіла повідомлення. Користувач бачить

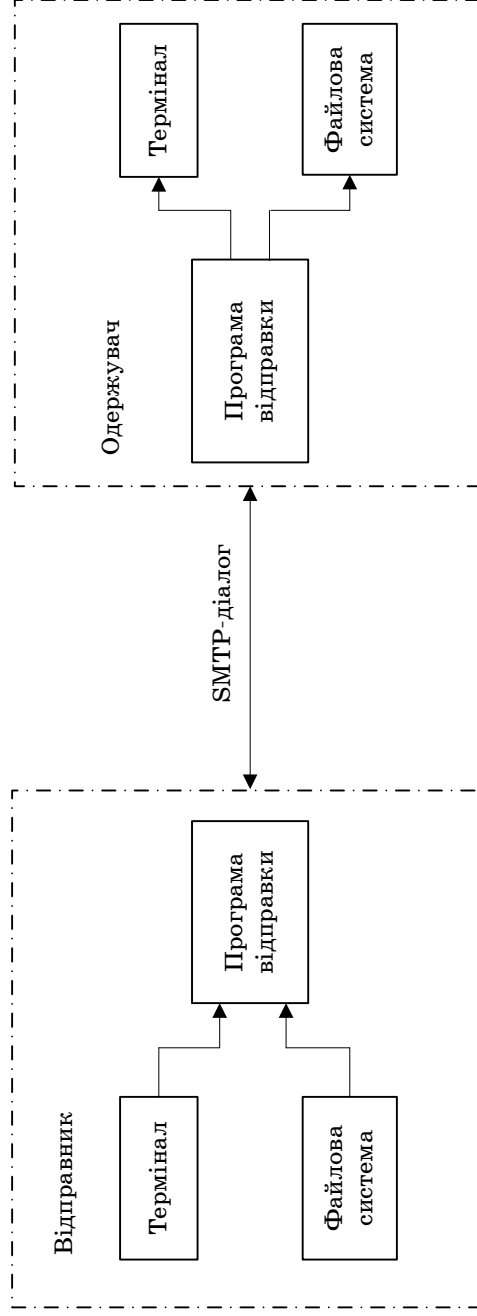


Рис. 7.10. Схема взаємодії за протоколом SMTP

тільки заголовок і тіло повідомлення. Конверт використовується лише програмами доставки. Заголовок завжди перебуває перед тілом повідомлення й відділений від нього порожнім рядком. RFC-822 регламентує зміст заголовка повідомлення, що складається з полів, які, у свою чергу, містять ім'я поля і його зміст. Ім'я поля відділене від змісту символом ":". Мінімумом необхідними є поля Date, From, cc або To.

Дисципліни роботи й команди протоколу

Обмін повідомленнями й інструкціями у SMTP ведеться в ASCII-кодах. У протоколі визначено кілька видів взаємодії між відправником поштового повідомлення і його одержувачем, які тут називаються дисциплінами. Найпоширенішою дисципліною є відправлення поштового повідомлення, що починається командою MAIL, яка ідентифікує відправника:

MAIL FROM: paul@quest.polyn.kiae.su

Наступною командою визначається адреса одержувача:

RCPT TO: paul@apollo.polyn.kiae.su

Після того, як визначені відправник і одержувач поштового повідомлення, можна відправляти останнє:

DATA

Команда DATA вводиться без параметрів та ідентифікує початок відправлення поштового повідомлення. Повідомлення вводиться доти, доки не буде введений рядок із крапкою в першій позиції. Відповідно до стандарту поштового повідомлення RFC 822 відправник передає заголовок та тіло повідомлення, які розділені порожнім рядком. Сам протокол SMTP не накладає яких-небудь обмежень на інформацію, що укладена між командами DATA і "." у першій позиції останнього рядка.

Для налагодження або перевірки з'єднання за SMTP можна використовувати telnet. Для цього слідом за адресою машини варто ввести номер порту:

telnet apollo.polyn.kiae.su 25

25-й порт використовується в Інтернеті для обміну повідомленнями за протоколом SMTP. В інтерактивному режимі користувач сам зображує клієнта SMTP і може подивитися реакцію вилученої машини на його дії.

Адресація в SMTP-системах

У системах на базі SMTP використовується інтуїтивно зрозуміла, проста й одночасно дуже потужна ієрархічна схема

адресації, аналогічна тій, що прийнята в службі імен Інтернету (Domain Name Services, або DNS). Ця схема може забезпечити унікальність адреси практично необмеженій кількості користувачів. Поштова адреса SMTP записується так:

mailbox@domain,

де *mailbox* — символічне ім'я поштової скриньки користувача, довжиною до 63 символів;

domain — унікальне ім'я (поштовий домен) системи, у якій зареєстрований згаданий користувач, довжиною до 255 символів.

Сполучення ім'я та домену утворить унікальний ідентифікатор користувача. Поштовий домен зберігає повну інформацію про положення системи в ієрархії поштового простору організації. Кожний наступний рівень ієрархії відокремлюється від попереднього крапкою. Розбір ім'я домену виконується зліва на право. Найвищий рівень (*top level*), який називають кореневим доменом (*root domain*), відповідає або типу організації (*com* — для комерційної, *gov* — державної, *org* — суспільної тощо), або географічному регіону (країні) (*ru* — для Росії, *fr* — Франції та ін.). Наступними в ієрархії йдуть домени першого рівня (*first level*), що, як правило, представляють ім'я організації. Реєстрацією імен domenів першого рівня займається міжнародний центр Інтернету (Internet Network Information Center, або InterNIC). За призначення імен domenів більш низького рівня найчастіше відповідають самі компанії. Оскільки організаціям не забороняється реєструвати для власних потреб декілька паралельних domenів (наприклад, CIT.MSK.RU і CIT.COM), користувач може мати більше однієї SMTP-адреси. Крім того, сучасні SMTP-системи найчастіше дають можливість призначати псевдоніми для самої поштової скриньки (наприклад, JohnDoe@CIT.MSK.RU і JonnyD@CIT.MSK.RU).

На рис. 7.11 наведений принцип утворення SMTP-адресації. У наведеному прикладі CIT.MSK.RU є субдоменом MSK.RU, що, у свою чергу, є субдоменом RU. Компанія CIT має два зареєстровані імені і кожний користувач може мати дві поштові адреси.

Маршрутизація

Для того щоб SMTP-сервер доставив пошту на ім'я адресата JohnDoe@CIT.MSK.RU, йому попередньо потрібно дізнатися

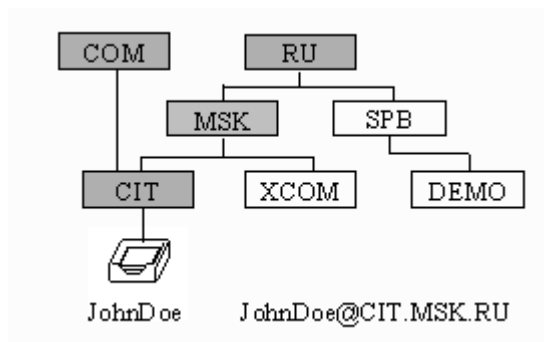


Рис. 7.11. Ієрархічна схема адресації SMTP

IP-адресу машини, що обслуговує поштовий домен CIT.MSK.RU, звернувшись із відповідним запитом до сервера DNS. У службі імен DNS передбачений спеціальний тип ресурсного запису для обслуговування таких запитів — MX, або Mail Exchanger, тобто сервер, що виконує обмін поштовими повідомленнями від імені домену.

Відповідно до термінології, прийнятої в Інтернеті, SMTP-сервер може бути:

- *mail exchanger* — комп'ютер, що безпосередньо підключений до Інтернету і виконує доставку повідомлень безпосередньо адресатам всередині організації, до якої він належить. В організації може бути кілька таких комп'ютерів з різними або однаковими значеннями показника вартості доставки;

- *relay* — комп'ютер, що виконує прийом поштового трафіку від імені інших доменів, які не мають безпосереднього і/або постійного підключення до Інтернету і, як правило, не належний до організацій, чиї домени він обслуговує. Із зазначеного вище випливає, що для кожного окремого домену може бути визначено не більше одного relay-сервера;

- *smart host* — комп'ютер, що здатний здійснювати пересилання повідомлень на основі власної статичної таблиці маршрутизації. Однією з функцій smart host є переписування на конверті адреси одержувача і/або відправника перед здійсненням подальшої передачі повідомлення.

Більшість сучасних реалізацій SMTP-серверів дають змогу сполучити всі перераховані функції на одному комп'ютері.

MIME (Multipurpose Internet Mail Extension)

Стандарт MIME, або в нотації Інтернету **RFC-1341, RFC-1521**, призначений для опису тіла поштового повідомлення Інтернет. Попередником MIME є *стандарт поштового повідомлення ARPA (RFC-822)*. Стандарт RFC-822 був розроблений для обміну текстовими повідомленнями. З моменту опублікування стандарту можливості апаратних засобів і телекомунікацій пішли далеко вперед і стало зрозуміло, що багато типів інформації, які широко використовуються в мережі, неможливо передати поштою без спеціальних хитрощів. Так у тіло повідомлення не можна включити графіку, аудіо, відео та інші типи інформації. RFC-822 не дає можливостей для передачі навіть текстової інформації, яку не можна реалізувати в семибітовому кодуванні ASCII. Природно, що під час використання RFC-822 не може бути й мови про передачу розміченого тексту для відображення його різними стилями. Обмеження RFC-822 стають ще більш очевидними, коли мова заходить про обмін повідомленнями в різних поштових системах. Наприклад, для прийому/передачі повідомлень із/в X.400, що дає можливість мати двійкові дані в тілі повідомлення, обмеження старого стандарту можуть стати фатальними, оскільки не рятує старий випробуваний спосіб кодування інформації процедурою *uuencode*, тому що ці дані можуть бути по-різному проінтерпретовані в X.400 і програмі розсилання пошти в Інтернеті (mail-agent). Розширенням стандарту RFC-1341 є стандарт RFC-1521, що додає деякі нові типи даних і поля тіла повідомлення.

У деякому розумінні стандарт MIME ортогональний стандарту RFC-822. Якщо RFC-822 докладно описує в заголовку поштового повідомлення текстове тіло листа й механізм його розсилання, то MIME, головним чином, зорієнтований на опис заголовка листа, структури тіла поштового повідомлення й можливості складання листа з інформаційних одиниць різних типів.

У стандарті зарезервовано декілька способів подання різно-рідної інформації. Для цієї мети використовуються спеціальні поля заголовка поштового повідомлення:

- поле версії MIME, що використовується для ідентифікації повідомлення, підготовленого в новому стандарті;
- поле опису типу інформації в тілі повідомлення, що дає змогу забезпечити правильну інтерпретацію даних;
- поле типу кодування інформації в тілі повідомлення, що вказує на тип процедури декодування;
- два додаткові поля, зарезервовані для більш детального опису тіла повідомлення.

Стандарт MIME розроблений як розширювана специфікація, яка базується на тому, що кількість типів даних буде зростати в міру розвитку форм подання даних. При цьому варто враховувати, що анархія типів (безмежне їхнє збільшення) теж не припустима. Кожний новий тип в обов'язковому порядку повинен бути зареєстрований в *IANA (Internet Assigned Numbers Authority)*.

Варто ще раз зазначити, що стандарт MIME дає змогу розширити сферу застосування електронної пошти, забезпечити доступ до інших інформаційних ресурсів мережі в стандартних форматах.

Доступ до поштової скриньки за допомогою POP3 і IMAP

Протоколи обміну поштовою інформацією POP3 і IMAP призначені для розбору пошти з поштових скриньок користувачів на їхні робочі місця за допомогою програм-клієнтів. Якщо за протоколом SMTP користувачі відправляють кореспонденцію за допомогою Інтернету, то за протоколами POP3 і IMAP користувачі одержують кореспонденцію зі своїх поштових скриньок на поштовому сервері в локальні файли. Розглянемо докладніше кожний із протоколів.

Протокол POP3 (Post Office Protocol version 3)

Номер TCP-порту протоколу POP3-110. Основна відмінність POP3 від інших Інтернет-протоколів верхнього рівня полягає в тому, що в ньому немає широкого спектра кодів помилок: у відповідь на будь-яку команду він посилає рядки, що починаються з "+OK" або "-ERR", які сигналізують відповідно про успішне або невдахе виконання команди.

Набір основних команд протоколу також досить простий:

USER name

Це перше, що посилає клієнт після того, як він зчитав рядок-вітання **+OK POP3 served ready**. Аргумент *name* вказує ім'я користувача на цьому поштовому сервері, для якого потрібно одержати доступ до поштової скриньки. Наприклад:

USER raaa

PASS password

Після того, як користувач вказав своє ім'я, він повинен вказати пароль до своєї поштової скриньки. Наприклад:

PASS doom

STAT

Якщо користувач існує і правильно ввів свій пароль, він може продивитися пошту. Команда **STAT** повідомляє поточний стан скриньки. Формат відповіді — **+OK n m**, де *n* — кількість повідомлень, *m* — кількість байт. Наприклад (у поштовій скриньці перебувають 11 листів загальним обсягом 1594 байти):

C: STAT

S: +OK 11 1594

LIST n

Для оцінки розміру конкретного листа є команда **LIST**. Формат виводу такий самий, як у **STAT**. Наприклад (третій лист має розмір 512 байт):

C: LIST 3

S: +OK 3 512

RETR n.

Для одержання листа із сервера використовується команда **RETR n**, де *n* — номер листа. Наприклад (одержуємо четвертий лист):

C: RETR 4

S: +OK 124 octets

S: Тут

S: іде

S: текст

S: листа

S:.

DELE n.

Після того, як листи успішно отримані й збережені локально, їх можна видалити з поштового сервера. Для цього є команда **DELE n**. Наприклад (видаляємо перший лист):

C: DELE 1
S: +OK message 1 deleted
QUIT.

Для завершення сеансу використовується команда **QUIT**

Протокол IMAP

Іншим протоколом розбору пошти є протокол **IMAP** (*Interactive Mail Access Protocol*) (**RFC-2060**), що за своїми можливостями дуже схожий на POP3, але був розроблений як більш надійна його альтернатива і до того ж має ширші можливості щодо керування процесом обміну із сервером.

Робота протоколу здійснюється за 143 портом TCP. Головною відмінністю від POP є можливість пошуку потрібного повідомлення й розбір заголовків повідомлення.

7.3. Інтегрована система Lotus Domino та Notes

Lotus Domino та **Notes** — це інтегрована система для колективної роботи, призначена для збирання, організації й розподілення інформації та знань, багатобічний програмний продукт, до складу якого входять такі інформаційні технології:

- документоорієнтована база даних;
- засоби розробки додатків;
- система електронної пошти;
- система реплікування (тиражування) документів, інформації і додатків;
- засоби захисту інформації і розмежування доступу;
- засоби календарного планування і складання розкладів;
- web-технології і технології інтернету/інтранету;
- засоби інтеграції з реляційними базами даних, системами керування ресурсами підприємств (ERP) і транзакційними системами.

Domino/Notes — це клієнт-серверна технологія, де сервером є Lotus Domino, а клієнтською частиною — Lotus Notes. Унікальність сервера Domino полягає в тому, що це ще і web-сервер, і поштовий сервер, який підтримує стандарти Інтернету, тому клієнтською частиною для роботи з додатками Domino

й електронною поштою можуть бути web-браузери та інші поштові клієнти Інтернету.

Документоорієнтована база даних Domino/Notes

Сховищем об'єктів, в яких зберігаються дані, є NSF-файли (Notes Storage File).

Бази даних Domino і Notes відрізняються від реляційних систем управління базами даних (СУБД), де дані описуються за допомогою таблиць. Реляційна база даних твердо структурована, а кожний запис у таблиці має однаковий набір полів, обсяг пам'яті під який визначений і виділений заздалегідь.

У більшості випадків люди працюють з документами, які є слабо структурованими об'єктами. Notes проектувався саме для роботи з такою інформацією. Це й визначило структуру бази даних Notes. Основною одиницею збереження інформації в базі даних Lotus Domino/Notes є окремий документ. Він не обов'язково має такі самі поля, що й інші документи, під поле виділяється стільки пам'яті, скільки необхідно для збереження конкретних даних; поля в документи можуть додаватися динамічно, у міру виникнення необхідності в них або змін розробників і користувачів. Наприклад, документ, що стосується обслуговування клієнтів, може містити дату, ім'я та ідентифікаційний номер клієнта, ім'я оператора, текстове поле для опису запиту клієнта, а також поле статусу запиту.

Структура документа Notes визначається формою, що містить набір полів різних типів. База даних Notes може зберігати будь-які типи даних — від простого тексту, чисел, часу і дати до форматowanego тексту, графічних образів, звуку, відео і довільних даних, що можуть зберігатися у вигляді приєднаних об'єктів у своєму рідному форматі. Наприклад, це може бути приєднаний файл формату MS Word або електронної таблиці Lotus 1-2-3.

Документ може мати як структурований, так і неструктурований формат, тому Notes може зберігати й обробляти такі масиви даних, обробка яких важко піддається реляційним та іншим системам баз даних.

Завдяки використанню документоорієнтованої моделі обробки Notes надає користувачам такі можливості.

- *Збереження форматowanego тексту, приєднаних і впроваджених об'єктів.* Сховище об'єктів Notes оптимально підходить для ефективного керування і розподілу ділової інформації: таблиці, отримані з реляційної бази даних, електронні таблиці, відформатований текст, web-сторінки, графіка, приєднані або впроваджені об'єкти, скановані зображення і факси, звукові та відеофрагменти. Таким чином, Notes може бути універсальним сховищем об'єктів і центральною точкою доступу до будь-якої корпоративної інформації.

- *Документи можуть мати стосунок один до одного як “батьківський” і “дочірній”.* Наприклад, якщо створено додаток для відстеження зовнішніх контактів, то батьківським документом може бути опис організації, дочірніми до нього — картки співробітників, наступним рівнем дочірніх документів — звіти про зустрічі зі співробітниками або листи тощо.

- *Повнотекстовий пошук.* Lotus Notes дає змогу користувачам індексувати документи і проводити їхній пошук за запитами, Notes наводить документи, що задовольняють критерії пошуку за ступенем їхньої відповідності або в заданому користувачем порядку.

- *Керування версіями.* Lotus Notes містить функцію, що відстежує численні зміни, внесені в документ різними користувачами. Автоматичне керування версіями реалізовано таким чином, що під час кожного сеансу редагування документ позначається або як основний, або як похідний від оригіналу. Зміни, внесені в документ Notes одним користувачем, не затираються, коли інший користувач зберігає свої зміни в документі. Функцію керування версіями Notes можна модифікувати відповідно до потреб будь-якої робочої групи. Крім того, користувачі мають можливість подавати додаткові коментарі до оригіналу документа, працюючи з ним як із похідним, тобто не зберігаючи оригінал повторно.

- *Посилання на документи.* Notes має засоби підтримки гіпертексту, тобто кожний документ може містити посилання на інші документи в будь-якій базі даних Notes або на документи у web-форматі.

- *Розмір сховища об'єктів Domino обмежений тільки доступними фізичними ресурсами.*

Бази даних Notes зазвичай розташовуються на серверах Domino, однак можуть перебувати і на клієнтських машинах з Notes, що дуже важливо з погляду підтримки роботи користувачів у режимі оф-лайн і мобільних користувачів. Користувачі одержують доступ до даних на сервері за допомогою мережі чи модема або, працюючи з даними локально за допомогою клієнта Notes. Однак як клієнти для роботи з даними і додатками на сервері Domino можуть використовуватися web-браузери, поштові клієнти Інтернету та ін.

У користувачів є можливість перегляду списків документів, що зберігаються в базі даних Domino/Notes, їх відображення називають поданням (view). Коли користувач Notes відкриває подання, назви полів виводяться як заголовки стовпців даних. Якщо, наприклад, користувач бажає переглянути документи за датою, Notes відсортовує їх за значеннями в цьому полі, відкриває подання, лівий крайній стовпець якого містить дату, а інша інформація з полів виводиться у стовпцях праворуч від основного. Різні подання можуть виконувати різні вибірки документів, а також їхнє сортування і/чи категоризацію (групування) за певними критеріями. Якщо продовжити приклад бази даних відстеження зовнішніх контактів, то одним з подань може бути перегляд усіх документів з категоризацією за назвою організацій, іншим поданням може бути тільки список особових карток співробітників, відсортований за прізвищами та ін.

Система реплікації

Система реплікації виконує два основні завдання:

- 1) підтримку територіально-розподіленої роботи (синхронізацію даних і додатків);
- 2) підтримку роботи мобільних користувачів.

Domino і Notes забезпечують колективне використання інформації в будь-який час і незалежно від місця розташування користувача. Користувачами баз даних і додатків Notes можуть бути співробітники з різних підрозділів організації у регіоні, країні або всьому світі. Кожний з цих підрозділів може мати свій сервер. Користувачі різних підрозділів працюють зі своєю “копією” бази даних, розташованою на локальному сервері, а реплікація забезпечує те, що робочі групи, розташовані

в різних географічних точках, працюють з актуальними версіями тих самих документів і обмінюються інформацією. Сервери Domino обмінюються даними відповідно до заданого розкладу і наявними каналами.

Domino і Notes дають змогу ефективно використовувати різні канали зв'язку: мережі TCP/IP, X.25, ISDN, телефонні канали, що комутуються, тощо.

Реплікація в Notes виконується на рівні окремих полів і характеризується такими властивостями.

- *Двоспрямованість.* Користувачі усіх підрозділів організації, які отримали за допомогою реплікації копію бази даних, можуть додавати, модифікувати і видаляти з неї документи. Двоспрямована реплікація в Notes синхронізує всі зміни, зроблені в усіх підрозділах, а не тільки поширює у віддалені сервери зміни, внесені в центральній точці.

- *Ефективність.* За синхронізації баз даних реплікація необхідна тільки для нових полів документів або для полів документів, до яких було внесено зміни у будь-якому з екземплярів бази даних, що беруть участь у процесі реплікації. Така реплікація на рівні поля забезпечує оптимальне використання ресурсів і найменшу тривалість циклу синхронізації.

- *Реплікація для клієнта Notes.* Користувачам, що підключаються до сервера від випадку до випадку (наприклад, мобільні користувачі, що працюють у віддаленій точці, відрядженні або вдома), необхідний такий же рівень доступу до інформації, як і підключеним користувачам. Notes не обмежується організацією взаємодії між серверами, він також підтримує реплікацію між клієнтом і сервером. За рахунок цього забезпечується підтримка роботи мобільних користувачів, що працюють з даними і додатками Notes у режимі оф-лайн, так, ніби вони перебувають в офісі та підключені до сервера. Користувач легко може взяти із собою актуальні копії баз даних Notes, працювати з ними локально, а потім синхронізувати їх, як тільки буде така можливість.

- *Вибіркова реплікація.* Користувачі Notes можуть скопіювати собі тільки певну підмножину інформації з бази даних Notes. Notes дає можливість їм визначати тип документів, з якими вони хочуть працювати на своїх клієнтських робочих

станціях. За допомогою вибіркової реплікації користувачі можуть копіювати тільки ті документи, що піддавалися змінам, скажімо, за останні 30 днів, або тільки складені яким-небудь конкретним членом робочої групи.

- *Фонова реплікація.* Проведення реплікації для мобільного користувача не припиняє усієї іншої роботи на портативному або домашньому комп'ютері. Реплікація в Notes може виконуватися у фоновому режимі, що дає змогу користувачеві продовжувати роботу над іншими завданнями.

- *Синхронізація дизайну і логіки додатків.* Технологія реплікації дає можливість легко поширювати додатки по всій організації і за її межами, вносити до них необхідні зміни у міру необхідності. Під час сеансів зв'язку між серверами Domino пересилаються не тільки самі дані, але й усі зміни в дизайні та логіці додатка. Domino зберігає дані та дизайн окремого додатка в єдиному файлі NSF. Наприклад, якщо розробники у Києві внесуть зміни у форму щоденної звітності, то в процесі чергового сеансу реплікації всі ці зміни будуть передані у віддалені підрозділи. У наступному сеансі роботи користувач зі Львова побачить, що дизайн додатка змінився, і почне працювати, по суті, з новою версією додатка.

Система електронної пошти і передачі повідомлень

Система передачі повідомлень Notes використовується:

- як зв'язок між людьми;
- як компонент додатків автоматизації робочих потоків (workflow);
- як платформа для групового ведення календаря і планування.

Сервер Domino забезпечує вбудовану підтримку будь-яких клієнтів передачі повідомлень, якими може скористатися замовник: web-браузерів, Microsoft Outlook, Eudora та інших поштових клієнтів POP3 та IMAP4.

Система передачі повідомлень Notes надає у розпорядження просту у використанні скриньку електронної пошти (рис. 7.12). Для обробки й організації великих обсягів пошти використовуються засоби керування повідомленнями. Користувацький інтерфейс Notes побудований на базі інтерфейсу Lotus cc:Mail, що став практично стандартом інтерфейсу електронної пошти

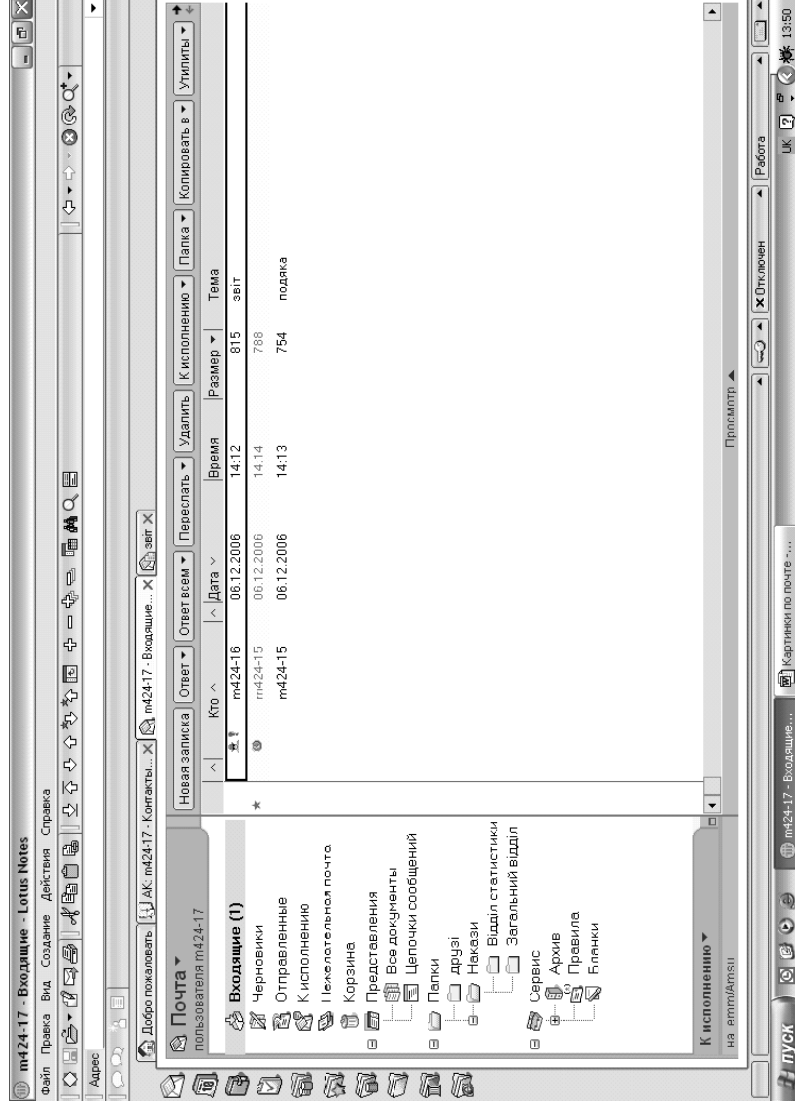


Рис. 7.12. Скринька електронної пошти Lotus Notes

для всіх виробників. Він містить потужний редактор для форматування тексту поштового повідомлення. Є можливість використання агентів для виконання різних завдань, таких, наприклад, як перегляд приєднаних до повідомлень файлів на наявність ключових слів і збереження їх у відповідній папці. Агенти можуть автоматизувати виконувані на сервері завдання, надаючи web-вузлу можливості автоматичної генерації поштових повідомлень певного змісту під час виконання певних умов і подій.

Електронна пошта є невід'ємною, фундаментальною частиною систем автоматизації потоків робіт і документообігу (workflow). Інтегрована в Domino/Notes система передачі повідомлень і бази даних документів поєднують обидва методи колективного використання інформації — “примусове проштовхування” і “добровільний витяг”, а також надають користувачам інтуїтивно зрозумілі й ефективні засоби для спільної роботи (рис. 7.13). Наприклад, під час створення вихідного варіанта документа, який мають переглянути деякі співробітники, користувач може надіслати їм повідомлення електронної пошти, що містить тільки посилання на цей документ. Кожний, хто отримав повідомлення, може відкрити документ, що забезпечує роботу всіх співробітників, з тим самим останнім варіантом. Поштові повідомлення можуть містити посилання на будь-які документи в базі даних Notes.

У більшості бізнес- і workflow-додатків часто потрібно довести до відома або оновити документ на основі значення певного поля чи стану процесу. Розглянемо додаток з обслуговування замовників. Запит замовника надходить у вигляді форми, заповненої ним на web-сторінці. Він вводиться в базу даних Domino з обслуговування замовників. Після її збереження сервер Domino автоматично посилає повідомлення електронної пошти відповідному представнику з обслуговування. Представник відкриває повідомлення і, клацнувши мишею на посиланні, що міститься в повідомленні, відкриває запит з колективно використовуваної бази даних, в якій можна зберігати свої зауваження і коментарі. Крім того, Domino-додаток контролює цей процес і, якщо він з якоїсь причини зупиняється (наприклад, якщо представник не починає ніяких дій за цим за-

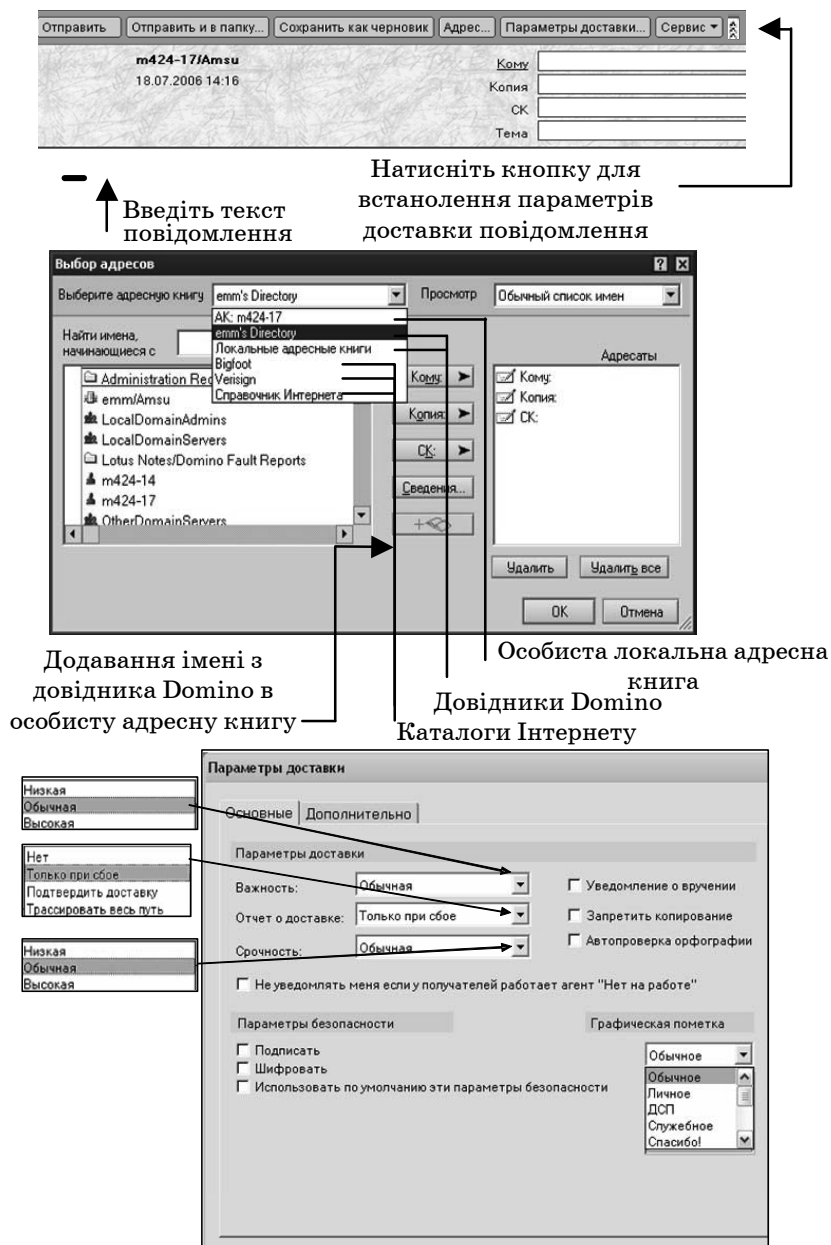


Рис. 7.13. Установлення умов доставки повідомлення

питом протягом 12 годин), то Domino розсилає додаткові повідомлення електронною поштою, цього разу не тільки представникові з обслуговування, а і його менеджеру, начальнику відділу обслуговування замовників, попереджаючи про потенційну проблему перед тим, як вона справді стане гострою.

За рахунок можливостей і функцій електронної пошти, шаблонів баз даних типу “Бібліотека документів”, “Дискусійна база даних”, “Узгодження документів” та інших, що поставляються разом з Domino, Domino і Notes є готовим рішенням у спільній роботі людей. Використання цих можливостей користувачами Інтернету, що не мають клієнта Notes, забезпечується за рахунок вибору шаблону, що підтримує роботу за допомогою web.

Функціонування системи електронної пошти як середовища передачі повідомлень ґрунтується на сервісах та службах, які підтримує сервер Domino. Серед них виокремлюють такі.

- *Надійне, гнучке і масштабоване сховище повідомлень Domino*, що ґрунтується на технології документоорієнтованих баз даних.

- *Сервіс каталогу масштабу підприємства (Domino Directory)*. Каталог Domino Directory — це масштабований і захищений компонент, що може легко виконувати вимоги до служби каталогів навіть величезних підприємств, забезпечуючи гарантовану підтримку мільйонів записів. Зміни, зроблені в одному екземплярі цього каталогу, можуть поширюватися по організації за допомогою ефективного і захищеного сервісу реплікацій Domino з гарантією синхронізації всіх копій Domino Directory. Можливості Domino і Notes щодо реплікування щойно змінених частин записів каталогу (до рівня поля) ще більше зменшують час реплікації і мережевий трафік, пов’язаний із синхронізацією каталогів у мережі. Domino Directory є основою моделі безпеки Domino і Notes. Він містить сертифікати, використовувані для аутентифікації всіх користувачів під час їхнього входу в систему, які, у свою чергу, містять публічні ключі, що використовуються для підписів і шифрування. Цей каталог також відіграє роль центру керування і конфігурування мережі. Він обслуговує користувачів, групи користувачів,

записи про з'єднання, ролі та іншу інформацію з контролю доступу, що дає змогу здійснювати централізоване керування (навіть у режимі оф-лайн) усієї мережної інфраструктури.

- *Сервіс маршрутизації повідомлень.* Маршрутизатор Domino забезпечує високопродуктивну і високоточну передачу повідомлень як для пошти, так і для додатків. Наприклад, користувачі Domino можуть працювати з безліччю протоколів, використовуючи і SMTP, і рідний для Notes протокол — Notes Remote Procedure Calls (NRPCs). Для сумісності з існуючими системами NRPCs може працювати із широким діапазоном мережних протоколів.

- *Сервіс безпеки* (більш докладно розглянемо пізніше).

- *Режим збереження “однієї копії об’єкта”* дає можливість заощаджувати дисковий простір і зменшувати трафік, розсилаючи ті самі повідомлення великій кількості користувачів.

Засоби розробки додатків

Платформа Notes містить інтегроване середовище розробки Domino Designer, що надає потужні засоби розробникам з різним рівнем підготовки.

Засоби розробки додатків, інтегровані в Domino Designer, є надійним, інтуїтивно зрозумілим середовищем, що забезпечує можливості використання стандартних засобів і мов розробки web-додатків та доступ до інших корпоративних систем.

Ієрархія засобів розробки за ступенем розширення можливостей:

- *дизайнер форм* — графічне середовище, що дає змогу задавати графічний вигляд документа, створювати поля, задавати їхні типи (текстовий, числовий, дата й час тощо), відстежувати й обробляти різні події, пов’язані з інформацією, що вводиться в ці поля, використовувати JavaScript для обробки подій, використовувати об’єкти групового календаря та ін.;

- *дизайнер сторінок* орієнтований на розробників, які звикли до стандартних засобів розробки web;

- *дизайнер структури* є графічним засобом створення структури web-вузла;

- *дизайнер рамок* є графічним засобом створення додатків з великою кількістю фреймів без необхідності програмування на HTML;

— *дизайнер графічних навігаторів* дає можливість розробляти й використовувати наочний інтерфейс навігаторів замість ієрархічних папок і подань у панелі пошуку Notes для ще більшого спрощення перегляду інформації в додатках;

— *графічне середовище створення подань*;

— *агенти* дають змогу вкладати складну логіку в додатки Notes і у такий спосіб розробники можуть автоматизувати виконання прикладних завдань на клієнтах і серверах. За допомогою агентів відстежують події, що можуть відбуватися або не відбуватися з документами в базах даних Notes та з поштовими повідомленнями. Наприклад, у додатку, що забезпечує узгодження документів, агент може відстежувати появу нових документів або факт того, що якась службова записка не була розглянута черговим учасником процесу узгодження протягом певного проміжку часу, про що начальникові автоматично сформується повідомлення електронної пошти з посиланням на відповідний документ;

— *засоби програмування*:

а) мова формул. Вона дуже схожа на мову, якою можна користуватися в електронних таблицях для обробки даних. Її можна використовувати для обробки інформації з різних полів документів для відображення у поданні;

б) Lotus Script: об'єктно-орієнтована версія мови програмування Basic, аналогічна Visual Basic;

в) Java і JavaScript.

Ці засоби дають повний програмувальний доступ до об'єктів і сервісів сервера Domino, таких як маршрутизація, реплікація, індексування подань, служба довідників, засоби контролю доступу та ін.

Захист інформації

Усі компоненти архітектури Domino і Notes використовують модель безпеки, яку визнано найбільш ефективною і гнучкою. Система безпеки Domino/Notes гарантує, що тільки авторизовані користувачі мають право на читання, створення і редагування інформації, котра зберігається в базах даних.

Стандартом доступу до каталогів X.500 є сертифікат X.509, що ґрунтується на технології шифрування RSA з відкритим ключем. Аутентифікація із застосуванням публічних ключів

виключає необхідність передачі паролів мережею. Публічні ключі, що використовуються разом з приватними ключами користувачів, уможливають створення цифрових підписів і повне шифрування документів і поштових повідомлень.

Інфраструктура Domino і Notes забезпечує чотири рівні безпеки.

1. *Аутентифікація* ґрунтується на сертифікатах і забезпечує надійну перевірку того, що користувачі, які підключаються до мережних ресурсів Domino, є тими, за кого вони себе видають.

2. *Цифрові підписи*, завдяки яким сервери Domino і клієнти Notes роблять аутентифікацію відправника, яка гарантує, що інформація, не підлягала змінам у процесі передачі.

3. *Контроль доступу* визначає, хто і який ресурс (сервер, базу даних, документ) може використовувати і що він може з цим ресурсом робити залежно від наявності імені користувача у відповідному списку контролю доступу (Access Control List) і наданих прав. Списки контролю доступу контролюють доступ до даних на рівні сервера, бази даних і окремих документів. Вони мають сім рівнів можливостей для роботи з інформацією у міру збільшення: “немає доступу”, депозитори, читачі, автори, редактори, дизайнери, менеджери. Окремі поля можуть бути зашифровані.

4. *Шифрування* гарантує безпечний зв’язок між окремими користувачами.

Шифрування може застосовуватися у таких випадках:

— для баз даних, включаючи документи і поля, як на серверах, так і на робочих станціях;

— для даних під час передачі, включаючи як передачу даних між серверами, так і передачу даних між клієнтом і сервером (це гарантує безпечну передачу даних небезпечними каналами, такими як Інтернет).

Каталог Domino Directory є основою моделі безпеки системи. Domino Directory підтримує делегування певних повноважень мережного керування за допомогою керування доступом до полів у собі самому. Будь-якому полю або групі полів можуть бути призначені обмеження тільки заданим користувачем, групою користувачів або роллю. Багато рівнів контролю

доступу користувачів, аж до доступу до полів документа, забезпечує делегування відповідальності за обслуговування спеціальних полів у Domino Directory або спеціальних параметрів конфігурації. Це дає змогу передати під відповідальність місцевих адміністраторів керування з'єднаннями серверів або доступом користувачів.

Засоби календарного планування

Однією з технологій, підтримуваних Domino/Notes, є технологія календарного планування.

“Календар” — це подання поштової бази даних Notes, необхідне для керування розпорядком дня (рис. 7.14). Передбачено роботу з власним календарем та календарем групи користувачів.

Власний календар застосовують для планування роботи одного користувача. За допомогою вбудованого в клієнтське місце Notes календаря можна призначати збори, інші заходи, річниці, нагадування і події (все разом називається записами календаря). Слід зазначити, що функції календаря доступні й під час роботи із сервером Domino через web-браузери.

Технологія календарного планування підтримує можливість перегляду календаря у форматі одного, двох днів, тижня, двох тижнів, місяця (рис. 7.15, 7.16).

Легке створення записів доповнюється можливостями створення повторюваних подій та нагадуванням про них.

У календарі передбачено створення розкладу вільного часу (рис. 7.17). За його допомогою користувач зазначає робочі дні тижня та години роботи, вільні для зборів. Ця інформація доступна іншим користувачам Notes для планування зборів. Переглядаючи розклад, інші користувачі можуть побачити ваш робочий і зайнятий час.

Робочі години визначають час, коли ви доступні для зборів, і задаються у властивостях розкладу вільного часу. Наприклад, ви можете бути доступні для зборів тільки у певні дні або у певний час кожного дня. Запланований час показує конфлікти в розкладі, наприклад, накладки в часі запланованих зборів.

За допомогою календаря групи можна швидко довідатися, чи є зайнятими або вільними члени групи у певний час. Календарі груп формуються на основі власних календарів користува-

Календарь

пользователя m424-17

Собрание

Создать

Сервис

День

Неделя

Месѧц

Собрания

Форматирование

Сентябрь 2006 г.

Сентябрь 2006 г.

Пн

Вт

Ср

Чт

Пт

Сб

Вс

28

29

30

31

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

1

Сегодня - 8 Сентябрь

2006

Отображение этой части
вашего календаря не
настроено.
Чтобы настроить
отображение, нажмите
кнопку, расположенную
ниже.

Настроить

понеѧдельник - 4 Сентябрь 2006 г.

13:00

инт

вторник - 5 Сентябрь 2006 г.

16:30 - 17:30

среѧа - 6 Сентябрь 2006 г.

пятница - 8 Сентябрь 2006 г.

суббота - 9 Сентябрь 2006 г.

воскресенье - 10 Сентябрь 2006 г.

Осталось недель: 16

Неделя 36

Просмотр

Рис. 7.14. Зовнішній вигляд подання “Календар”

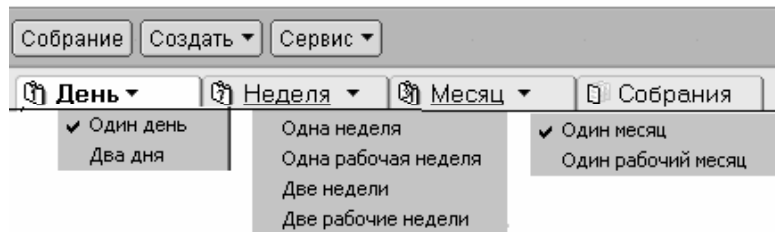


Рис. 7.15. Режимы просмотра календаря

чів. Кожний власник календаря надає відповідні рівні доступу іншим користувачам групи (рис. 7.18). Можна настроїти відображення відомостей про розклад, а також задати вигляд відображуваних відомостей для користувачів, що складають розклад зборів і перевіряють для цього ваш розклад.

Рівень відомостей визначається адміністратором Domino. При цьому інші користувачі, як мінімум, можуть переглянути, які години у вас зайняті або вільні. Можна також надати іншим користувачам доступ до тексту записів календаря.

Додатково на основі комунікаційних можливостей Domino і Notes забезпечуються такі функції групового календаря:

- сповіщення учасників про зустрічі й наради;
- пошук вільних проміжків часу;
- резервування ресурсів і приміщень;
- можливості перегляду календаря інших співробітників (якщо надані права);
- делегування повноважень у роботі з календарем та поштовою скринькою.

Упровадження засобів календарного планування і керування ними виконується за рахунок їх інтеграції з інфраструктурою передачі повідомлень і колективної роботи (рис. 7.19). Користувачі Domino/Notes можуть бачити вільний і зайнятий робочий час у режимі реального часу, приймати і відсилати повідомлення про ділові зустрічі електронною поштою, а потім корегувати свої ділові розклади (календарі) в автономному режимі (оф-лайн) так само ефективно, як і в підключеному (он-лайн).

Сохранить и закрыть

Запись календаря

Оповещение

Пометить как личное

Тема: Засідання кафедри

Место: Расположение: ауд. 418

Когда: Начало: Ср 13.09.2006 15:00

Окончание: Ср 13.09.2006 17:00

Указать другой часовой пояс

Повторы

Описание: Добавление вложений

Проверка навчально-методичних комплексів дисциплін

Параметры повтора

Укажите, когда повторяется это событие

Еженедельно

По средам

Укажите, как долго повторяется это событие

Начало: 13.09.2006

по 10 недель

в течение

Начало 13.09.2006, повторяется в течение 10 недель, кончая 15.11.2006

Собрание: запланировано на 10 дней

13 сентября 2006 г.
20 сентября 2006 г.
27 сентября 2006 г.
4 октября 2006 г.
11 октября 2006 г.
18 октября 2006 г.
25 октября 2006 г.
1 ноября 2006 г.
8 ноября 2006 г.
15 ноября 2006 г.

Параметры оповещений

Оповещение включено

Отключить оповещение перед возникновением этого события

Выдача уведомления

Время отключения оповещения: 30 минут до события

Действие при отключении оповещения

Вывести окно с текстом оповещения

Воспроизвести звук: chord

Отправить почтовое уведомление с темой

Получатели: Rogovenko Wladimir/Amsu, m424-

OK

Отмена

Рис. 7.16. Створення запису з налагодженням режимів повтору та сповіщення

Параметры

Почта

Календарь и задачи

Доступ и делегирование

Основные

Вывод

Планирование

Оповещения

Задачи

Автообработка

Цвета

Ваша доступность

Укажите даты и время, когда вы свободны и можете присутствовать на собраниях. Когда кто-либо будет планировать собрания, он будет видеть, что вы доступны только в это время.

Время (например: 09:00 - 12:00, 13:00 - 17:00, но не 17:00 - 05:00)

Воскресенье

Понедельник

Вторник

Среда

Четверг

Пятница

Суббота

09:00 - 10:00, 13:00 - 14:00

08:00 - 09:00, 16:00 - 17:00

08:00 - 09:00, 16:00 - 17:00

08:00 - 09:00, 16:00 - 17:00

08:00 - 09:00, 16:00 - 17:00

09:00 - 10:00, 13:00 - 14:00

Часовой пояс

Местное время

При добавлении записи в ваш календарь

Проверка конфликтов с другими записями:

При добавлении мероприятий, принятии собраний, планировании новых собраний

Для новых собраний планировщик исходно отображает:

Сведения о расписании каждого из участников

Наиболее подходящее время собрания

OK

Отмена

Рис. 7.17. Планирования розклада вільного часу

?

✕

Добавление пользователей или групп

1

Введите имя пользователя или группы, которым нужно предоставить доступ к вашему почтовому файлу

☒

Введите или выберите пользователя или группу

☐

Доступ всем пользователям

Иван Петрович Иванов

2

Выберите разделы почтового файла, доступ к которым нужно предоставить этому пользователю или группе

☒

Вся почта календарь и задачи

☒

Только календарь и задачи

☐

Нет

3

Выберите уровень доступа, который нужно предоставить этому пользователю или группе

Чтение любых записей календаря или задач

4

Автоматически пересылать этому пользователю присылаемые вам извещения календаря

Включение автоматической пересылки позволяет другим пользователям управлять вашим календарем, не держа его постоянно открытым.

☐

Пересылать извещения когда вы являетесь приглашенным на собрание

☐

Пересылать извещения когда вы являетесь ответственным за собрание

Если сообщение помечено как служебное:

Не пересылать

Примечание: этот параметр влияет на все автоматически пересылаемые сообщения

OK

Отмена

Рис. 7.18. Надания доступу до почты, календаря та завдань



Рис. 7.19. Вікно перевірки стану учасників зборів групи

За рахунок інтегрованих засобів збереження календарної інформації, сервісу реплікацій вбудовані засоби календарного планування Lotus Notes повністю підтримують роботу мобільних користувачів, для яких постійно оновлюється не тільки поштова інформація, дані та додатки, а й інформація про календар зустрічей, контрольні дати тощо.

Архітектура цілком підтримує функцію календарного планування спільних заходів декількох організацій за допомогою глобальних мереж.

Domino як web-сервер та інтернет/інтранет-технології

Сервер Domino та клієнт Notes підтримують цілий спектр технологій і стандартів Інтернету.

Domino — це web-сервер, що підтримує стандарти HTTP і HTTPS. Як будь-який інший web-сервер, він може взяти HTML-файл і надати його web-браузеру. Унікальною відмінністю сервера Domino від інших web-серверів є можливість конвертувати документи Notes у формат HTML і надавати, таким чином, абсолютно актуальну інформацію з баз Notes користувачеві, що її запитує, за допомогою браузера. Отже, інформація для web-вузла зберігатиметься не у вигляді файлів HTML у файловій системі, а у вигляді документів бази даних Domino як захищеного надійного сховища об'єктів, що підтримує всі необхідні посилання.

Це означає, що можна без додаткових витрат використовувати усі засоби розробки Lotus Domino та зробити додатки й дані Domino доступними для користувачів Інтернету/інтранету. При цьому всі сервіси Domino, такі як індексування документів, категоризація, повнотекстовий пошук, реплікація, агенти, що запускаються за розкладом і за надходженням певних подій, автоматично стають доступними для розробника web-сервера.

Сервер Domino підтримує основні стандарти Інтернету.

Клієнт Notes за рахунок підтримки стандартів POP3, MIME, HTML — це повноцінний поштовий клієнт Інтернету, за допомогою якого користувачі можуть керувати всіма своїми поштовими скриньками, незалежно від того, розташовані вони на сервері Domino чи надані провайдером.

Засоби інтеграції з іншими корпоративними системами, реляційними СУБД і системами керування ресурсами підприємства

Під час інтеграції сховища об'єктів Notes з іншими базами даних підприємства Notes дають змогу збільшити загальну цінність інформаційних активів організації.

Сервер Domino має можливість обміну даними з іншими інформаційними системами, такими як реляційні СУБД. У сполученні з потужними можливостями Notes можна створити передовий інтерфейс доступу до корпоративних даних як засобами Notes, так і за допомогою web, що дозволить поєднати практично всі джерела інформації.

Lotus містить цілий спектр технологій інтеграції, що дають можливість розробникам додатків повною мірою використовувати усі функції Lotus Notes та реляційних баз даних.

Таким чином, технологія Domino і Notes надає в розпорядження користувачам інфраструктуру передачі повідомлень, електронної пошти, бізнес-додатків та web світового класу, що в сукупності дають готове рішення у спільній роботі. Властивості незалежності від платформи, масштабованість, чудові можливості інтеграції даних і додатків та безліч інших додаткових функцій забезпечують стабільність роботи цих технологій в організації будь-якого рівня.

Запитання і завдання для самоконтролю

1. Що розуміють під електронним обміном даними? Які переваги та можливості електронного обміну даними?
2. У чому причина необхідності стандартизації подання електронних документів для обміну даними?
3. Які компоненти підлягають стандартизації під час підготовки документів для передачі каналами комунікацій?
4. Які положення покладено в основу стандарту EDIFACT?
5. Охарактеризуйте особливості стандарту OBI та його призначення.

6. Визначте основні особливості стандарту EANCOM.
7. Дайте визначення електронної пошти та розкажіть про особливості її застосування.
8. Який міжнародний стандарт покладено в основу систем передачі електронних повідомлень? Дайте характеристику компонентів системи управління повідомленнями та способів їх взаємодії згідно зі стандартом.
9. Назвіть складові повідомлення та їх призначення.
10. Охарактеризуйте структуру функціональної моделі системи обробки повідомлень.
11. Які способи взаємодії між компонентами системи обробки повідомлень?
12. Наведіть приклади схем фізичної реалізації електронної пошти згідно зі стандартом X.400.
13. Яке призначення та принципи організації довідкової служби в системах передачі повідомлень?
14. Яке призначення системи Lotus Domino/Notes? Назвіть технології, які вона підтримує.
15. Дайте характеристику документоорієнтованій базі даних. Які її переваги порівняно з реляційною?
16. Для чого призначена система реплікацій? Які можливості надає механізм реплікацій у системі Lotus Domino/Notes?
17. Назвіть основні характерні риси системи електронної пошти Lotus Domino/Notes. Які функціональні процеси забезпечує електронна пошта Lotus Domino/Notes?
18. Які можливості розробки власних додатків надає система Lotus Domino/Notes?
19. Які положення покладено в основу системи захисту інформації Lotus Domino/Notes? На яких рівнях може бути забезпечений захист інформації у цій системі?
20. Які можливості управління персоналом надає система календарного планування Lotus Domino/Notes?
21. Які можливості роботи у мережі Інтернет забезпечуються системою Lotus Domino/Notes?
22. Назвіть характерні риси протоколу SMTP та його моделі.

- 23. Які ви знаєте команди протоколу SMTP?
- 24. Надайте характеристику схеми адресації систем на базі SMTP.
- 25. Для чого призначений протокол обміну поштовою інформацією POP3 (RFC-1939)? Наведіть приклади основних команд протоколу.

Розділ 8

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

8.1. Захист інформаційних ресурсів від несанкціонованого доступу

Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої держави. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути найновіші автоматизовані технічні засоби.

Останнім часом в Україні відбуваються якісні зміни у процесах управління на всіх рівнях, які зумовлені інтенсивним впровадженням новітніх інформаційних технологій. Швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем.

Наскільки актуальна проблема захисту інформації від різних загроз, можна побачити на прикладі даних, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

- 1) несанкціонований доступ — 2 %;

- 2) укорінення вірусів — 3 %;
- 3) технічні відмови апаратури мережі — 20 %;
- 4) цілеспрямовані дії персоналу — 20 %;
- 5) помилки персоналу (недостатній рівень кваліфікації) — 55 %.

Таким чином, однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки вони становлять 75 % усіх випадків.

Відповідно до вимог законів України “Про інформацію”, “Про державну таємницю” та “Про захист інформації в автоматизованих системах” основним об’єктом захисту в інформаційних системах є інформація з обмеженим доступом, що становить державну або іншу, передбачену законодавством України, таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження.

Загалом, об’єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації.

Порушник — користувач, який здійснює несанкціонований доступ до інформації

Загроза несанкціонованого доступу — це подія, що кваліфікується як факт спроби порушника вчинити несанкціоновані дії стосовно будь-якої частини інформації в інформаційній системі.

Потенційні загрози несанкціонованого доступу до інформації в інформаційних системах поділяють на цілеспрямовані (умисні) та випадкові. *Умисні загрози* можуть маскуватися під випадкові шляхом довгочасної масованої атаки несанкціонованими запитами або комп’ютерними вірусами.

Вимоги національних стандартів і нормативних документів з питань технічного захисту інформації в Україні, а також досвід розвитку міжнародних стандартів безпеки досліджено у працях М.С. Вертузаєва, О.М. Юрченка, В.В. Домарева.

Розглянемо можливі канали витоку інформації та варіанти несанкціонованого доступу до неї¹.

За відсутності законного користувача, контролю та розмежування доступу до термінала кваліфікований порушник легко використовує його функціональні можливості для несанкціонованого доступу до інформації, що підлягає захисту, шляхом уведення відповідних запитів або команд.

За наявності вільного доступу до приміщення можна візуально спостерігати інформацію на засобах відбиття і документування, викрасти паперовий носій, зняти зайву копію, а також викрасти інші носії з інформацією: лістинги, магнітні носії та ін.

Особливу загрозу становить безконтрольне завантаження програмного забезпечення, в якому можуть бути змінені установки, властивості, дані, алгоритми, введено “троянську” програму або вкорінено комп’ютерний вірус, що виконують деструктивні несанкціоновані дії. Наприклад, записування інформації на сторонній носій, незаконне передавання у канали зв’язку, несанкціоноване друкування документів, порушення їх цілісності, несанкціоноване копіювання важливої інформації, вагомість якої визначається та обмежується на дуже короткий або, навпаки, тривалий час.

Загрозливою є ситуація, коли порушник — санкціонований користувач інформаційної системи, який у зв’язку зі своїми функціональними обов’язками має доступ до однієї частини інформації, а користується іншою за межами своїх повноважень. З боку санкціонованого користувача є багато способів порушення роботи інформаційної системи й одержання, модифікування, поширювання або знищення інформації, що підлягає захисту. Для цього можна використовувати, насамперед, привілейовані команди введення-виведення, неконтрольованість санкціонованості або законності запиту і звернень до баз та банків даних, серверів тощо. Вільний доступ дає порушникові можливість звертатись до чужих файлів і баз даних та змінювати їх випадково або умисно.

¹ Вертузаєв М.С. Захист інформації в комп’ютерних системах від несанкціонованого доступу : навч. посіб. / М.С. Вертузаєв, О.М. Юрченко. — К. : Вид-во Європ. ун-ту, 2001.

Під час технічного обслуговування апаратури можуть бути виявлені залишки інформації на її носіях (поверхні твердих дисків, магнітні стрічки та інші носії). Стирання інформації звичайними методами (засобами операційних систем, спеціальних програмних утиліт) неефективне з погляду технічного захисту інформації. Порушник може поновити і прочитати її залишки, саме тому потрібні тільки спеціальні засоби стирання інформації, що підлягає захисту.

Під час транспортування носіїв територією, яка не охороняється, виникає загроза перехоплення інформації, що підлягає захисту, і подальшого ознайомлення з нею сторонніх осіб.

Зловмисник може стати санкціонованим користувачем інформаційної системи у режимі розподілу часу, якщо він попередньо якось визначив порядок роботи санкціонованого користувача або якщо він працює з ним на одних лініях зв'язку. Він може здійснити підключення до лінії зв'язку між терміналом та процесором ЕОМ. Крім того, без переривання роботи санкціонованого користувача порушник може продовжити її від його імені, анулювавши сигнали відключення санкціонованого користувача.

Обробка, передавання та зберігання інформації апаратними засобами інформаційної системи забезпечуються спрацюванням логічних елементів на базі напівпровідникових приладів. Спрацювання логічних елементів зумовлено високочастотним зміщенням рівнів напруг і струмів, що призводить до виникнення в ефірі, ланках живлення та заземлення, а також у паралельно розміщених ланках й індуктивностях сторонньої апаратури електромагнітних полів, які несуть в амплітуді, фазі й частоті своїх коливань ознаки оброблюваної інформації. Використання порушником різних приймачів може призвести до не санкціонованого витоку та перехоплення дуже важливої інформації, що зберігається в інформаційній системі. Зі зменшенням відстані між приймачем порушника й апаратними засобами інформаційної системи ймовірність приймання таких інформаційних сигналів збільшується.

Окремим видом дуже небезпечної перспективної загрози професійних порушників є так звані радіочастотні засоби електромагнітного ураження, які спричиняють ураження напівпровідникової елементної бази за рахунок надпотужної енерге-

тичної дії електромагнітних випромінювань радіочастотного діапазону, що може призвести до повної або тимчасової відмови в роботі інформаційної системи у найбільш відповідальних ситуаціях.

Несанкціоноване підключення порушником приймальної апаратури та спеціальних датчиків до ланцюгів електроживлення та заземлення, інженерних комунікацій і каналів зв'язку в трактах передачі даних може спричинити модифікацію та порушення цілісності інформації в комп'ютерних мережах.

Таким чином, порушники технічного захисту інформації можуть створювати такі *потенційні загрози для безпеки інформації* в інформаційних системах:

1) загрози конфіденційності (несанкціонованого одержання) інформації всіма потенційними і можливими каналами її витоку, особливо каналами побічних електромагнітних випромінювань і наведень, таємними каналами зв'язку в імпортному обладнанні та розвідувальними закладними пристроями;

2) загрози цілісності (несанкціонованої зміни) інформації;

3) загрози доступності інформації (несанкціонованого або випадкового обмеження) та ресурсів самої інформаційної системи;

4) загрози спостереженості роботи інформаційної системи (порушення процедур ідентифікації та аутентифікації, процедур контролю доступу і дій користувачів, повна або часткова втрата керованості інформаційної системи, загрози від несанкціонованих атак і вторгнень порушників технічного захисту інформації до програмних, телекомунікаційних та апаратних засобів інформаційної системи, загрози для передачі даних і маніпуляцій з протоколами обміну (контролю) та із загально-системним програмним забезпеченням, реєстрація, вірогідний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, аутентифікація під час обміну, аутентифікація відправника (невідмова від авторства), аутентифікація одержувача (невідмова від одержання) та ін.);

5) загрози проникнення комп'ютерних вірусів;

6) загрози радіочастотних засобів електромагнітного ураження високопрофесійних порушників.

Загрози порушників технічного захисту інформації можуть здійснюватись:

1) технічними каналами: акустичними, оптичними, хімічними тощо;

2) каналами спеціального впливу шляхом формування полів і сигналів для руйнування системи захисту або порушення цілісності інформації;

3) несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскуванню під зареєстрованого користувача, подолання засобів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

8.2. Методи і засоби захисту інформації в інформаційних системах

Сукупність методів і засобів захисту інформації включає програмні й апаратні засоби, захисні перетворення та організаційні заходи (рис. 8.1).

Апаратний, або схемний, захист полягає в тому, що в приладах ЕОМ та інших технічних засобах обробки інформації передбачається наявність спеціальних схем, що забезпечують захист і контроль інформації, наприклад, схеми контролю на чесність, які контролюють правильність передачі інформації між різними приладами ЕОМ, а також екрануючими приладами, що локалізують електромагнітні випромінювання.

Програмні методи захисту — це сукупність алгоритмів і програм, які забезпечують розмежування доступу та виключення несанкціонованого використання інформації.

Сутність методів захисних перетворень полягає в тому, що інформація, яка зберігається в системі та передається каналами зв'язку, подається в деякому коді, що виключає можливість її безпосереднього використання.

Організаційні заходи із захисту інформації містять сукупність дій з підбору та перевірки персоналу, який бере участь у підготовці й експлуатації програм та інформації, чітке регламентування процесу розробки та функціонування інформаційної системи.

Лише комплексне використання різних заходів (рис. 8.2) може забезпечити надійний захист інформації, тому що кожний метод або захід має слабкі та сильні сторони.

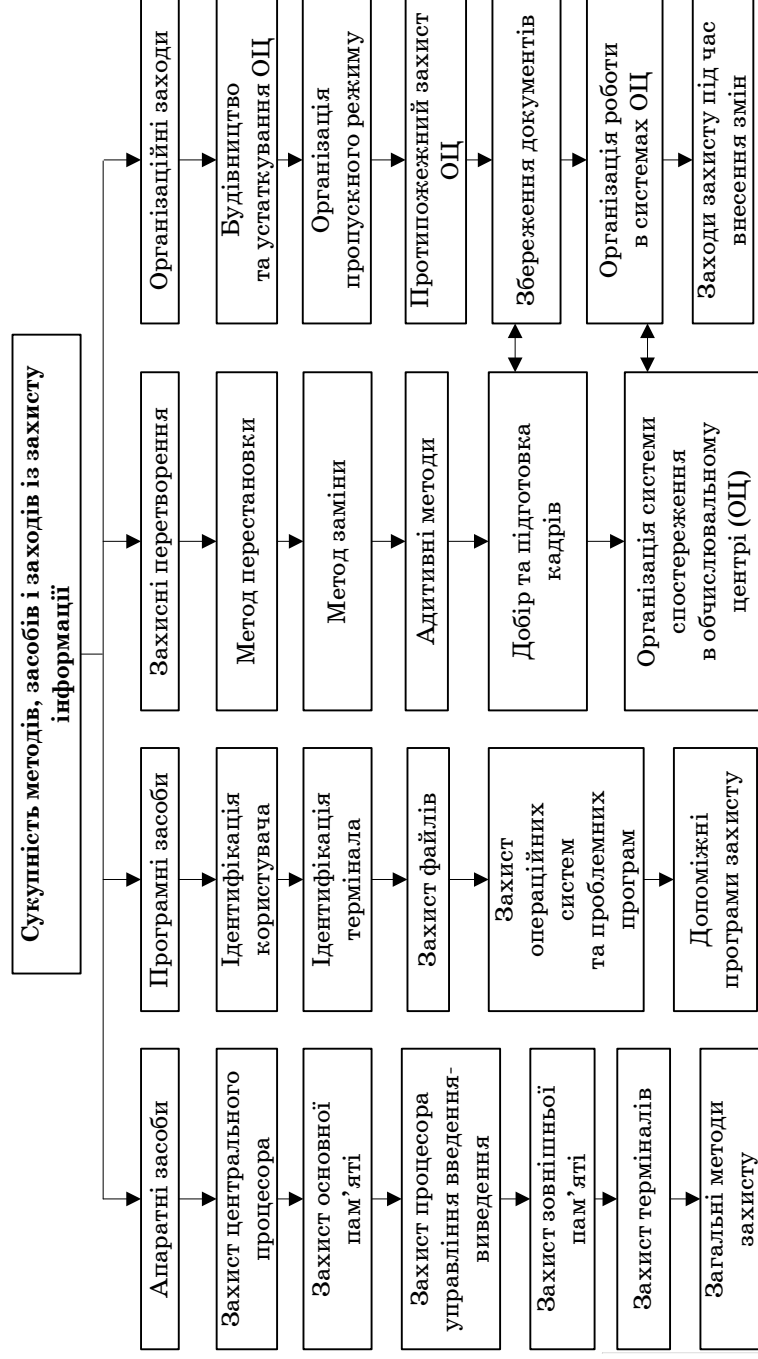


Рис. 8.1.1. Методи і засоби захисту інформації

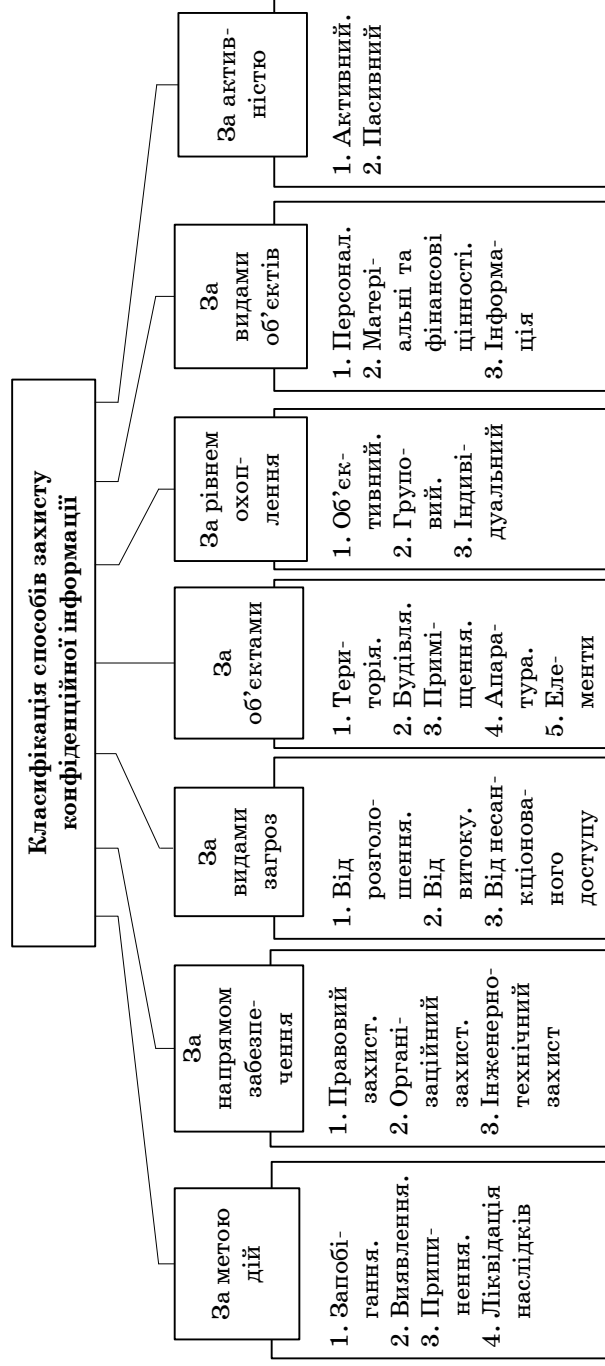


Рис. 8.2. Класифікація способів захисту конфіденційної інформації

8.3. Правове забезпечення режиму електронного цифрового підпису

Закон України “Про електронний цифровий підпис”, прийнятий 22 травня 2003 р. № 852-IV (далі — Закон № 852), набрав чинності 1 січня 2004 р. Цей закон визначає правовий статус електронного цифрового підпису і регулює відносини, що виникають під час використання електронного цифрового підпису.

У ст. 1 цього Закону подаються такі визначення.

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.

Особистий ключ — параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Відкритий ключ — параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб’єктам відносин у сфері використання електронного цифрового підпису.

Підписувач — особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа.

Документом, який засвідчує чинність і належність відкритого ключа підписувачу, є **сертифікат відкритого ключа** (далі — сертифікат ключа), виданий центром сертифікації ключів.

Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача.

Сертифікат ключа, що засвідчує відкритий ключ підписувача, згідно зі ст. 6 Закону містить такі обов’язкові дані:

- найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);

- зазначення, що сертифікат виданий в Україні;
- унікальний реєстраційний номер сертифіката ключа;
- основні дані (реквізити) підписувача — власника особистого ключа;

- дату і час початку та закінчення строку чинності сертифіката;

- відкритий ключ;

- найменування криптографічного алгоритму, що використовується власником особистого ключа;

- інформацію про обмеження використання підпису.

Правовий статус електронного цифрового підпису

Статтею 3 Закону № 852 визначено, що *електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки)* у разі, якщо:

- електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;

- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;

- особистий ключ підписувача відповідає відкритому ключу, зазначеному в сертифікаті.

Посилений сертифікат відкритого ключа (далі — посилений сертифікат ключа) — сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом.

Акредитований центр сертифікації ключів — центр сертифікації ключів, акредитований у встановленому порядку (ст. 9 Закону № 852).

Засвідчувальний центр центрального органу виконавчої влади — центр, визначений Кабінетом Міністрів України для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи центрів сертифікації ключів, які надають послуги електронного цифрового підпису цьому органу і

підпорядкованим йому підприємствам, установам та організаціям (ст. 10 Закону № 852).

Центральний засвідчувальний орган визначається Кабінетом Міністрів України (ст. 11 Закону № 852).

Зазначимо, що електронний підпис не може бути визнано недійсним лише тому, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.

Призначення електронного підпису

У ст. 4 Закону “Про електронний цифровий підпис” зазначено, що електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

Електронний цифровий підпис використовується фізичними та юридичними особами — суб’єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

Нотаріальні дії із засвідчення справжності електронного цифрового підпису на електронних документах учиняються відповідно до порядку, встановленого законом.

Статтею 5 Закону України “Про електронний цифровий підпис” визначено, що органи державної влади, органи місцевого самоврядування, підприємства, установи й організації державної форми власності для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа.

Інші юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом ключа, сформованим центром сертифікації ключів, а також використовувати електронний цифровий підпис без сертифіката ключа.

У випадках, коли відповідно до законодавства необхідне засвідчення дійсності підпису на документах та відповідності копій документів оригіналам, печаткою на електронний документ накладається ще один електронний цифровий підпис юридичної особи, спеціально призначений для таких цілей.

Права й обов’язки підписувача визначено у ст. 7 Закону № 852 (табл. 8.1).

Таблиця 8.1. Права й обов'язки підписувача

Права	Обов'язки
Вимагати скасування, блокування або поновлення свого сертифіката ключа	Зберігати особистий ключ у таємниці
Оскаржити дії чи бездіяльність центру сертифікації ключів у судовому порядку	Подавати центру сертифікації ключів дані для засвідчення чинності відкритого ключа
	Своєчасно подавати центру сертифікації ключів інформацію про зміну даних, відображених у сертифікаті ключа

У ст. 13 Закону України “Про електронний підпис” указано умови, за яких скасовується, блокується посилений сертифікат ключа, а також умови, за яких його дія поновлюється.

Сформований посилений сертифікат ключа може бути негайно скасовано акредитованим центром сертифікації ключів.

Послуги блокування посиленого сертифіката ключа, крім акредитованого центру сертифікації ключів, надають Центральний засвідчувальний орган та засвідчувальний центр. Скасування блокування проводять усі перераховані вище органи.

Розглянемо умови, за яких скасовується, блокується посилений сертифікат ключа, а також умови, за яких його дія поновлюється (табл. 8.2).

Таблиця 8.2. Скасування, блокування та поновлення посиленого сертифіката ключа

Скасування	Блокування	Поновлення роботи
Закінчення строку чинності сертифіката ключа	—	—
Подання заяви власника ключа або його уповноваженого представника	У разі подання заяви власника ключа або його уповноваженого представника	У разі подання заяви власника ключа або його уповноваженого представника

Закінчення табл. 8.2

Скасування	Блокування	Поновлення роботи
Припинення діяльності юридичної особи — власника ключа	—	—
Смерть фізичної особи — власника ключа або оголошення його померлим за рішенням суду	За рішенням суду, що набрало законної сили	За рішенням суду, що набрало законної сили
Визнання власника ключа недієздатним за рішенням суду	—	—
Надання власником ключа недостовірних даних	—	—
Компрометація особистого ключа	У разі компрометації особистого ключа	У разі встановлення недостовірності даних про компрометацію особистого ключа

Скасування і блокування посиленого сертифіката ключа набуває чинності з моменту внесення до реєстру чинних, скасованих і блокованих посилених сертифікатів із зазначенням дати й часу виконання цієї операції.

Центральний засвідчувальний орган, засвідчувальний центр, акредитований центр сертифікації ключів негайно повідомляють власника про скасування або блокування посиленого сертифіката його ключа.

Визнання іноземних сертифікатів ключів

У Законі “Про електронний цифровий підпис” зазначено: “Якщо міжнародним договором, згода на обов’язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Законом, застосовуються правила міжнародного договору”.

Зокрема, у ст. 17 визначено, що іноземні сертифікати ключів, засвідчені відповідно до законодавства тих держав, де вони

видані, визнаються в Україні чинними у порядку, встановленому законом.

Українські стандарти електронного цифрового підпису

Реалізацію ідей, пов'язаних із застосуванням засобів захисту, забезпечують технічні стандарти, від вибору яких значно залежатимуть як захищеність, так і зручність системи в користуванні.

В Україні офіційно визнано 4 стандарти: один стандарт (шифрування) колишнього СРСР (ГОСТ 28147—89, який досі не опубліковано повністю, тобто не відкрито), два міждержавних (Азербайджан, Білорусь, Казахстан, Киргизія, Таджикистан, Росія, Туркменистан, Україна) стандарти — (ГОСТ 34.310—95, ГОСТ 34.311—95) і один стандарт України (ДСТУ 4145—2002).

Як доповнення до них затверджено наказом Департаменту спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України (ДСТСЗІ СБУ) Правила посиленої сертифікації від 31 січня 2005 р. № 3 (далі — Правила СБУ).

Стандарти, прийняті в Україні для електронного цифрового підпису (ЕЦП), мають свою особливість. Як відомо, для формування цифрового підпису створюється пара ключів — відкритий ключ для перевірки підпису і закритий (особистий) для накладення (створення) підпису. Ключі однієї пари нерозривно пов'язані, при цьому за відкритим ключем практично неможливо вирахувати закритий. Це дає змогу відкритий ключ віддавати всім охочим для перевірки підпису, а закритий потрібно зберігати в суворому секреті. Алгоритми цифрового підпису, прийняті в Україні, мають ще один ключовий елемент — так званий довгостроковий ключовий елемент (ДКЕ), який є невід'ємною частиною стандартів ЕЦП України, що забезпечує стійкість алгоритму до зламування. ДКЕ видає СБУ (користуючись закритою частиною ГОСТу 28147—89). А вже на основі цього ДКЕ генеруються ключі користувачів. Крім того, ДКЕ використовується під час накладення/перевірки ЕЦП. За нормативними вимогами СБУ довгостроковому ключовому елементу відводиться один рік життя, після чого ДКЕ треба знищувати й отримувати новий.

Під час застосування українських стандартів виникає низка питань. На рис. 8.3 зображено трьох користувачів, кожен з яких має свій закритий ключ підпису і сертифікат відкритого

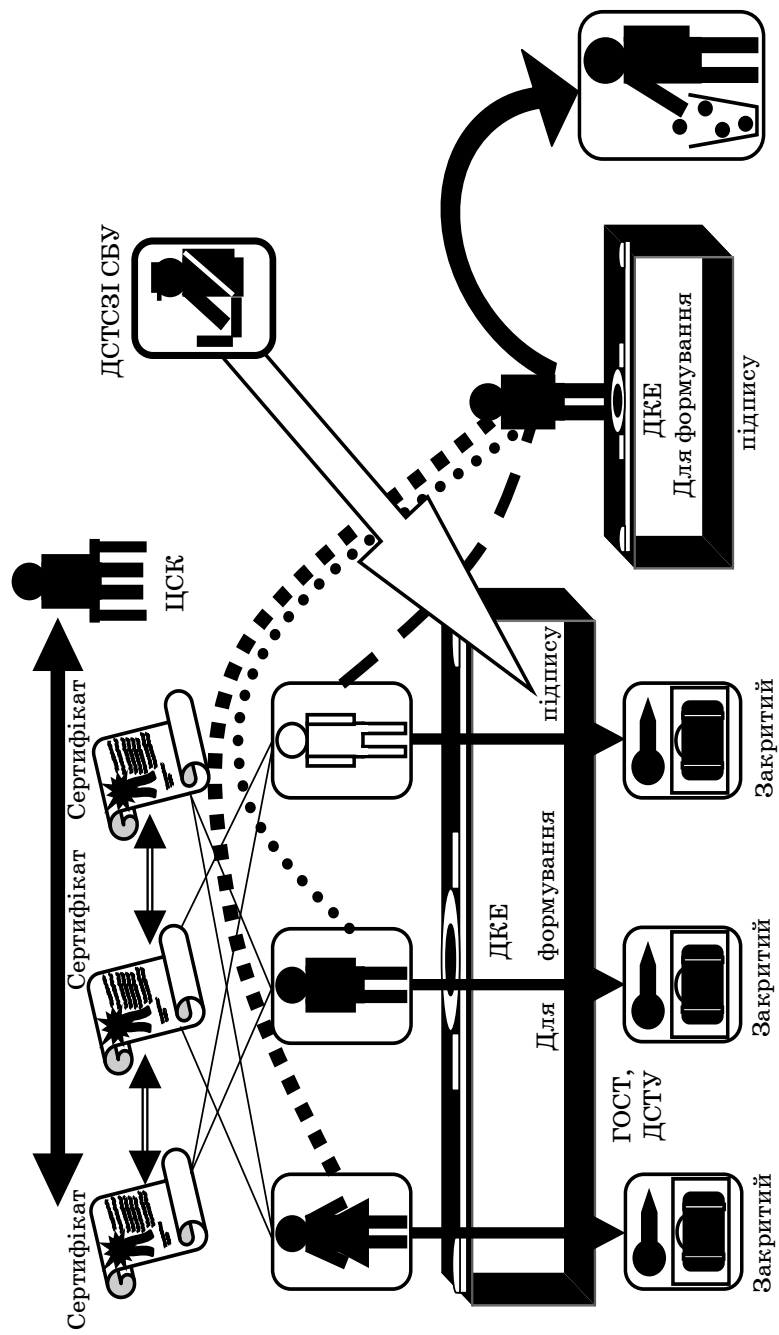


Рис. 8.3. Схема роботи з довгостроковим ключовим елементом

ключа, завірений деяким (не обов'язково одним і тим самим) центром сертифікації ключів. Чи зможуть зазначені особи обмінятися підписаними електронними документами? Не завжди. Річ у тому, що ДКЕ буває різним для різних організацій. Однак для того, щоб користувачі могли перевірити цифрові підписи один одного, крім сертифікатів своїх колег, вони мають також знати їхній ДКЕ.

За нормами, після року використання ДКЕ треба знищувати й отримувати новий. Але знищивши ДКЕ, неможливо перевірити підпис на електронних документах, створених з цим довгостроковим ключовим елементом. Отже, разом з ДКЕ фактично можна знищувати всі архіви електронних документів, тому що термін дії цих архівів дорівнює терміну зберігання ДКЕ.

В Євросоюзі проблема впровадження єдиних стандартів у сфері використання інформаційних послуг державного сектору стала предметом розгляду Європейської комісії у 2003 р. Щоб запобігти розриву європейського ринку у зв'язку з несумісністю електронних систем і стандартів, правил і методів використання інформаційних ресурсів державами-членами, Єврокомісія взяла курс на застосування відкритих стандартів, а також просування міжнародних. Йдеться про стандарти, складені міжнародними органами стандартизації (ISO, IEC, ITU). Міжнародні зобов'язання ЄС у цій сфері виражені в угоду COT щодо технічних бар'єрів для торгівлі, яка вимагає від сторін, щоб їхні стандарти і правила не створювали непотрібних перешкод для торгівлі та не були дискримінаційними.

У розвинених країнах секретних частин алгоритмів не існує, тому підпис, виданий в одній країні, легко читається (перевіряється) і може визнаватися в іншій. Алгоритми бувають різні, але вони пронумеровані, та кожний користувач знає, який алгоритм (відкритий) використовується.

В Україні ще не прийнято (офіційно визнано або рекомендовано) жодного з більш ніж 40 міжнародних стандартів і близько 40 стандартів ЄС, пов'язаних з інфраструктурою цифрового підпису. При цьому жоден з українських стандартів не визнано як європейський або міжнародний.

У зв'язку з тим, що українські стандарти електронного цифрового підпису не відповідають міжнародним, для електронного документообігу з держорганами необхідно застосовувати

ЕЦП, створений за державними стандартами, а для спілкування з міжнародними партнерами — за міжнародними.

Центральний засвідчувальний орган національної системи електронного цифрового підпису

Обов'язковим об'єктом технології ЕЦП є сертифікат ключа — документ в електронній або паперовій формі, необхідний для верифікації відкритого ключа — доказ того, що певна особа правомірно володіє відповідним особистим ключем.

Для управління сертифікатами в Україні створюється інфраструктура національної системи ЕЦП, елементами якої є центри сертифікації ключів та засвідчувальні центри. Головна складова в цій системі — центральний засвідчувальний орган (ЦЗО). Положення про ЦЗО затверджено Постановою Кабінету Міністрів України від 28 жовтня 2004 р. № 1451.

Як технічний організатор усієї системи ЕЦП в Україні ЦЗО реєструє центри сертифікації ключів та проводить їх акредитацію, а також формує кореневі сертифікати ключів.

Центральний засвідчувальний орган забезпечує юридично обґрунтовану та надійну реалізацію:

- електронних державних послуг (звітність перед державними органами, реєстраційні процедури тощо);
- електронного документообігу в органах державної влади;
- електронної комерції;
- електронного документообігу між комерційними організаціями;
- електронної взаємодії між банками та клієнтами.

Основні функції, обов'язки й права ЦЗО такі:

- реєстрація засвідчувальних центрів (ЗЦ) органів виконавчої влади та інших державних органів;
- акредитація ЗЦ і центрів сертифікації ключів (ЦСК);
- формування та видача сертифікатів ключів ЗЦ і ЦСК;
- ведення електронних реєстрів сертифікатів ключів ЗЦ і ЦСК;
- збереження сертифікатів ключів ЗЦ і ЦСК та забезпечення постійного доступу до них;
- надання ЗЦ і ЦСК консультацій з питань використання ЕЦП;
- внесення пропозицій щодо вдосконалення законодавства у сфері ЕЦП.

Наказом Міністерства транспорту та зв'язку від 1 грудня 2004 р. № 1055 функції ЦЗО делеговано Державному департаменту з питань зв'язку та інформатизації, а на Державне підприємство “Державний центр інформаційних ресурсів України” покладено технічне і технологічне забезпечення виконання функцій ЦЗО.

На базі Державного департаменту з питань зв'язку та інформатизації засновано технологічний центр ЦЗО, який складається з основного та резервного технологічних центрів (згідно із законодавством вони територіально відокремлені). Розроблено спеціалізоване програмне забезпечення, яким оснащено програмно-технічний комплекс технологічного центру ЦЗО, підготовлено нормативні, нормативно-правові й методичні документи, які регламентують діяльність ЦЗО та визначають вимоги до регламенту роботи центрів сертифікації ключів і ЗЦ органів державної влади.

Створено та відкрито web-сайт ЦЗО: <http://www.czo.gov.ua>.

Будову ЦЗО та взаємовідносин у системі електронного цифрового підпису ілюструє рис. 8.4.

Організаційно-правові основи діяльності центрів сертифікації ключів (ЦСК) з надання послуг ЕЦП регулюються Законом “Про електронний цифровий підпис”, який установлює правовий статус, права й обов'язки ЦСК. При цьому Законом уведено два типи ЦСК: власне ЦСК і акредитований ЦСК.

Для того щоб стати ЦСК, юридичній або фізичній особі — суб'єктові підприємницької діяльності — необхідно виконати низку організаційних, технічних і технологічних умов, зареєструватися в ЦЗО і далі виконувати регламентні вимоги та функції щодо надання послуг ЕЦП, які визначено законом. При цьому діяльність ЦСК щодо надання послуг ЕЦП не підлягає ліцензуванню.

Для підвищення рівня надійності, безпеки функціонування та якості надання послуг центрами сертифікації ключів Законом України “Про електронний цифровий підпис” уведено процедуру акредитації ЦСК. Аби одержати статус акредитованого, ЦСК має виконати низку додаткових організаційних, технічних і технологічних умов, визначених Кабінетом Міністрів України для таких центрів. При цьому зауважимо, що акредитація ЦСК є процедурою добровільною.

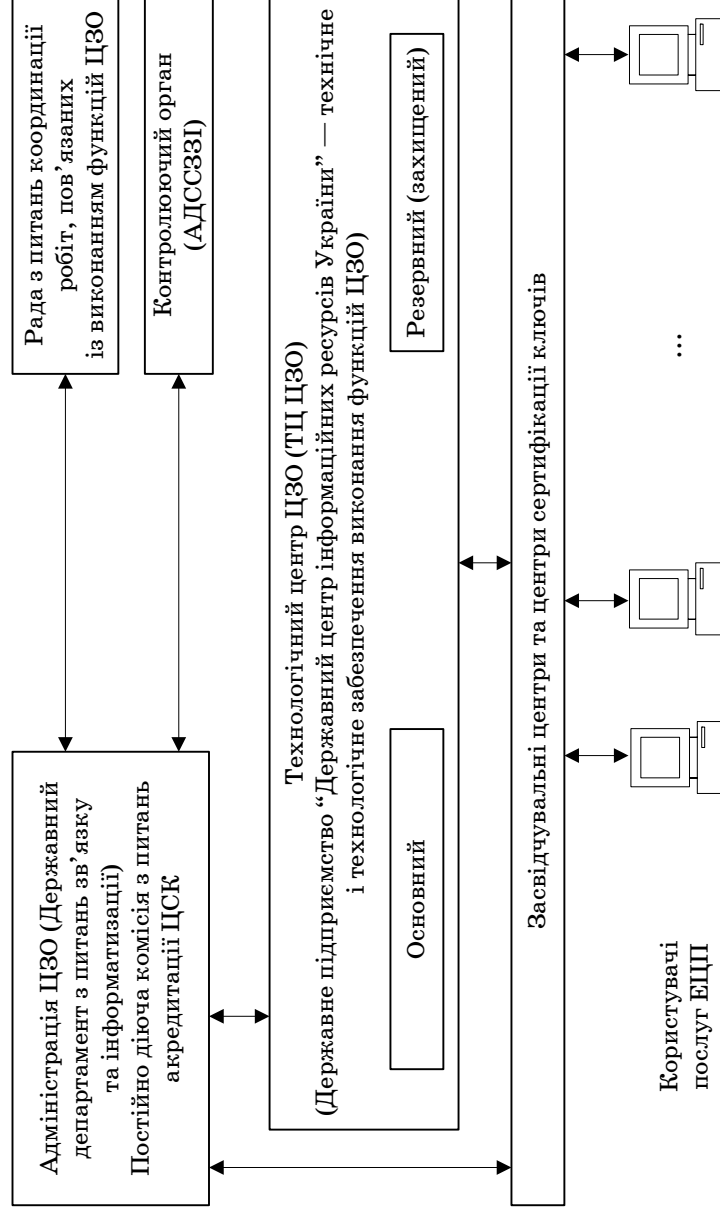


Рис. 8.4. Структура ЦЗО та взаємвідносини в системі електронного цифрового підпису

Які правові наслідки можливі для користувача — юридичної або фізичної особи, яка надає перевагу ЦСК чи акредитованому ЦСК?

Відповідно до Закону, якщо ЕЦП перевіряється з використанням сертифіката ключа, який має право формувати тільки акредитований ЦСК, а саме — посиленого сертифіката ключа, і виконується низка інших організаційних умов, то ЕЦП за правовим статусом автоматично прирівнюється до власноручного підпису.

Водночас згідно із законом ЕЦП не можна визнати недійсним, якщо він має електронну форму і не ґрунтується на посиленому сертифікаті ключа. Це означає, що коли використовуються послуги ЦСК (не акредитованого), то для того, щоб ЕЦП за правовим статусом прирівнювався до власноручного підпису, між суб'єктами електронної взаємодії має бути укладено договір у письмовій формі, котрий визначає умови визнання електронних цифрових підписів один одного, що ґрунтуються на послугах визначеного ЦСК. Крім цього, законом передбачено можливість застосування ЕЦП без використання послуг ЦСК — також на підставі договірних відносин.

Уведення інституту акредитованих ЦСК дає змогу забезпечити юридично значущий електронний документообіг між учасниками, не пов'язаними один з одним попередніми договорами в паперовому вигляді.

Фізичні та юридичні особи (щодо останніх йдеться про заміщення електронним цифровим підписом традиційної печатки) можуть використовувати ЕЦП за будь-якою з описаних схем.

Якщо електронний документообіг здійснюється державними органами, органами місцевого самоврядування, підприємствами, установами й організаціями державної форми власності або іншими юридичними та фізичними особами з державними установами, ЕЦП має застосовуватися з використанням послуг акредитованих ЦСК. Крім того, відповідно до Закону порядок застосування ЕЦП державними органами встановлюється Кабінетом Міністрів України.

Такий порядок визначається постановою Кабінету Міністрів України “Про затвердження Порядку застосування електронного цифрового підпису органами місцевого самоврядування,

підприємствами, установами та організаціями державної форми власності” від 28 жовтня 2004 р. № 1452.

Контролюючий орган відповідно до законодавства — це спеціально вповноважений центральний орган виконавчої влади у сфері криптографічного захисту інформації — Адміністрація державної служби спеціального зв'язку та захисту інформації (АДССЗЗІ). Він перевіряє виконання суб'єктами ЕЦП вимог законодавства у сфері ЕЦП. Крім цього, на АДССЗЗІ покладено проведення сертифікації та державної експертизи засобів ЕЦП, а також експертизи комплексної системи захисту інформації програмно-технічних комплексів ЦСК, що є одними з обов'язкових умов акредитації центрів.

Станом на 1 травня 2006 р. центри сертифікації ключів було створено на таких підприємствах:

- ДП УСС;
- ТОВ НВФ “Українські національні інформаційні системи (УНІС)”;
- ЗАТ “Інфраструктура відкритих ключів (ІВК)”.

Інфраструктура національної системи електронного цифрового підпису в Україні тільки починає створюватися. Тому згідно із завданнями національної програми інформатизації заплановано надалі вдосконалювати нормативно-правову і методичну бази, розробляти тарифну політику у сфері електронного цифрового підпису, маючи на меті забезпечувати ефективне та гарантоване державою функціонування національної системи електронного цифрового підпису, її динамічний розвиток і взаємодію із системами цифрового підпису інших країн.

8.4. Організаційне забезпечення електронного цифрового підпису

Організаційне забезпечення електронного цифрового підпису (ЕЦП) здійснюється відповідно до законодавства держави, на території якої використовується такий засіб ЕЦП. Якщо такого законодавства немає, правове регулювання в галузі застосування засобів ЕЦП здійснюється на основі нормативних актів адміністративних органів.

Необхідність сертифікації засобів ЕЦП

Засіб ЕЦП — це програмне і/чи апаратне забезпечення, призначене для генерації пари ключів (закритого й відкритого) та їх автоматизованого застосування під час шифрування або дешифрування електронного підпису. Оскільки від алгоритмів, на основі яких діє засіб ЕЦП, залежить надійність і стійкість документообігу, до засобів ЕЦП існують спеціальні вимоги.

Необхідність сертифікації відкритих ключів

Відкритий ключ тому й називається відкритим, що він доступний кожному з партнерів власника закритого ключа. Якщо в разі звертання від партнера *Oksanka* до партнера *Mary* потрібен захищений канал зв'язку, то партнер *Oksanka* може скористатися відкритим ключем партнера *Mary*. Тоді він може бути відносно впевнений, що в каналі зв'язку повідомлення не перехоплять. Але залишається відкритим питання, чи веде цей канал справді до партнера *Mary*? Є дуже простий прийом підміни відкритого ключа для створення помилкового каналу зв'язку. Припустимо, сторона *Arturo* бажає перехопити чужі дані. У цьому разі вона може за допомогою засобу ЕЦП створити собі пару ключів й опублікувати відкритий ключ нібито від імені партнера *Mary*. Тоді всі повідомлення від партнера *Oksanka* до партнера *Mary* перехоплюватимуться і читатимуться стороною *Arturo*, причому ні *Oksanka*, ні *Mary* навіть не здогадуватимуться про те, що *Arturo* бере участь у “договірних” відносинах.

Наведений приклад ілюструє лише найпростішу форму зложивання, бо хоча у відкритому ключі й наводяться дані про його власника, у ньому немає засобів, які засвідчують справжність цих даних. Без вирішення цього питання механізм ЕЦП не можна використовувати ні в електронній комерції, ні в електронному документообігу.

Значна частина державних законодавчих актів, що стосуються електронних цифрового підпису, комерції та документообігу, присвячена механізму посвідчення особи власника відкритого ключа. В усіх випадках цей механізм ґрунтується на тому, що вводиться (призначається) додаткова сторона, яка засвідчує належність відкритого ключа конкретній юридичній або фізичній особі.

Хто саме має право засвідчувати відкриті ключі, коли і як, у законодавствах різних держав вирішується по-різному. Зокрема, це може бути державний орган або організація, уповноважена державою для ведення такої діяльності. Можливо, що для внутрішнього документообігу підприємства цю функцію можна доручити особі, призначеній керівництвом, а для документообігу всередині відомства — уповноваженому підрозділу.

Поняття електронного сертифіката

На практиці сертифікація відкритих ключів виконується в такий спосіб.

1. Особа (юридична або фізична), що створила собі пару ключів (відкритий і закритий) за допомогою засобу ЕЦП, має звернутися в орган, уповноважений виконати сертифікацію. Цей орган називається *Центром сертифікації (Certification Authority, CA)*.

2. Центр сертифікації перевіряє належність відкритого ключа заявнику і засвідчує цей факт додаванням до відкритого ключа свого підпису, зашифрованого власним закритим ключем.

3. Будь-який партнер, що бажає вступити в контакт із власником відкритого ключа, може прочитати засвідчувальний запис за допомогою відкритого ключа центру сертифікації. Якщо цілісність цього запису не порушена і він довіряє центру сертифікації, то може використовувати відкритий ключ партнера для зв'язку з ним.

Слід звернути увагу, що центр сертифікації завіряє тільки факт належності відкритого ключа конкретній особі чи організації. У літературі існують некоректні твердження про те, що центр сертифікації нібито завіряє сумлінність власника відкритого ключа. Насправді, сертифікація відкритого ключа не стосується сумлінності, платоспроможності, ретельності й будь-яких інших ділових якостей його власника. Приклад — загальногромадянський паспорт. Це засіб посвідчення тільки особи його власника. Паспорт не може і не має містити якінебудь дані, що характеризують свого власника. Для цього є інші засоби. Наявність повноцінного сертифіката відкритого ключа говорить про те, що ключ можна використовувати для

посвідчення особи партнера. Але доцільність цих відносин центром сертифікації не засвідчується.

Дві моделі системи сертифікації

Розглянемо питання довіри до сертифікаційного органу. Якщо, наприклад, у рамках одного міністерства є свій центр сертифікації, то, швидше за все, є й наказ міністра, що дає змогу довіряти сертифікатам, підписаним цим центром. Те саме можна сказати й про інші міністерства. Але що робити, якщо виникають договірні відносини між підрозділами, які належать до різних відомств між державними і недержавними структурами? У цьому разі необхідна певна система органів сертифікації, що утворює структуру.

Є дві структурні моделі системи сертифікації, перша з яких централізована. Вона має ієрархічний характер і відповідає потребам службового документообігу. Друга модель — децентралізована (мережний характер), яка може використовуватися в цивільному електронному документообігу.

1. *Централізована система сертифікації. Кореневі та довірені центри.* Оскільки централізована модель сертифікації ієрархічна, її основою є один уповноважений орган сертифікації. Такий орган називається *кореневим центром сертифікації*.

Якщо кореневий центр суто технічно не може забезпечити усі запити на видачу й перевірку сертифікатів, що надходять від юридичних і фізичних осіб, то він може сертифікувати інші додаткові органи, що мають назву *довірених центрів сертифікації*.

Довірені центри також можуть засвідчувати чужі відкриті ключі своїми закритими ключами, але при цьому їхні відкриті ключі теж потребують засвідчення. Їх засвідчує своїм закритим ключем вищий центр сертифікації.

Таким чином, учасник електронного документообігу, що одержав звідкись відкритий ключ невідомого партнера, може:

- а) установити наявність сертифіката, засвідченого електронним підписом центру сертифікації;
- б) перевірити дійсність підпису центру сертифікації у вищому центрі сертифікації;
- в) якщо вищий центр також не кореневий, а довірений, то і його підпис можна перевірити у вищому центрі, і так далі, поки перевірка не дійде до кореневого центру сертифікації.

Розглянемо приклад. Нехай, в державі функції кореневого центру сертифікації покладено на Національний банк, але він не в змозі виконувати весь електронний документообіг країни, тому відкрив кілька довірених центрів сертифікації на базі уповноважених банків: “Бета-Банк”, “Гамма-Банк”, “Дельта-Банк” та ін. Припустімо, що “Бета-Банк”, авторитет якого в Дніпропетровській області дуже високий, відкрив на базі своєї місцевої філії довірений центр сертифікації в Дніпропетровську. У цьому разі юридичні й фізичні особи Дніпропетровської області можуть використовувати його сертифікати під час взаємодії. Однак коли їм доведеться взаємодіяти з партнером з Одеської області, той може висловити недовіру до електронного сертифіката, виданого Дніпропетровською філією “Бета-Банку”. У цьому разі він перевірить сертифікат самої філії за сертифікатом, виданим “Бета-Банком”. Якщо одеський партнер ніколи не мав справ з цим банком, то в нього може не викликати довіри і цей сертифікат. Тоді він перевірить сертифікат, виданий кореневим центром — Національним банком.

Таку перевірку треба виконати тільки один раз. Переконавшись у правомочності довіреного центру сертифікації, можна налаштувати своє програмне забезпечення так, щоб надалі довіра йому виражалася автоматично. І лише в тих випадках, коли ланцюжок сертифікатів не вдається простежити до раніше перевіреного довіреного центру (або кореневого), програмне забезпечення видасть попередження про те, що відкритий ключ не має засвідченого сертифіката і користуватися ним не можна. Сертифікат, вірогідність якого не можна простежити до кореневого центру сертифікації, не може викликати довіри.

2. Мережна модель сертифікації. Взаємна сертифікація. Структура системи сертифікації ЕЦП у державі визначається законом про електронний цифровий підпис. Якщо такого закону немає, то можуть діяти інші моделі системи сертифікації, що ґрунтуються на підзаконних актах або на взаємних домовленостях сторін, коли вони матимуть правове значення тільки за умови прямого відображення в обопільних угодах. Наприклад, за відсутності централізованої структури довірених центрів сертифікації (чи паралельно з нею, якщо закон це допускає) можуть діяти *мережні моделі сертифікації*. Такі моделі

охоплюють групи юридичних і фізичних осіб за відомчою чи, скажімо, картельною належністю.

Дві юридичні або фізичні особи, що вступають в електронні комерційні відносини, можуть самі взаємно завірити один одному відкриті ключі, якщо обмінюються ними під час особистої зустрічі з пред'явленням один одному установчих документів чи посвідчень особи (для фізичних осіб). У цьому разі в них немає підстав сумніватися в справжній належності відкритих ключів.

Однак електронна комерція будується на тому, що її учасники не потребують очної зустрічі. Дві сторони можуть домовитися про те, що їм взаємно завірить ключі третя сторона, яку вони виберуть самі. Так само можуть домовитися й інші учасники ринку. У результаті утворюється складна структура, де всі учасники, з одного боку, пов'язані двосторонніми договірними відносинами, а з іншого — ще й виконують функції завірительів для своїх традиційних партнерів. Довіра до відкритого ключа комерсанта буде вищою, якщо він одержить якомога більшу кількість сертифікатів від інших учасників ринку.

Наприклад, припустімо, клієнту *Oksanka* доводиться регулярно купувати папір для письма у постачальника *Mary* і дотепер проблем у їхніх відносинах не було, незважаючи на те, що електронний підпис постачальника ніким не сертифіковано. У цьому разі можна говорити про те, що клієнт *Oksanka* сам сертифікував для себе відкритий ключ свого партнера *Mary*, виразивши йому *повну* довіру. Це можливо, якщо партнери зустрілися особисто й обмінялися відкритими ключами “з рук у руки”.

Нехай в клієнта *Oksanka* виникла потреба придбати картридж для лазерного принтера. За допомогою електронних засобів зв'язку він звертається до постачальника *Arturo*, одержує від нього відкритий ключ і бачить, що цей ключ має сертифікат компанії *Mary* з *повною* довірою. У цьому випадку *Oksanka* може припустити, що *Mary* й *Arturo* колись теж зустрічалися особисто і взаємно сертифікували один одному відкриті ключі. Отже, виникає ситуація, за якої *Oksanka* теж може довіряти ключеві *Arturo*, хоча ця довіра і не повна (адже вони не зустрічалися), а *обмежена*.

Чи може в цьому разі клієнт *Oksanka* відправляти постачальникові *Arturo* свої конфіденційні дані, зашифрувавши їх його відкритим ключем? Це вирішує сам клієнт. Чим більше серед сертифікатів ключа *Arturo* буде таких, котрі видані партнерами, відомими клієнтові *Oksanka*, тим більше довіри до ключа *Arturo*. Далі *Oksanka* може на свій розсуд налаштувати своє програмне забезпечення. Наприклад, можна зробити так, щоб два чи три сертифікати з обмеженою довірою розглядалися як один сертифікат з повною.

Так працює мережна модель сертифікації. Вона пов'язує групу учасників, що перебувають у складній системі взаємин. Слід ще раз звернути увагу на те, що, взаємно сертифікуючи відкриті ключі, а отже, й електронні підписи один одного, ніхто не бере на себе відповідальність за ділову репутацію партнера. Йдеться тільки про те, що сторони або підтверджують факт належності відкритого ключа такому партнерові, або мають підставу на це покладатися. У першому випадку вони виражають *повну*, а в другому — *обмежену* довіру.

8.5. Технічне забезпечення режиму електронного цифрового підпису.

Поняття електронного цифрового підпису

Особливості рукописного підпису

Власноручний підпис під документом віддавна вважається доказом того, що людина, яка підписала цей документ, ознайомила з ним і згодна з його змістом. Тобто рукописний підпис є одним із засобів *ідентифікації* особи, в основу якого покладено гіпотезу про унікальність особистих біометричних параметрів людини. Чому ж підпис заслужив таку довіру? Основні причини такі:

- дійсність підпису можна перевірити (його наявність у документі дає змогу переконатися, чи справді він був підписаний людиною, що володіє правом ставити цей підпис);

- підпис не можна підробити (справжній підпис — доказ того, що саме та людина, якій він належить, поставила цей підпис під документом);

— підпис, що вже стоїть під одним документом, не може бути використаний ще раз для підписання іншого документа (підпис — невід’ємна частина документа і його не можна перенести в інший документ);

— підписаний документ не підлягає ніяким змінам;

— від підпису неможливо відректися (той, хто поставив підпис, не може згодом заявити, що він не підписував цей документ).

Насправді жодна з перерахованих властивостей підпису на всі 100 % не виконується. У нашому сучасному криміналізованому суспільстві підписи підробляють і копіюють, від них відрікаються, а в уже підписані документи вносять довільні зміни. Тобто застосування рукописного підпису не позбавлене недоліків:

— недостатній ступінь захисту (коли необхідна підвищена достовірність відомостей, що містяться у документі, використовують додаткові засоби захисту: наявність додаткових рукописних підписів, печатки юридичних осіб, засвідчення у нотаріуса, спеціальні бланки тощо);

— нерозривний фізичний зв’язок з матеріальним носієм (рукописний підпис можливий тільки на документах з матеріальною природою, тому особа, що підписує документ, має безпосередньо контактувати з матеріальним носієм цього документа);

— розбіжності між оригіналом та копіями, отриманими засобами копіювально-множильної техніки (копії не мають тієї юридичної сили, яку має оригінал документа);

— ніяким чином не забезпечує *аутентифікацію* документа, тобто його цілісність і незмінність (без додаткових засобів захисту рукописний підпис не гарантує незмінності вмісту документа під час його збереження або транспортування).

Особливості електронного цифрового підпису

Застосування глобальних комунікацій в економічній діяльності та повсякденному житті зумовило появу принципово нового виду відносин, пов’язаних з обміном інформацією без використання паперових носіїв, тобто за допомогою електронних документів. Під електронним документом мають на увазі документ, в якому інформацію подано в електронній формі та який містить необхідні реквізити (у тому числі електронний цифровий підпис).

Електронний цифровий підпис (ЕЦП) є реквізитом електронного документа і призначений для його захисту від підробки. ЕЦП має не фізичну, а логічну природу. Під час побудови цифрового підпису замість звичайного зв'язку між печаткою або рукописним підписом та аркушем паперу простежується складна залежність між документом в електронному вигляді, секретним і загальнодоступним (відкритим) ключами, а також цифровим підписом. Складність підробки ЕЦП зумовлена дуже великим обсягом математичних обчислень.

ЕЦП може мати цілком “буквений” вигляд, але частіше він поданий у вигляді послідовності довільних символів. Цифровий підпис може зберігатися разом з документом, наприклад, стояти на його початку, в кінці або в окремому файлі (природно, що в останньому випадку, перевіряючи підпис, необхідно мати у своєму розпорядженні як сам документ, так і файл, що містить підпис).

Електронний цифровий підпис — це засіб, що дає змогу на основі використання криптографічних методів визначити авторство і дійсність документа. При цьому електронний цифровий підпис має такі переваги:

- дематеріалізація документів (незалежність ЕЦП від носія дає можливість використовувати його в електронному документообігу й установлювати договірні взаємовідносини без безпосереднього контакту між фізичними або юридичними особами);

- рівнозначність копій (логічна природа ЕЦП дає змогу не розрізняти копії одного документа та зробити їх рівнозначними);

- додаткова функціональність: в основі механізму ЕЦП лежить криптографія, тому ЕЦП є не тільки засобом ідентифікації, а й засобом аутентифікації документа (в електронний документ, підписаний ЕЦП, не можна внести зміни, не порушивши підпису);

- автоматизація (створення, застосування, засвідчення та перевірка ЕЦП виконується із застосуванням програмних та апаратних засобів обчислювальної техніки, тому добре автоматизується);

- порівнянність захисних властивостей (об'єктивна оцінка сертифікованих програмних та апаратних засобів обчислюваль-

ної техніки, призначених для створення ЕЦП (далі — засобів ЕЦП), базується на чіткому математичному аналізі, а не на гіпотезі про унікальність біометричних параметрів людини);

— масштабованість (виходячи з оцінки захисних властивостей ЕЦП, у цивільному документообігу можна використовувати найпростіші засоби ЕЦП, у службовому — сертифіковані для секретної інформації — спеціальні засоби ЕЦП).

Усі наведені властивості ЕЦП широко використовуються в електронній комерції. Однак у використанні ЕЦП є й недоліки. Хоча електронний документообіг з електронним підписом сприяє підвищенню продуктивності праці, але виводить механізм підпису з-під контролю звичайними методами (візуальними) та може створювати ілюзію благополуччя. Тому для використання ЕЦП необхідне спеціальне технічне, організаційне та правове забезпечення.

Криптографічні основи застосування електронного цифрового підпису

У подальшому застосування електронного цифрового підпису розглядатиметься в договірних відносинах між віддаленими сторонами, що не мають між собою прямого або опосередкованого контакту через матеріальні носії інформації. Цей випадок найбільш загальний і відповідає двом основним моделям електронної комерції, що розвиваються сьогодні: *Виробник — Виробник* і *Виробник — Споживач*.

Важливою проблемою договірних відносин, що відбуваються в електронній формі, є можливість відмови (*repudiation*) однієї зі сторін від умов угоди і/чи свого підпису. З неї випливає потреба в засобах об'єктивної ідентифікації партнерів. Якщо таких засобів немає або вони недосконалі, договірні сторони одержують можливість відмови від своїх зобов'язань, що впливають з умов договору.

Важливо мати на увазі, що за такими відмовами не обов'язково стоїть злий намір. Відмова цілком виправдана, якщо партнер установив зловживання своїми реквізитами з боку неуповноважених осіб чи факт одностороннього внесення змін у зміст договору. Такі події можливі як з боку кожного з партнерів, так і на шляхах транспортування.

Для спрощення технічної сторони питання слід перейти від використання понять *договір* і *документ* до поняття *повідом-*

лення. Це дає змогу формально підійти до розгляду документів зважаючи тільки на *зміст повідомлення*. Такий методологічний прийом характерний для інформатики. Далі ми будемо розглядати документи як *унікальні послідовності символів*. Вимога унікальності пов'язана з тим, що, коли хоча б один символ у послідовності буде якось змінено, це буде вже зовсім інший документ, не адекватний вихідному.

Ще одне припущення, яке слід зробити, стосується способу транспортування повідомлення. Будь-які види транспортування: звичайна кур'єрська, електронна або інша пошта — замінимо терміном *канал зв'язку*.

Для того щоб послідовність символів, тобто повідомлення, могло однозначно ідентифікувати її автора, необхідно, аби воно мало унікальні ознаки, відомі тільки його відправнику й одержувачу. З незапам'ятних часів це досягається застосуванням засобів шифрування (більш загальний термін — *криптографія*). Якщо обидві сторони використовують той самий метод шифрування повідомлень, відомий тільки їм, то можна сказати, що вони *спілкуються в захищеному каналі*, де кожна зі сторін матиме відносну впевненість у тому, що:

— автором повідомлення справді є партнер (*ідентифікація партнера*);

— повідомлення не було змінено в каналі зв'язку (*ауθενфікація повідомлення*).

Ця впевненість відносна, тому що стороннім особам можуть стати відомі метод шифрування і його ключ.

Метод і ключ шифрування

Метод шифрування — це формальний алгоритм, що описує порядок перетворення вихідного повідомлення в результат. **Ключ шифрування** — набір параметрів (даних), необхідних для застосування методу. Є безліч методів (алгоритмів) шифрування. За історичними джерелами, Юлій Цезар для зв'язку зі своїми воєначальниками використовував метод підстановки з ключем, що дорівнював 3. У вихідному повідомленні кожен символ заміщався іншим, віддаленим від нього в алфавіті на 3 позиції

$$A = D \quad B = E \quad C = F \text{ та ін.}$$

Такий метод, як і ключ шифрування, дуже простий, тому на його захищеність можна розраховувати тільки тоді, коли канал обслуговують особи (посильні), які не мають елементарної грамотності. Трохи підвищити захист можна, якщо використовувати довший ключ шифрування, наприклад: 3—5—7. У цьому випадку перший символ повідомлення зміщується на три позиції, другий — на п'ять, третій — на сім позицій, після чого процес циклічно повторюється. Послідовність символів ключа можна розглядати як *ключове слово*. Якщо ключ містить кілька ключових слів, його називають *ключовою фразою*.

Коли той самий ключ використовується багаторазово для роботи з різними повідомленнями, його називають *статичним*, а якщо для кожного повідомлення використовується новий ключ, то — *динамічним*. У цьому випадку повідомлення має нести зашифровану інформацію про те, який ключ з відомого набору було у ньому використано.

Симетричні та несиметричні методи шифрування

Розглянутий вище метод підстановки — класичний приклад *симетричного шифрування*. Симетричність полягає в тому, що обидві сторони використовують той самий ключ. Яким ключем повідомлення шифрувалося, тим воно і дешифрується. Тому цей ключ секретний. Перевагою симетричних методів шифрування є їх достатня теоретична вивченість та висока криптостійкість, тому вони можуть використовуватися для впевненої аутентифікації повідомлень. До основних недоліків цих методів слід зарахувати додаткові заходи таємності під час поширення ключів і пов'язані з цим проблеми, можливі витрати, а також той факт, що методи з секретним ключем працюють тільки в умовах повної довіри партнерів один до одного.

Таким чином, для електронної комерції традиційні методи шифрування, що базуються на симетричних ключах, застосовувати незручно.

Лише в останні три десятиліття з'явилися й набули розвитку нові методи, що одержали назву *методів несиметричної криптографії*. Несиметрична криптографія використовує спеціальні математичні методи, розроблені в результаті розвитку нових галузей математики. На цих методах ґрунтується електронна комерція взагалі та програмні засоби, які отримали назву *засоби ЕЦП*. Після застосування одного з таких засобів

утворюється пара взаємозалежних ключів, що мають унікальну властивість: *те, що зашифровано одним ключем, може бути дешифровано тільки іншим, і навпаки*. Власник пари ключів може залишити один ключ собі, а інший — поширити (опублікувати). Публікація відкритого ключа відбувається прямим розсиланням через незахищений канал, наприклад, електронною поштою. Зручніше виставити відкритий ключ на своєму (або орендованому) web-сервері, де його зможе одержати кожен бажаючий. Ключ, залишений для себе, називається *закритим*, або *особистим ключем (private)*, а опублікований ключ — *відкритим*, або *публічним (public)*.

Повідомлення (замовлення, договори тощо), котрі надсилаються власникові ключової пари, шифруються його відкритим ключем, а дешифруються за допомогою закритого. Якщо власник ключової пари захоче звернутися з повідомленням до своїх клієнтів, він зашифрує його закритим ключем, а одержувачі прочитають його за допомогою відповідного відкритого ключа.

Застосування несиметричних методів шифрування надає такі можливості.

Використання закритого ключа дає змогу ідентифікувати відправника. Під час використання несиметричного шифрування досягається можливість ідентифікації відправника. Якщо клієнт звернувся із замовленням до фірми *МКС*, що торгує програмними засобами, й одержав у відповідь зашифрований файл, то він може застосувати до нього відкритий ключ фірми. Якщо цей файл направила йому не фірма *МКС*, а невідома особа, то ключ не підійде, повідомлення не буде дешифровано і шкідливі наслідки від використання невідомого програмного забезпечення не настануть.

Використання відкритого ключа дає можливість аутентифікувати повідомлення. Якщо клієнт фірми *МКС* разом із замовленням указує конфіденційні дані, наприклад, про свою платіжну карту, то він може бути впевнений у тому, що ніхто сторонній цю інформацію не прочитає, тому що повідомлення, зашифроване відкритим ключем, може прочитати тільки власник закритого ключа.

Обмін відкритими ключами між партнерами уможливорює створення ними спрямованого каналу зв'язку між собою. Якщо два партнери, які ніколи раніше не зустрічалися, бажають почати листування, вони можуть зробити це, обмінявшись своїми

відкритими ключами. Тоді кожний з них відправлятиме своє повідомлення, зашифрувавши його своїм закритим ключем, а партнер читатиме його відповідним відкритим ключем. При цьому одержувач повідомлення може бути впевнений у тому, що одержав листа від партнера, а не від особи, що побажала залишитися невідомою.

Подвійне послідовне шифрування спочатку своїм особистим ключем, потім відкритим ключем іншої сторони дає змогу партнерам створити захищений спрямований канал зв'язку. У попередній схемі шифрування використовується не для захисту інформації, що міститься в повідомленні, а тільки для ідентифікації відправника. Можна поєднати обидві ці функції. Для цього відправник мусить застосувати до повідомлення два ключі. Спочатку він шифрує повідомлення своїм закритим ключем, а потім те, що вийде, шифрується відкритим ключем одержувача. Той діє в зворотному порядку. Спочатку він дешифрує повідомлення своїм закритим ключем і робить його таким, що можна прочитати; потім дешифрує повідомлення відкритим ключем відправника і переконується в особі того, хто надіслав цей лист.

Найпростіша структура ЕЦП

У найпростішому вигляді електронний цифровий підпис — це деякі відомості про себе, наприклад, прізвище, ім'я, по батькові та посада, зашифровані особистим ключем. Кожен, хто має відкритий ключ, зможе ці відомості прочитати і переконатися, хто є автором повідомлення. Таким чином, у найпростішому розумінні **ЕЦП** — це засіб ідентифікації відправника. Однак на практиці в ЕЦП включають не тільки відомості про відправника, а й додаткові дані.

Поняття про компрометацію ЕЦП

ЕЦП як засіб ідентифікації партнера більш надійний, ніж традиційний рукописний підпис. Однак і його можна фальсифікувати. Це може статися, коли зловмисник у той чи інший спосіб одержить доступ до закритого ключа. Тоді говорять про компрометацію закритого ключа, з якої випливає компрометація електронного підпису, створеного з його допомогою.

Закритий ключ може бути скомпрометовано традиційними і нетрадиційними способами.

Традиційні способи компрометації, як правило, пов'язані з протизаконними діями:

- викрадення ключа шляхом копіювання в результаті не-санкціонованого прямого фізичного або віддаленого мережного доступу до устаткування, на якому він зберігається;
- одержання ключа в результаті відповіді на запит, виконаний з ознаками шахрайства чи підробки;
- викрадення ключа разом з устаткуванням, на якому він зберігався (навіть, якщо викрадення устаткування здійснюється не для доступу до ключа);
- викрадення ключа в результаті змови з особами, що мають право на його використання (навіть факт звільнення співробітника, який мав доступ до закритого ключа організації, теж розглядається як компрометація ключа).

Незаконність традиційних методів компрометації ключа дає змогу деякою мірою розраховувати на те, що захист ключа, хоча й опосередковано, забезпечує законодавство. На жаль, це не стосується *нетрадиційних способів компрометації*, що базуються на реконструкції закритого ключа за вихідними даними, отриманими легально, зокрема за відкритим ключем. Зараз довести незаконність дій щодо реконструкції чужого закритого ключа практично неможливо (принаймні поки не відбудеться подія незаконного використання реконструйованого ключа).

Передумови можливої реконструкції такі:

- реконструктор має легальний доступ до відкритого ключа, а він, як відомо, пов'язаний із закритим ключем певними математичними співвідношеннями, оскільки разом вони утворюють ключову пару;
- він може експериментувати не на випадкових, а на спеціально підібраних повідомленнях, підготовлених власноручно так, як йому зручно;
- він має повний доступ до зашифрованих повідомлень, оскільки сам може створити їх за допомогою відкритого ключа;
- йому відомий метод шифрування і дешифрування, за яким працює програмний засіб ЕЦП (у загальному випадку алгоритм не ховається, а навпаки, широко публікується для загального тестування).

Криптостійкість засобів ЕЦП

Теоретично знання методу шифрування, відкритої половини ключа, вихідного і зашифрованого текстів дають зловмис-

никові повну можливість реконструкції закритого ключа. На практиці процес реконструкції стикається з наявністю спеціальних апаратних і програмних засобів, а також з величезними витратами обчислювального часу.

Окрім криптографії, є *криптоаналіз* — наука про методи розкриття і/або підробки даних. Вона розробляє методи, що дають змогу:

- відтворювати зашифровану інформацію, тобто знімати з неї захист;

- оцінювати якість захисту інформації, тобто давати об'єктивну оцінку прийнятим методам захисту.

Під час використання криптографії якість захисту визначається одночасно як методами, так і даними. Метод у цьому разі закладено в алгоритмі шифрування. Дані полягають у вихідному повідомленні та в ключі шифрування. Зашифроване повідомлення може слабо протистояти методам криптоаналізу з двох причин: у зв'язку із “слабкістю” алгоритму, що лежить в основі дії засобу ЕЦП, та характерними рисами ключа (невдалі властивості ключової пари).

До проблеми оцінки криптостійкості алгоритмів є два підходи. Перший — *централізований*, ґрунтується на закритості алгоритмів шифрування, і другий — *децентралізований*, базується на їх відкритості.

За централізованого підходу відповідальність за надійність засобів шифрування взагалі та засобів ЕЦП зокрема бере на себе держава в особі органу, уповноваженого розробляти засоби ЕЦП або давати оцінку засобам, виконаним іншими розробниками. У цьому разі захист може ґрунтуватися на “закритості” алгоритму.

З погляду держави, це найпростіший, найдешевший і легко контрольований шлях. Уповноважений адміністративний орган може зробити секретним алгоритм, що рекомендується до загального застосування, а використання інших алгоритмів законодавчо заборонити. Це, звичайно, ускладнить реконструкцію закритих ключів і підробку ЕЦП, але багато споживачів так і не знатимуть про справжні властивості захисту запропонованого (“нав’язаного”) алгоритму. Їм залишиться тільки довіряти адміністративному органу, що запевняє у надійності алгоритму.

У разі децентралізації алгоритм шифрування робиться відкритим. Він широко публікується і кожен може самостійно перевірити його криптостійкість. Зрозуміло, звичайний користувач не стане цього робити, але він може бути впевненим у тому, що безліч фахівців, озброєних і належною технікою, і належними методами, активно цим займаються. Якщо вони неспроможні що-небудь зробити, то на цьому етапі розвитку технології алгоритм можна вважати надійним: йому можна довіряти, поки у відкритій пресі не з'являться повідомлення про його спростування.

На практиці водночас у різних сферах можуть застосовуватися різні підходи. Одна справа — захист цивільної електронної пошти, інша — службовий і фінансовий документообіг підприємств і, нарешті, зовсім інша справа — спецзасоби, що використовуються там, де є загроза безпеці держави.

На криптостійкість ЕЦП впливають також властивості пари ключів. Ключі створюються в результаті застосування *засобу ЕЦП* — програмного чи апаратного забезпечення, що генерує пару ключів за запитом користувача. В основі цього засобу також лежить деякий алгоритм. Є кілька різновидів алгоритмів, за допомогою яких створюються пари ключів, однак не всі вони мають однакові властивості. Деякі, на перший погляд, бездоганні алгоритми можуть не завжди генерувати повноцінні криптостійкі ключі, причому користувач, що створив собі пару ключів за допомогою придбаного ним засобу ЕЦП, ніколи не довідається про дефекти ключа, поки не зазнає збитку внаслідок незаконного використання його ЕЦП чи втрати важливих даних.

На державному рівні можливі два підходи до забезпечення стійкості ключів, що перебувають в обігу. *По-перше*, можлива сертифікація засобів ЕЦП уповноваженим органом. У цьому разі засоби ЕЦП, що не пройшли експертизу, не одержують відповідного сертифіката і забороняються до застосування. Недолік цього методу в тому, що подібна сертифікація пов'язана зі значними витратами фінансів і часу. Не кожен розробник засобів ЕЦП має можливість вкласти необхідні кошти в їх сертифікацію. Проте це страхує суспільство від використання засобів ЕЦП, виконаних некваліфікованими кадрами.

Другий підхід може полягати в сертифікації не засобів ЕЦП, а конкретних ключів, створених з їх допомогою. У такому разі пару ключів (закритий і відкритий) потрібно подавати органу, що виконує сертифікацію. Він приймає рішення з огляду як на відносну криптостійкість ключів, так і на характер діяльності заявника. Те, що допустиме для малого торговельного підприємства, може бути неприйнятним для банківської структури. Недоліком такого підходу є наявність копій закритих ключів у державному органі, де їх захист від неправомочного використання (чи втрати) сумнівний.

Можливі й комбіновані рішення, що поєднують сертифікацію засобів ЕЦП з сертифікацією ключів.

Вплив розміру ключів на їх криптостійкість

Цікаво, що чим досконалішими стають системи шифрування і пов'язані з ними засоби ЕЦП, тим рідше з'являються повідомлення про незаперечні шифри та "абсолютні захисти". Чим вища криптографічна культура суспільства, тим очевидніший факт, що абсолютних засобів захисту немає, і питання зняття будь-якого захисту зводиться лише до питання про технічні засоби, що використовуються, витрати часу й економічної доцільності.

Початкових даних для реконструкції закритого ключа більше ніж досить. Якщо важко знайти оригінальні методи, що ґрунтуються на криптоаналізі, можна скористатися методом простого перебирання, який завжди веде до розв'язування завдання, хоча заздалегідь невідомо, коли це відбудеться. Тривалість реконструкції визначається, по-перше, продуктивністю використовуваної обчислювальної техніки, а по-друге, розміром ключа.

Розмір ключа вимірюється в бітах (двійкових розрядах). Чим він більший, тим, відповідно, більше часу потрібно на перебирання можливих значень, тим довше працює алгоритм. Тому вибір оптимальної довжини ключа — це питання балансу. Знов-таки воно вирішується по-різному залежно від характеру діяльності організації (табл. 8.3). Те, що необхідне для цивільного листування, не підходить для банківських організацій і тим більше не може бути застосовано в діяльності служб, пов'язаних з державною безпекою.

Таблиця 8.3. Мінімальні розміри ключів для різних типів інформації

Різновид інформації	Термін таємності	Довжина ключа, біт
Військова тактична	Хвилини, години	56
Оголошення про випуск нової продукції	Дні тижня	56—64
Промислові таємниці	Місяці	64
Секрет водневої бомби	Більше 40 років	128
Досьє секретних агентів	Більше 50 років	128
Приватна	Більше 50 років	128
Дипломатична	Більше 65 років	128 (не менше)

Криптостійкість *симетричних* ключів оцінюється просто. Наприклад, якщо довжина симетричного ключа становить 40 біт (таке шифрування називають *слабким*), то для його реконструкції треба перебрати 2^{40} чисел. Використовуючи для цього декілька сучасних передових комп'ютерів, задачу можна розв'язати швидше, ніж за добу. Це недешевий, але цілком можливий захід. Якщо довжина ключа становить 64 біти, то необхідно мати мережу з кількох десятків спеціалізованих комп'ютерів, і задача розв'язується протягом кількох тижнів. Це вкрай дорогий захід, але технічно він можливий за сучасного рівня розвитку техніки. *Сильним* називають шифрування з довжиною симетричного ключа 128 біт. На будь-якому сучасному устаткуванні реконструкція такого ключа займає часу в мільйони разів більше, ніж вік Всесвіту. Це технічно неможливий захід, якщо немає яких-небудь додаткових даних, наприклад, відомостей про характерні налаштування засобу ЕЦП, що використовувався під час генерації ключа. Теоретично такі дані у "зломщика" можуть бути (наприклад, отримані агентурними методами), і тоді реконструкція навіть сильного ключа стане технічно можливою.

Для ключів несиметричного шифрування одержати таку просту формулу, як для симетричних ключів, зазвичай не вдається. Алгоритми несиметричного шифрування ще не до кінця

вивчено. Тому під час використання несиметричного шифрування говорять про **відносну криптостійкість** ключів. Зрозуміло, що їх криптостійкість, як і для симетричних ключів, залежить від довжини (табл. 8.4), але виразити це співвідношення простою формулою для більшості алгоритмів поки що не вдалося. Звичайно відносну криптостійкість оцінюють за емпіричними даними, отриманими дослідним шляхом.

Таблиця 8.4. Довжина симетричного і несиметричного ключів за однакового рівня безпеки, біт

Симетричний ключ	Несиметричний ключ
56	384
64	512
128	2304

Підсумки багатовікового протистояння розробника шифру — криптограми, і його опонента — криптоаналітика, підбив голландець **Керкхгофф** (1835—1903), який сформулював правила цього протистояння. Основне з них полягає в тому, що під час розробки і застосування шифру треба зважати на те, що весь механізм шифрування, множина правил чи алгоритмів рано або пізно стає відомою опонентові, а стійкість шифру визначається тільки таємністю ключа, яка, у свою чергу, визначається його довжиною.

Принцип достатності захисту

Теоретична оцінка трудомісткості реконструкції дуже довгих несиметричних ключів показує неможливість розв’язання цього завдання в розумний термін, проте не слід розглядати це як привід для зайвого самозаспокоєння.

З часом може бути виявлено які-небудь нові властивості алгоритмів несиметричного шифрування, що спрощують реконструкцію закритого ключа. Змінюється і рівень розвитку техніки, і середній рівень продуктивності комп’ютерів. Тому в основі використання засобів ЕЦП лежить базовий принцип **достатності шифрування**, відповідно до якого:

- ніякі засоби шифрування не вважаються абсолютними;
- повідомлення вважається досить захищеним, якщо для його реконструкції необхідні матеріальні витрати, які значно перевищують цінність інформації, що є в повідомленні;
- захист повідомлення, що вважається достатнім для сучасного стану науки і техніки, може виявитися недостатнім у найближчому майбутньому.

Таким чином, в основі принципу достатності захисту лежить принцип економічної доцільності.

Поняття про дайджест повідомлення. Електронна печатка. Хеш-функція

Дотепер ми вважали, що електронний підпис містить інформацію про автора, зашифровану за допомогою його закритого ключа. Це дає змогу власнику відкритого ключа переконатися в тому, що автором повідомлення є та особа, від імені якої воно надійшло. Разом з тим є технічна можливість включити до складу ЕЦП і дані, що характеризують саме повідомлення, щоб виключити ймовірність внесення в нього змін під час передачі каналами зв'язку. Для цього використовується поняття дайджесту повідомлення.

Дайджест повідомлення — це унікальна послідовність символів, що однозначно відповідає змісту повідомлення. Зазвичай дайджест має фіксований розмір, наприклад, 128 або 168 біт, що не залежить від довжини самого повідомлення. Дайджест вводиться до складу ЕЦП з відомостями про автора і шифрується разом з ними.

Найпростіший прийом створення дайджесту можна розглянути на прикладі контрольної суми. Оскільки кожен символ повідомлення становить числовий код (наприклад, за таблицею *ASCII*), то можна підсумувати всі коди послідовності й визначити числовий параметр, що відповідає такому повідомленню, назовемо його *контрольною сумою*. Передбачається, що у разі зміни змісту повідомлення в каналі зв'язку зміниться і контрольна сума, що буде встановлено приймаючою стороною. Про справжню контрольну суму вона довідається з підпису і, порівнявши їх, знайде стороннє втручання. Однак такий механізм не можна вважати задовільним, оскільки в ньому немає одно-

значної відповідності між текстом повідомлення і величиною контрольної суми. За належного старання можна виконати ряд взаємозалежних змін у повідомленні, за яких контрольна сума не зміниться. Є й інші механізми обчислення контрольних сум, але вони не можуть вважатися прийнятними. Їхній основний недолік полягає в *оборотності*. Можна запропонувати алгоритм, що дасть змогу за відомою контрольною сумою створити нове повідомлення, яке відрізнятиметься від вихідного, але матиме таку саму контрольну суму.

Сучасній математиці відомі спеціальні функції, що не мають властивості оборотності. Вони дають можливість з однієї послідовності чисел (з одного повідомлення) одержати іншу (інше повідомлення) таким чином, що зворотне перетворення буде неможливим. Такі функції використовують у криптографії і називають *хеш-функціями*.

З принципом дії хеш-функцій зручно познайомитися на прикладі того, як на комп'ютерах організовано зберігання паролів. *Пароль* — це секретна послідовність символів, які клієнт має повідомити системі, щоб вона почала його обслуговувати. Перевірку паролів виконують шляхом їх порівняння з деякими контрольними записами, але в цьому випадку ми мали б припустити, що десь у системі зберігаються справжні паролі всіх її зареєстрованих клієнтів. Це зовсім неприйнятно з погляду безпеки. Насправді справжні паролі клієнтів спочатку обробляються хеш-функцією і тільки після такого шифрування закладаються на зберігання. Викрадені зашифровані паролі не стануть корисними зловмисникові, оскільки хеш-функція не-оборотна і реконструювати справжній пароль за його хеш-кодом — занадто складне завдання. Коли до системи підключається законний користувач і вводить свій пароль, то цей пароль теж обробляється хеш-функцією, після чого отриманий хеш-код порівнюється з контрольними кодами, що зберігаються в системі. Якщо збіг встановлено, то пароль було введено правильно.

Схожий метод використовується і для автентифікації документів засобами ЕЦП. Вихідне повідомлення обробляється хеш-функцією, після чого утворюється деякий хеш-код. Він так само унікальний для такого повідомлення, як відбитки

пальців для людини. Це і є *дайджест повідомлення*. Його нерідко називають *відбитком*, за аналогією до відбитків пальців, *електронною печаткою*, або *штампом*. Дайджест (електронна печатка) повідомлення приєднується до електронного підпису і далі є його складовою.

Приймаюча сторона розшифровує повідомлення (якщо воно було зашифровано), перевіряє електронний підпис за допомогою своєї половини ключа, потім обробляє повідомлення тією самою хеш-функцією, що й відправник, після чого звіряє отриманий дайджест із тим, що містився у підписі. Якщо дайджест збіглися, то повідомлення не було змінено в каналі зв'язку.

Таким чином, ми познайомилися з двома компонентами електронного підпису: відомостями, що вважав за потрібне подати про себе автор (власне підпис), і дайджестом повідомлення. Вони становлять два поля у форматі електронного підпису. У принципі, їх уже досить для двобічного зв'язку, але до них додається ще низка полів, пов'язаних з деякими реєстраційними й організаційними аспектами механізму електронного підпису.

Запитання і завдання для самоконтролю

1. Чому стали актуальними проблеми захисту інформації? Обґрунтуйте відповідь прикладами.
2. Які нормативні акти регулюють питання захисту інформації в інформаційних системах?
3. Наведіть можливі варіанти витоку інформації на робочому місці митника.
4. Наведіть класифікацію потенційних загроз для безпеки інформації в інформаційних системах.
5. Які методи захисту інформації є в інформаційних системах? Поясніть сутність цих методів.
6. Назвіть засоби та заходи, які використовуються для захисту інформації в інформаційних системах будь-якої системи управління.

7. Дайте визначення рукописного підпису, розкажіть про особливості його застосування.
8. Назвіть характерні риси електронного цифрового підпису. Виконайте порівняння рукописного та електронного підписів.
9. Розтлумачте терміни “криптографія”, “метод шифрування”, “ключ шифрування”, “криптоаналіз”.
10. У чому полягає сутність симетричних і несиметричних методів шифрування? Назвіть переваги та недоліки кожного з них.
11. Які є способи компрометації ЕЦП?
12. Що розуміють під засобами ЕЦП? Які показники використовують для оцінки криптостійкості ЕЦП?
13. Як на рівні держави може бути забезпечена відповідальність за надійність засобів ЕЦП та окремих ЕЦП?
14. Проведіть аналіз впливу розміру ключів на їх криптостійкість. Поясніть причини використання ключів різних розмірів для різних типів інформації.
15. У чому полягає принцип достатності захисту інформації засобами ЕЦП?
16. Дайте визначення дайджесту повідомлення. У чому полягає його призначення?
17. Чому виникає необхідність у сертифікації засобів ЕЦП та відкритих ключів?
18. Яке призначення електронного сертифіката? Дайте характеристики наявним моделям сертифікації.
19. Як виконується організаційне забезпечення електронного цифрового підпису в Україні?
20. Дайте визначення електронного цифрового підпису та сертифіката відкритого ключа згідно із Законом України “Про електронний цифровий підпис”.
21. Який правовий статус електронного цифрового підпису згідно із Законом України “Про електронний цифровий підпис”?
22. Який порядок надання сертифіката електронного цифрового підпису в Україні?

23. В яких випадках дію електронного цифрового підпису може бути скасовано?

24. Які є стандарти електронного цифрового підпису в Україні та чим вони відрізняються від міжнародних стандартів?

25. Назвіть складові інфраструктури національної системи ЕЦП України. Для чого їх призначено?

Частина IV

**ПРИКЛАДНЕ ПРОГРАМНЕ
ЗАБЕЗПЕЧЕННЯ ЄДИНОЇ
АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ
СИСТЕМИ ДЕРЖАВНОЇ МИТНОЇ
СЛУЖБИ УКРАЇНИ**

Розділ 9

КОМПОНЕНТИ ЕЛЕКТРОННОГО ДЕКЛАРУВАННЯ

Важливими пріоритетами у використанні інформаційних технологій у сфері зовнішньоекономічної діяльності є запровадження комплексної системи управління ризиками й розвиток систем електронного декларування.

Ураховуючи завдання, покладені Президентом і Урядом України на Митну службу України та спрямовані на наближення митних правил України до світових норм і стандартів, наказом Державної митної служби України від 18 жовтня 2006 р. № 907 затверджено Концепцію створення, запровадження і розвитку системи електронного декларування товарів.

Роль інформаційних технологій у митній справі відображено в Міжнародній конвенції про спрощення та гармонізацію митних процедур (Киотська конвенція, 1999 р.), яка:

- передбачає максимальне практичне використання інформаційних технологій;
- розглядає інформаційні технології як один з принципів митного оформлення, реалізація якого сприятиме спрощенню та гармонізації митних процедур;
- установлює стандартне правило використання інформаційних технологій і засобів електронних комунікацій для вдосконалення митного контролю.

Реалізація процедури електронного декларування товарів дає змогу сформуванню необхідних умов для застосування інформаційних технологій на якісно новому рівні й забезпечити запровадження електронного документообігу між митними органами та суб'єктами ЗЕД з використанням механізму електронного цифрового підпису.

Електронну форму декларування орієнтовано на реалізацію єдиного алгоритму автоматизованої обробки відомостей, що заявляються у ВМД, на рівні митних органів з автоматизованим форматно-логічним контролем, аналізу ризиків і виданням різноманітних застережень для посадових осіб митних органів, які здійснюють митний контроль та митне оформлення товарів.

Положення Концепції ґрунтуються на Законах України “Про електронні документи та електронний документообіг” від 22 травня 2003 р. № 851-IV і “Про електронний цифровий підпис” від 22 травня 2003 р. № 852-IV.

Процедура електронного декларування товарів є попередньою операцією, яка покликана сприяти прискоренню митного оформлення товарів і транспортних засобів, а також здійсненню передбачених Митним кодексом України митних процедур. Попередніми операціями вважаються дії, що виконуються до початку митного оформлення товарів і транспортних засобів. Законодавчою підставою для впровадження електронного декларування товарів є ст. 91 Митного кодексу України.

Процедура електронного декларування товарів виконується в такому порядку:

- підприємство заповнює в установленому порядку вантажну митну декларацію в електронному вигляді;
- додає до неї електронні копії документів, необхідних для здійснення митного контролю та митного оформлення товарів;
- формує повідомлення та засвідчує його електронним цифровим підписом;
- передає зазначене авторизоване повідомлення каналами передачі даних за допомогою системи інформаційно-телекомунікаційного комплексу Держмитслужби України “Електронна пошта” до відповідного структурного підрозділу митного органу, де воно буде проаналізовано за допомогою програмного

забезпечення “Інспектор-2006”, або направляє авторизоване повідомлення безпосередньо до Центральної бази даних Єдиної автоматизованої інформаційної системи Держмитслужби, де воно буде проаналізовано за допомогою відповідних програмно-інформаційних комплексів.

Застосування електронного цифрового підпису в електронних документах здійснюється з використанням послуг акредитованого центру сертифікації ключів відповідно до Закону України “Про електронний цифровий підпис”. Під час приймання електронних документів здійснюється відповідна процедура перевірки ЕЦП з використанням відповідних програмно-інформаційних комплексів (на рівні митного органу або центральної бази даних), що дає можливість пересвідчитися у цілісності та достовірності електронного документа.

Програмно-інформаційний комплекс (на рівні митного органу — “Інспектор-2006”) в автоматичному режимі перевіряє:

- достовірність ЕЦП на авторизованому повідомленні;
- дотримання структури й формату даних, що встановлюються Держмитслужбою України до документів, які подаються в електронному вигляді;
- правильність заповнення електронних копій ВМД та інших документів на предмет відповідності форматно-логічному контролю.

У разі негативних результатів перевірки програмно-інформаційний комплекс формує й направляє декларанту протокол, який містить перелік помилок у ВМД.

У разі позитивних результатів перевірки:

- ВМД реєструється з присвоєнням їй реєстраційного номера;
- аналізується ризик за ВМД;
- формується й направляється декларанту протокол, який містить реєстраційний номер ВМД з діапазону номерів, зарезервованих митним органом, та інформацію про результати контролю в митному органі.

Результати контролю в митному органі містять інформацію про форми митного контролю, необхідні для завершення митного оформлення товарів, що заявляються митному органу шляхом подання паперових примірників документів, необхід-

них для здійснення митного контролю та митного оформлення товарів, а саме здійснення митного контролю:

- без пред'явлення товарів для митного огляду;
- з обов'язковим застосуванням окремих форм митного контролю (перевірка документів, частковий огляд товарів тощо);
- з обов'язковим проведенням митного огляду тощо.

9.1. Автоматизована система митного оформлення “Інспектор-2006”

Призначення та умови застосування

Автоматизована система митного оформлення (АСМО) “Інспектор-2006” розроблена у 1996—2007 рр. і призначена для автоматизованого оформлення митних документів у структурних підрозділах митного органу, зайнятих у процесі митного оформлення вантажів.

Програма дає змогу вирішувати такі завдання:

- автоматизована підтримка технології митного оформлення, прийнятої в митному органі й основаної на нормативних документах Держмитслужби України і митного органу;
- введення і форматно-логічний контроль електронних копій документів, необхідних для митного оформлення та перевірка вантажної митної декларації (ВМД) згідно з критеріями ризику;
- ведення бази даних митного органу — основного сховища інформації про митне оформлення (електронні копії ВМД, інші документи, задіяні в процесі митного оформлення, дані про проходження технологічних етапів митного оформлення тощо);
- обмін інформацією з іншими підрозділами митного органу із застосуванням криптографічного захисту інформації;
- формування інформації з метою подальшого введення її до центральної бази даних Єдиної автоматизованої інформаційної системи (ЦБД ЄАІС) ДМСУ.

Програма “Інспектор-2006” розроблена за архітектурою клієнт — сервер та працює під керуванням операційної системи Microsoft Windows 98/ME/2000/XP/2003. Серверна (СУБД

Microsoft SQL Server 2000/2005 та база даних) і клієнтська частини можуть бути встановлені як на один, так і на різні комп'ютери, причому кількість клієнтських установок обмежується тільки потужністю сервера.

Меню програми розкривається у вікні *Навігатор* у вигляді відповідних папок, підпапок та режимів. Усі функції програми розподілені у папках: *Документи*, *Звіти*, *Довідники*, *Тексти документів*, *Сервіс*, та підпорядкованих їм режимах (рис. 9.1). При входженні в певний режим у правій частині екрана наводиться вікно для роботи у цьому режимі. Панель закладок режимів, з якими проводилась робота, розміщується у верхній частині робочого вікна і призначена для повернення у відповідний режим. За допомогою позначки  на панелі закладок можна вивести весь перелік відкритих режимів і повернутись до потрібного або закрити режими. За допомогою позначки  режим, що відповідає позначеній курсором закладці, закривається.

Налагодження програми

Умовою виконання основних функцій програми є налагодження роботи програми адміністратором. Загальне налагодження роботи “Інспектор-2006” виконується за допомогою режимів папки *Сервіс* (рис. 9.2), які надають адміністратору можливість налагодити вибрану в митному органі систему для роботи з документами митного оформлення вантажів, занести інформацію про користувачів системи, встановити технологію митного оформлення вантажів згідно з вимогами, що викладені у “Порядку митного контролю й митного оформлення товарів із застосуванням вантажної митної декларації”, затверджені наказом Держмитслужби України від 20 квітня 2005 р. № 314.

Режим *Загальні установки* призначений для встановлення головних параметрів налагодження програми: вказується інформація про митний орган, його підрозділи та керівників, для кожної бази даних митного підрозділу зазначається назва та номер порту сервера Регіонального інформаційно-телекомунікаційного комплексу (поштового сервера), імена поштових скриньок, за допомогою яких буде здійснюватися обмін повідомленнями і на яку будуть приходити протоколи прийому документів в ЄАІС, задаються налагодження синхронізації між базами даних інформації щодо платежів тощо.

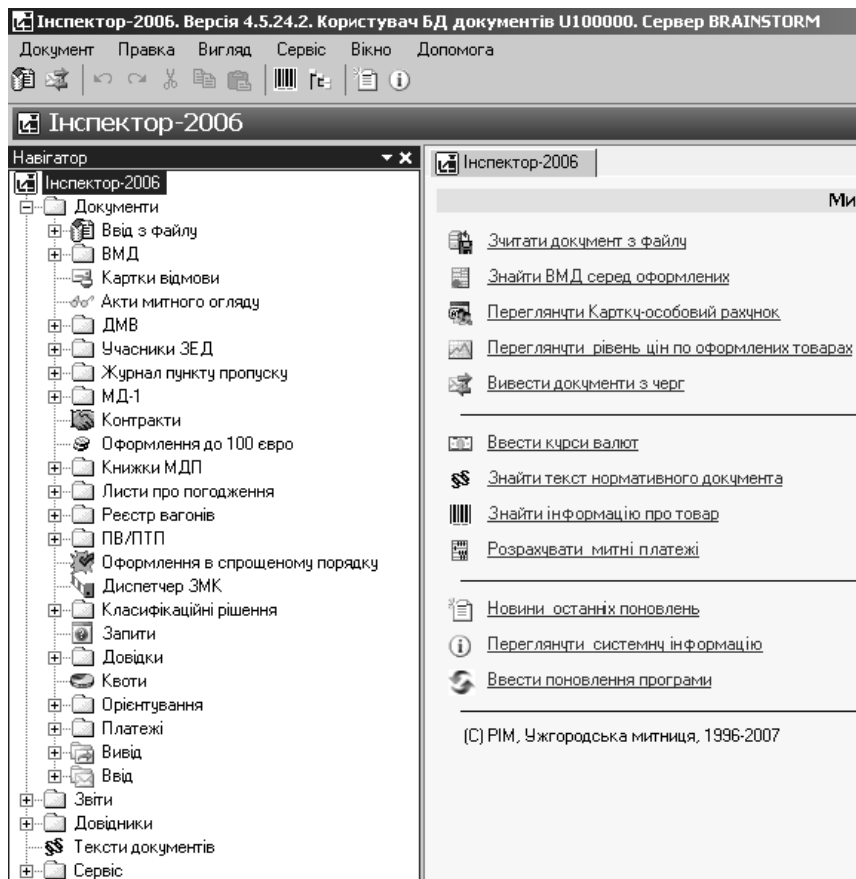


Рис. 9.1. Навігатор Програми “Інспектор-2006”

Адміністратор виконує введення користувачів та надання їм певних повноважень. Залежно від наданих повноважень, користувачеві будуть доступні відповідні режими роботи програми.

Для реєстрації посадових осіб, які беруть участь у здійсненні митного контролю та митного оформлення, у програмі “Інспектор-2006” необхідно:

— сформулювати перелік підрозділів, що працюють із локальною (відділу митного оформлення) базою даних;

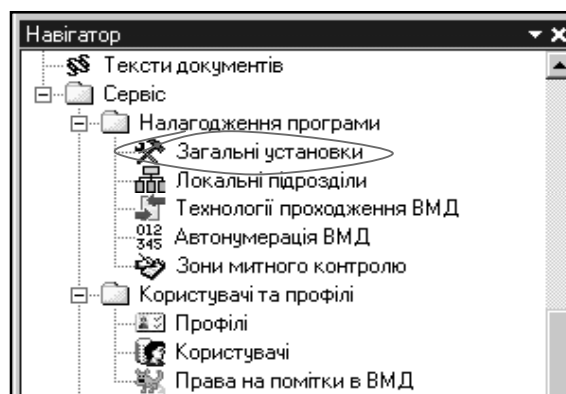


Рис. 9.2. Режими налагодження програми “Інспектор-2006”

— розробити перелік профілів, що визначають стандартний набір прав доступу та повноваження для інспекторів, які виконують однакові функції у митному оформленні ВМД;

— зареєструвати користувачів бази даних із наданням їм відповідних повноважень;

— визначити етапи технологій митного оформлення згідно із задіяними митними режимами та сформувати список профілів та користувачів, що мають доступ до роботи з цими етапами;

— встановити перелік технологій, які можна застосовувати у кожному із локальних підрозділів.

Створення переліку підрозділів, що працюють із локальною базою даних, виконується за допомогою режиму *Сервіс/Налагодження програми/Локальні підрозділи* (рис. 9.3).

Режим *Сервіс/Користувачі та профілі/Профілі* використовують для полегшення адміністрування програми та спрощення надання прав користувачам. Профілі дають можливість надати однакові повноваження користувачам, що виконують однакові посадові обов’язки, та визначити права на роботу з етапами митного оформлення (рис. 9.4).

Для створення профілю на панелі режиму вибирається посилання *Створити* або пункт контекстного меню *Створити*, після чого відкривається вікно *Профіль*. У поле *Ідентифіка-*

Інспектор-2006 Локальні підрозділи

Створити Створити новий локальний підрозділ

Шукати серед існуючих

Назва

Статус ☒ Діючі ☐ Всі

Код	Митний	Назва
1	110000001	Відділ митного оформлення №1

Додання локального підрозділу

Основні дані

Код 2 Митний код 110000002

Тип Внутрішній пост

Назва Відділ митного оформлення №2

☒ Використовується автонумерація ВМД

Базова технологія оформлення ВМД

☒ Використовуються технології

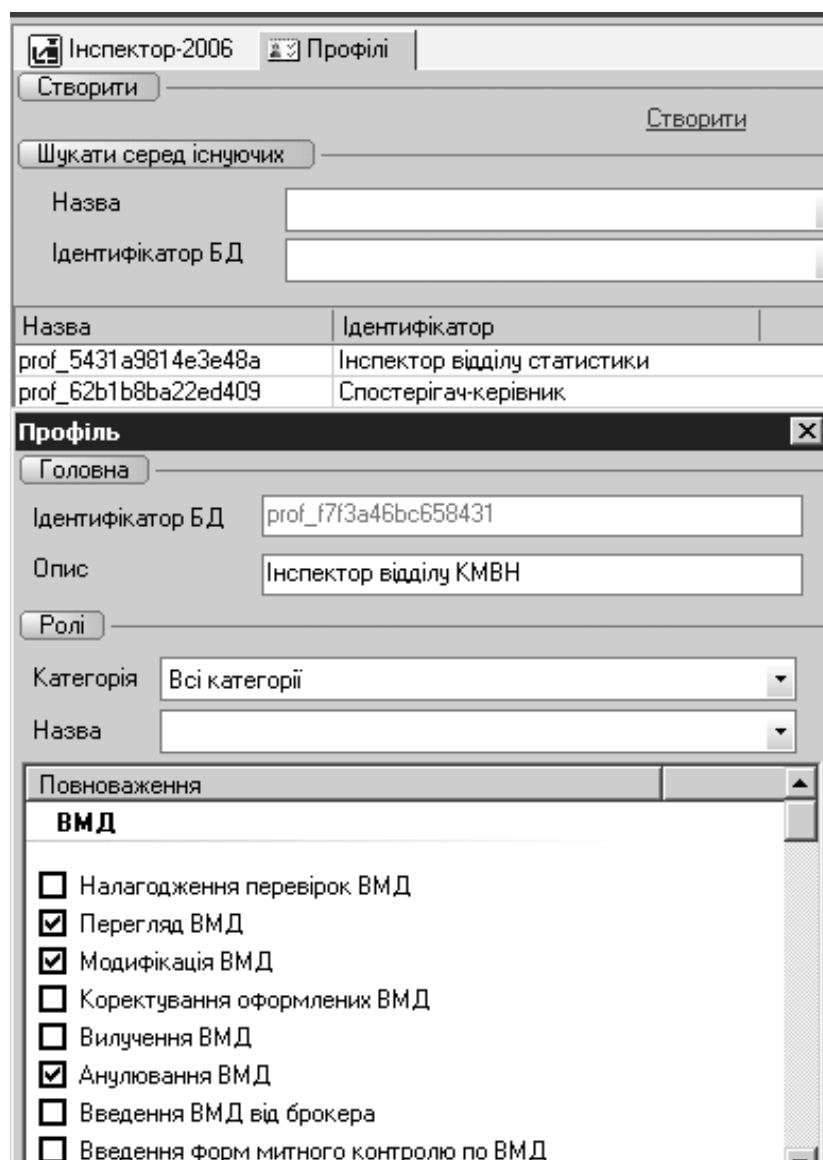
Технологія Технологія оформлення ІМ

Рис. 9.3. Вікно реєстрації локального митного підрозділу

тор БД програмою самостійно заноситься унікальний ідентифікатор профілю; у полі *Описання* вказується назва профілю (наприклад, Інспектор статистики), яка буде відображатись в програмі, та вибираються ролі, необхідні для цього профілю.

Програма “Інспектор-2006” поставляється з набором стандартних профілів: *Інспектор відділу статистики*, *Інспектор відділу платежів*, *Інспектор відділу тарифів*, *Інспектор вантажного відділу*, *Спостерігач-керівник*. Адміністратор має право змінювати, вилучати та створювати нові профілі.

Для створення списку посадових осіб, які будуть працювати з програмою “Інспектор-2006”, використовують режим *Сервіс/Користувачі та профілі/Користувачі* (рис. 9.5). У програмі можливі такі варіанти створення нового користувача:



Інспектор-2006 Профіль

Створити Створити

Шукати серед існуючих

Назва

Ідентифікатор БД

Назва	Ідентифікатор
prof_5431a9814e3e48a	Інспектор відділу статистики
prof_62b1b8ba22ed409	Спостерігач-керівник

Профіль

Головна

Ідентифікатор БД prof_f7f3a46bc658431

Опис Інспектор відділу КМВН

Ролі

Категорія Всі категорії

Назва

Повноваження

ВМД

- ☐ Налагодження перевірок ВМД
- ☒ Перегляд ВМД
- ☒ Модифікація ВМД
- ☐ Коректування оформлених ВМД
- ☐ Вилучення ВМД
- ☒ Анулювання ВМД
- ☐ Введення ВМД від брокера
- ☐ Введення форм митного контролю по ВМД

Рис. 9.4. Вікно створення та редагування профілів

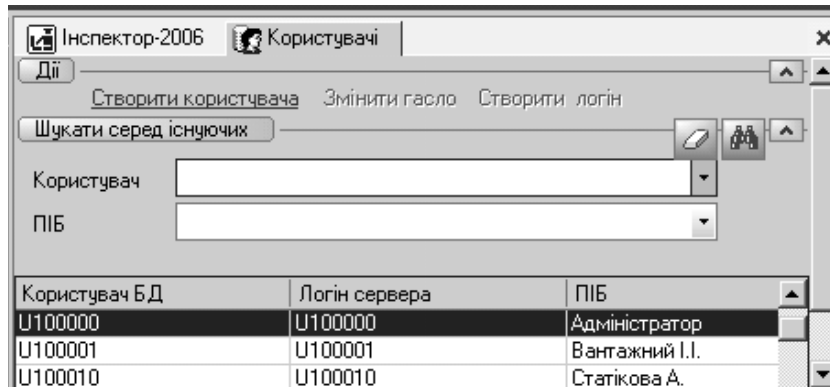


Рис. 9.5. Вікно формування списку користувачів

- створити користувача SQL-сервера з числа користувачів домену Windows NT та надати йому права доступу до бази даних;
- вибрати користувача з числа наявних користувачів SQL-сервера та надати йому права доступу до бази даних;
- створити нового користувача SQL-сервера та надати йому права доступу до бази даних.

Під час створення нового користувача з SQL-аутентифікацією послідовно відкриваються вікна для занесення посадової інформації (поля, назви яких виділені у вікні жирним шрифтом, обов'язкові для заповнення). Набори повноважень і права доступу до етапів технологій митного оформлення для користувачів задаються за допомогою профілів (у виключних випадках — з використанням повноважень).

Надаючи користувачу повноваження, слід пам'ятати:

- тільки повноваження *Адміністратор SQL-сервера* надає можливість створювати нових користувачів, але для користувачів з цим повноваженням програма блокує роботу з документами митного оформлення;
- повноваження *Адміністратор бази даних* надає право працювати з усіма документами митного оформлення, тобто право доступу до всіх режимів програми "Інспектор-2006" не-

залежно від того, чи були безпосередньо надані повноваження до цих режимів, але користувачі з цим повноваженням не можуть виконувати функції *Адміністратора SQL-сервера*);

— без повноваження *Оператор виводу* користувач не зможе вивести з програми жодного документа ні в ЦБД, ні в інший митний підрозділ, ні в будь-яке інше місце, перелік яких встановлюється в списку місць обміну інформацією (режим *Сервіс/Передача інформації/Місця обміну інформацією (митні адресати)*).

Для налагодження технологій та їх етапів проходження ВМД після прийняття декларації від брокера використовують режим *Сервіс/Налагодження програми/Технології проходження ВМД* (рис. 9.6).

Панель режиму поділена на два вікна (рис. 9.6). У вікні *Технології* натисненням кнопок чи командами контекстного меню створюються, редагуються та вилучаються технології. Редагування виділеної технології може бути доступне шляхом подвійного натиснення лівої кнопки миші.

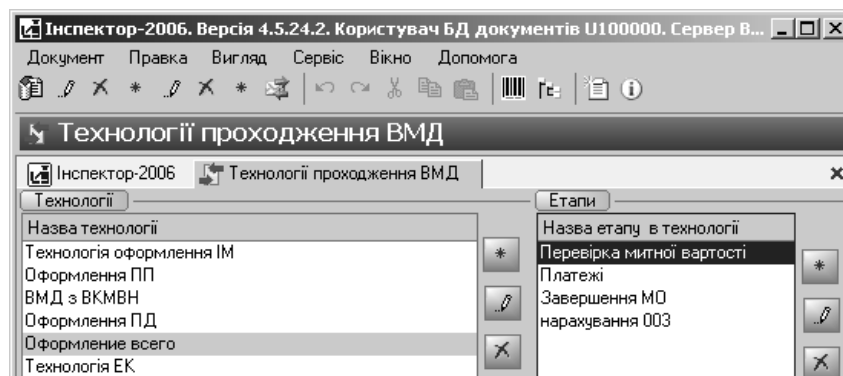


Рис. 9.6. Вікно налагодження технологій та їх етапів проходження ВМД

Для виділеної технології у вікні *Етапи* можна створити чи редагувати етап цієї технології. На сторінці *Етапи* вікна *Етапи* указуються (рис. 9.7):

— у полі *Назва* — назва підрозділу, який буде проводити оформлення на такому етапі, або короткий зміст роботи цього етапу;

— у полі *Код етапу* — будь-який набір символів;

— у полі *Номер етапу* в технології — порядковий номер етапу в технології;

— позначки *Штамп на виході*, *Пломба на виході*, *Печатка на виході*, *Номер на виході* — означають, що під час переведу ВМД з цього етапу на наступний обов’язково повинно проставлятися відповідне митне забезпечення із занесенням його реквізитів в базу даних. Позначку *Переводити ВМД на даний етап тільки в разі наявності ДМВ* рекомендується включати для тих етапів, які стосуються підрозділів контролю митної вартості. Включення позначки *Етап використовується* означає, що цей етап буде враховуватись під час проходження ВМД за технологією.

Рис. 9.7. Вікно формування етапу технології митного оформлення

На сторінці *Користувачі* вікна *Етап* кнопками *Додати користувача* та *Додати профіль* зі списків вибираються користувачі та профілі, які матимуть права доступу на цей етап технології митного оформлення ВМД (рис. 9.8). Встановлення позначки *Редагувати ВМД* надає такому користувачу або

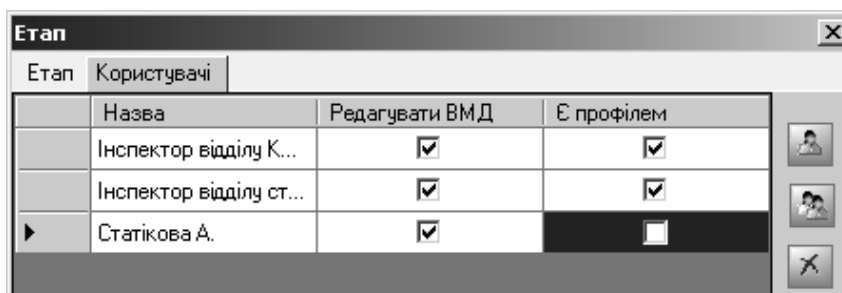


Рис. 9.8. Надання користувачам прав доступу на виконання етапу технології митного оформлення

профілю право на внесення змін у ВМД на цьому етапі (користувач або профіль повинні мати повноваження, які дають право на редагування ВМД). При включенні позначки *Є профілем* в етап, всі користувачі, які мають право на цей профіль, також дістають право на етап, навіть якщо вони безпосередньо не включені до нього.

Вилучення технологій або етапів можливе тільки в тому випадку, якщо за ними не проводилось оформлення.

Після налагодження режиму *Технології проходження ВМД* необхідно у режимі *Сервіс/Налагодження програми/Локальні підрозділи* встановити перелік технологій, які можна застосовувати у кожному з митних підрозділів. У вікні *Локальні підрозділи* кнопкою *Шукати серед існуючих* відображається список локальних підрозділів, знаходиться та відкривається для редагування потрібний запис (рис. 9.9).

Позначка *Використовуються технології* проставляється для визначення базової технології митного оформлення підрозділу, зі списку *Технологія* вибирається назва базової технології.

Позначка *Допускаються виключення* проставляється у випадку, якщо окремі типи ВМД оформлюються в зазначеному підрозділі за іншими технологіями, відмінними від базової. Після цього становиться доступним вікно для формування (вилучення) записів для типів ВМД, які оформлюються за технологією, відмінною від базової.

Редагування локального підрозділу

Основні дані

Код: 1 Митний код: 110000000

Тип: Митниця

Назва: Відділ митного оформлення № 1

☒ Використовується автонумерація ВМД

Базова технологія оформлення ВМД

☒ Використовуються технології

Технологія: Оформление всего

Інші технології

☒ Допускаются исключения (некоторые типы ВМД оформляются за технологией, отличной от базовой)

Тип ВМД	Технологія
IM 40 KO Импорт компле	Технологія оформлення
IM ПД Импорт - попере	Оформлення ПД
IM ПП Импорт - попере	Оформлення ПП
IM 40 Импорт	Технологія оформлення

Тип ВМД: IM 40 KO Импорт комплектного объекта

Технологія: Технологія оформлення IM

OK Відмінити

Рис. 9.9. Формування переліку технологій для підрозділу митного оформлення

Для автоматичного формування номерів ВМД у межах підрозділу у вікні **Локальні підрозділи** необхідно встановити прапорець *Використовується автонумерація ВМД*.

У режимі *Сервіс/Автонумерація* для кожного бажаного діапазону номерів слід створити журнал автонумерації, в якому вказати:

- назву журналу;
- режим присвоєння коду митниці (під час формування номера ВМД у першій частині номера задається код митного органу з підрозділу користувача, який приймає ВМД у базу даних);
- локальні підрозділи, в яких використовується журнал;
- перший та останній номер ВМД у журналі;
- дати введення журналу в дію та його виведення з неї (за необхідності);
- для яких типів ВМД створюється журнал (для основного журналу — *Всі типи ВМД*);
- на вкладці *Повноваження* обов'язково вказати профілі, які мають доступ до цього журналу.

Основні режими роботи

Режими папки *Документи* призначені для введення електронних копій документів, сформованих брокером, формування електронних документів на робочому місці інспектора та роботи з ними. Зазначені функції реалізуються за допомогою режимів, наведених у навігаторі програми (рис. 9.10), за умови надання адміністратором відповідних повноважень користувачеві.

Режим *Документи/Ввід з файлу* призначений для введення електронних копій документів. Введення документів у програмі можливе із файлів з такими розширеннями: *imf* — ВМД, картки учасника ЗЕД; *smf* — ВМД, картки учасника ЗЕД, реєстри залізничних вагонів; *zxt* — листи узгодження, ДМВ, ПТП; *xml* — ДМВ.

Виведену на екран електронну копію документа перевіряють на помилки. Форматно-логічний контроль документа можна здійснювати як у повному обсязі, так і за мінімумом. У протоколі перевірки наводиться перелік наявних у документі помилок. За умови відсутності грубих помилок у протоколі перевірки та наявності у користувача повноважень на модифікацію відповідного документа здійснюється запис документа у базу даних.

Введений у базу даних документ наводиться у переліку документів відповідного режиму папки *Документи: ВМД, ДМВ, Учасники ЗЕД, МД-1, Книжки МДП; Листи про погодження, Реєстр вагонів, Провізні відомості/ПТП*.

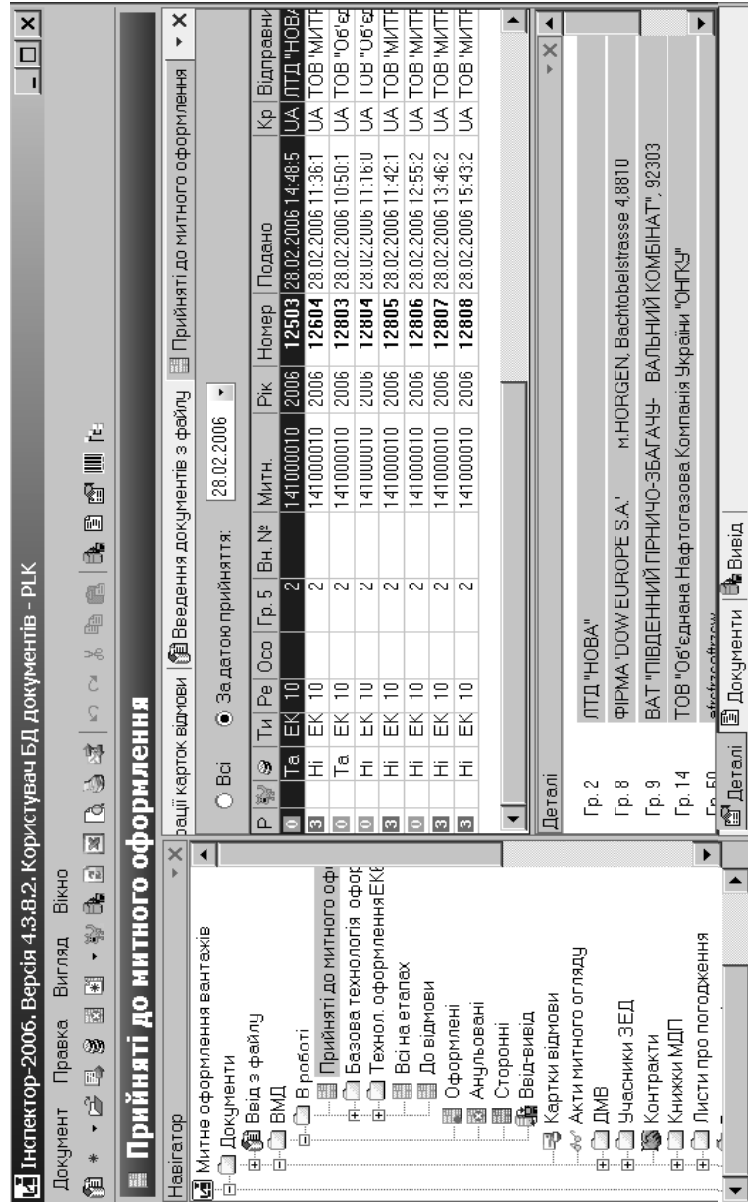


Рис. 9.10. Режим Документи / ВМД / Прийняті до митного оформлення

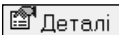
Режим *Документи/ВМД* призначений для роботи з ВМД, прийнятими до митного оформлення, та переведення їх за відповідними етапами технологій митного оформлення.

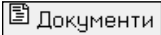
Усі ВМД, що збережені у базі даних, за ступенем обробки у процесі митного оформлення розподіляються за такими режимами:

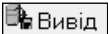
- *У роботі* — призначений для роботи з ще неоформленими ВМД;
- *Оформлені* — призначений для роботи з оформленими ВМД;
- *Анульовані* — призначений для роботи з анульованими ВМД;
- *Сторонні* — призначений для роботи з ВМД інших митниць;
- *Ввід-Вивід* — призначений для введення ВМД з бази даних ДОС версії програми, виведення у ЦБД оформлених ВМД та ВМД у роботі та виведення ВМД в інший підрозділ митниці.

Залежно від умов налагодження програми ВМД, оформлення яких у програмі відбувається без використання технології, будуть наводитися у режимі *Документи/ВМД/ В роботі*; ВМД, оформлення яких у програмі відбувається із застосуванням технології, наводяться у режимі *Документи/ВМД/ В роботі/Прийняті до митного оформлення*.

Вікно режиму *Документи/ВМД/Прийняті до митного оформлення* складається з трьох частин: панелі фільтрації; таблиці-переліку ВМД, виведених з урахуванням вибраної умови фільтрації та розділу, що залежно від вибраної закладки може містити:

 **Деталі** — детальну інформацію про позначену курсором ВМД;

 **Документи** — супровідні документи за ВМД (наприклад, вексель);

 **Вивід** — номери ВМД, що підлягають виведенню у зовнішній файл.

У таблиці-переліку ВМД:

— у графі *Ризик* наводяться індикатори ризику ВМД із зазначенням ступеня ризику від 0-го до 3-го. Ступінь ризику і

відповідно колір індикатора змінюється під час введення інформації про результати проведення митного контролю із застосуванням форм контролю;

— у графі *Помітки*  наводиться ознака наявності поміток до оформлення ВМД. Ознаку червоного кольору мають ті ВМД, серед поміток до оформлення яких є такі, що унеможливають подальше оформлення ВМД;

— у графі *Платежі*  наводиться ознака наявності списання платежів за ВМД;

— у графі *Вн. №* наводиться внутрішній номер (номер декларанта) ВМД.

Перегляд вмісту ВМД можливий за виконання однієї з таких дій:

- виділити та натиснути клавішу *F2* або *Enter*;
- на рядку ВМД двічі натиснути ліву кнопку миші;
- на рядку ВМД натиснути праву кнопку миші та з контекстного меню вибрати команду *Відкрити*.

Вікно електронної копії ВМД (рис. 9.11) обладнане панелями інструментів з кнопками, які призначені для роботи з графами ВМД (табл. 9.1).

У режимі *Документи/ВМД/Прийняті до митного оформлення* для роботи із виділеною у таблиці-переліку ВМД, використовується контекстне меню. Команди контекстного меню дають змогу виконати таке.

Перевести на наступний етап — ВМД зі статусом “прийнята до митного оформлення” після її перевірки та підтвердження дії переводиться на перший, задіяний в технології етап (його найменування наводиться у повідомленні про здійснення дії).

Списати платежі (наводиться в меню за наявності у користувача повноважень роботи з платежами) — призначений для списання платежів за ВМД в автоматичному режимі. Під час входження в цей режим за умови, що списання платежів ще не відбувалось, на екран виведеться перше вікно майстра списання платежів (рис. 9.12), яке містить таблицю з інформацією про платежі, зазначені у графі “В”, що підлягають списанню. Майстер надає можливість з граф ВМД занести інформацію про платника, переглянути його платіжну інформацію та за

[illegible]

Головна		Товар		Специфікація	
УНІФІКОВАНИЙ АДМІНІСТРАТИВНИЙ ДОКУМЕНТ (уід)					
2. Відправник/експортер		UA 328754908308 ТОВ "Агро Фуд Транс"			
69068 м. Запоріжжя, Шевченк. р.н., вул. Авалані, 7 кв. 1 Україна					
Регистр №		10 1 22 00 - 23 / 0032875490			
8. Одержувач/імпортёр		RU UA 305398008304 ТОВ "Підер"			
193312, м. Санкт-Петербург, вул. Колонтай, буд. 41, корп. 1 Росія					
Регистр №		10 1 22 00 - 23 / 0032875491			
14. Декларант/представник		UA 305398008304 ТОВ "Зовнішторгтранс"			
м. Запоріжжя, с. Леваневського ДСП1009					
Регистр №		10 1 22 00 - 23 / 0030539806 11200/032БМ-01240 від 06.10.2000			

Графи		Вартість		Зворот	
1. Тип декларації		R/R		260091024	
EK	10	МФО		313827 Код ЗОД АТПБ "Аваль"	
3. Док. зрк спецфр.	4. Відвант	B/P		МФО	
1				Код	
5. Товарів	6. Місьч	7. Довідковий номер			
1	770	112000002 / 2007 / 1			
9. Особа, відповідальна за фінансове вжиття		UA 3287549083			
ТОВ "Агро Фуд Транс"					
69068 м. Запоріжжя, вул. Авалані, 7 кв. 1 Україна					
Регистр №		10 1 22 00 - 23 / 0032875491			
11. Торг. країна		12. Митна вартість			
643	Росія	42420,1			
15. Країна відправлення		17. Країна призначення			
		643		Росія	
20. Умови поставки		12. Митна вартість			
12	DDU	Санкт-Петербург			

Рис. 9.11. Робоче вікно електронної копії ВМД

необхідності поділити суму платежу вибраного платника (курсор встановлено на відповідному рядку) між іншими платниками. Позначка у віконці графи “Рез” проставляється за потреби резервування коштів (для ВМД типу ІМ ПД).

Таблиця 9.1. Перелік основних кнопок для роботи з ВМД

Кнопка	Призначення
	Запис у базу даних
	Перевірка (форматно-логічний контроль) документа
	Детальна інформація про код результату митного огляду та його складові
	Помітки щодо ВМД
	Аналіз нетарифного регулювання за ВМД
	Переведення ВМД на наступний задіяний етап технології
	Здійснення відмови (вилучення або анулювання ВМД)
	Відміна дії під час коригування ВМД
	Налаштування параметрів друку та роздрукування ВМД
	Виведення переліку граф, що містять інформацію на зворотному боці
	Виведення зобов'язань
	Виведення значень граф 2, 8, 9, 14, 50 (клієнти)
	Виведення значень граф 18 та 21 (транспортний засіб відправлення і транспортний засіб на кордоні)
	Виведення навігатора за певними графами ВМД, що мають складну структуру
	Виведення форм митного контролю

Закінчення табл. 9.1

Кнопка	Призначення
	Перелік товарів з інформацією про них та підсумком щодо кількісних та вартісних показників за всіма товарами ВМД
	Виведення граfi “С”
	Виведення граfi “В”
	Список помилок
	Інформація про тарифне й нетарифне регулювання за товаром (першим у ВМД або тим, сторінку якого виведено на екран)
	Проведення аналізу цін за попередніми оформленнями товару (першого у ВМД або того, сторінку якого виведено на екран)

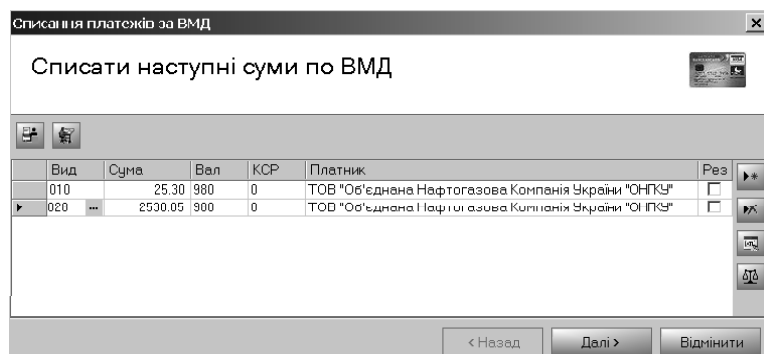


Рис. 9.12. Вікно майстра списання платежів (крок 1)

На другому етапі майстра виконується перевірка платіжної інформації (рис. 9.13). Якщо під час перевірки виявлено певні невідповідності, то у другому вікні майстра виведуться відповідні попередження (за зазначеним платником в базі даних (режим *Платежі/Платіжні документи*) відсутні платіжні документи або коштів, зазначених в них, недостатньо для списання).

Списання платежів за ВМД

Перевірка введеної інформації

✓

Перевірка правильності заповнення

ОК

✓

Перевірка відповідності графі В

Списання відповідає графі В ВМД

✓

Перевірка залишку клієнта, код субрахунку - 0

Клієнт: ЛТД "НОВА", поточний залишок: 200000.00, заблоковано по ВМД в роботі: 0, зарезервовано по ПД: 0, списується по даній ВМД: 101.00, залишається: 199899.00

✓

Заповнення графи С

Графа С може бути сформована, див. наступну сторінку

або

⊖

Перевірка залишку клієнта, код субрахунку - 0

Клієнт: ЛТД "НОВА", поточний залишок: 200000.00, заблоковано по ВМД в роботі: 5274.34, зарезервовано по ПД: 0, списується по даній ВМД: 2222587.17, залишається: -2027861.51

⚠

Заповнення графи С

В базі даних платіжних документів недостатньо інформації для заповнення графи С. Її прийдеться заповнити вручну

< Назад

Далі >

Відмінити

Рис. 9.13. Вікно майстра списання платежів (крок 2)

У третьому вікні майстер списання виконує заповнення графи “С”.

Якщо графа “С” ВМД не була заповнена перед процедурою списання (рис. 9.14), у графі *Номер документа* наводиться номер платіжного документа, за яким списуються платежі. За допомогою клавіші *ОК* відбувається завершення списання коштів за ВМД та заповнення графи “С” ВМД. У графі  таблиці-переліку ВМД ознака “Ні” змінюється на ознаку “Так”.

Якщо графа “С” була заповнена перед списанням коштів, то у третьому вікні надається попередження (рис. 9.14).

За наявності позначки у віконці *Заповнити графу С наступними даними* за допомогою клавіші *ОК* відбудеться спи-

Списання платежів за ВМД

Заповнення граfi С

☒ Заповнити графу С наступними даними:

Код	СП	Платник	Номер документа	Дата док.	Сума	Вал
▶ 010	01	0019056351	221101	22.11.2006	2587.17	980

< Назад ОК Відмінити

Списання платежів за ВМД

Заповнення граfi С

⚠ Увага! В графі С ВМД уже є дані.
Перезаповнення граfi С призведе до к знищення

☐ Заповнити графу С наступними даними:

Код	СП	Платник	Номер документа	Дата док.	Сума	Вал
▶ 010	01	0019056351	221101	22.11.2006	2587.17	980

< Назад ОК Відмінити

Рис. 9.14. Вікно майстра списання платежів (крок 3)

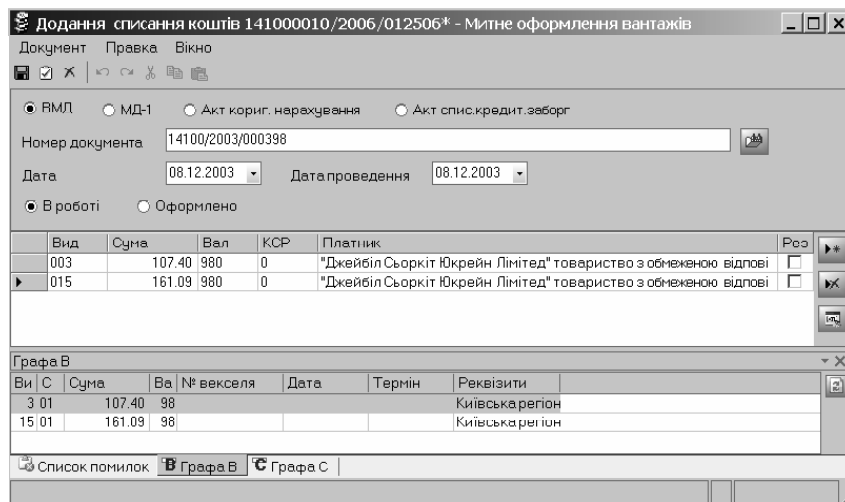
сання коштів та редагування граfi “С” ВМД відповідно до платіжних реквізитів, наведених у цьому вікні.

За відсутності позначки у віконці *Заповнити графу С наступними даними* за допомогою клавіші *ОК* відбудеться списання коштів відповідно до платіжних реквізитів, наведених у графі “С” ВМД.

Списані кошти відображаються в платіжній інформації учасника ЗЕД під рубрикою *заблоковано по ВМД в роботі* доти, доки ВМД не буде оформлено.

Для редагування списання платежів “вручну” за умови, що списання платежів уже відбувалось, у режимі *Документи/ВМД/Прийняті до митного оформлення* з контекстного меню вибирають команду *Форма списання платежів*. На екран виведеться вікно (рис. 9.15), в якому необхідно активізувати позначку стільки разів, за скількома видами платежів списуватимуться кошти, та ввести інформацію про платежі у наведені рядки таблиці. При цьому можна вивести на екран для

перегляду зміст граф “В” або “С”, активізувавши відповідну закладку на нижній панелі робочого вікна та скориставшись кнопкою  правої панелі сторінки, що розташована за активізованою закладкою (рис. 9.15).



Вид	Сума	Вал	КСР	Платіжик	Рез
003	107.40	980	0	"Джейбіл Сьоркіт Юкрейн Лімітед" товариство з обмеженою відпові	☐
015	161.09	980	0	"Джейбіл Сьоркіт Юкрейн Лімітед" товариство з обмеженою відпові	☐

Ви	С	Сума	Ва	№ векселя	Дата	Термін	Реквізити
3	01	107.40	98				Київська регіон
15	01	161.09	98				Київська регіон

Рис. 9.15. Вікно редагування списання коштів

Якщо списання коштів відбулось з включеною позначкою *В роботі*, то списані кошти відображаються в платіжній інформації учасника ЗЕД під рубрикою *заблоковано по ВМД у роботі* доти, доки ВМД не буде оформлено. Якщо списання коштів відбулось з включеною позначкою *Оформлено*, то списання цих коштів відображається у поточному залишку учасника ЗЕД.

Для видалення або анулювання ВМД у режимі *Документи/ВМД/Прийняті до митного оформлення* з контекстного меню вибирають команду *До відмови*. Під час входження в режим за відсутності списання платежів за ВМД на екран виведеться додаткове вікно (рис. 9.16), у якому необхідно:

— вибрати тип відмови (*Відкликання декларантом, Відмова в митному оформленні, Інше*);

Рис. 9.16. Вікно вилучення або анулювання ВМД

- для типу *Інше* ввести текст примітки;
- для типу *Відмова в митному оформленні* вибрати картку відмови (створюється в режимі *Картки відмови* навігатора програми або в режимі контекстного меню *Створити з ВМД — Картку відмови*);
- вибрати дію (*Вилучити* або *Анулювати*);
- вибрати причину відмови;
- за потреби для вибраної причини вказати номер товару за ВМД у графі *№ тов.*;
- за допомогою клавіші *ОК* записати дані про відмову.

Незалежно від виконаної дії (*Вилучити*, *Анулювати*) ВМД переводиться у перелік *До відмови*. Під час входження в режим *Відмова* за наявності інформації про списання платежів за ВМД на екран виведеться вікно-попередження про неможливість відмови або анулювання без зняття з ВМД усіх списаних сум. За клавішею *ОК* відбудеться зняття заблокованих сум, на екран виведеться електронна копія картки відмови.

Для створення електронних копій документів: векселя, заяви-зобов'язання, акта митного огляду, картки відмови вилучення або анулювання ВМД у режимі *Документи/ВМД/*

Прийняті до митного оформлення з контекстного меню вибирають команду *Створити з ВМД*.

У вікні створення векселя програмно встановлюється номер поточної ВМД та за наявності у графі “В” ВМД інформації про вексель — за номером векселя у відповідні поля робочого вікна вводяться реквізити векселя.

Під час створення картки відмови номер картки формується програмно, в полі *Декларант* наводиться найменування декларанта (гр. 14 ВМД), у розділі *Документи* — документи графі 44 ВМД (за всіма товарами) та номер поточної ВМД.

Створені документи наводяться відповідно в режимах: *Платежі/Інші документи/ Векселі/Заяви-зобов’язання, Акти митного огляду та Картки відмови*.

За потреби перегляду та зміни реєстраційних даних у режимі *Документи/ВМД/Прийняті до митного оформлення* з контекстного меню вибирають команду *Реєстраційні дані*. Реєстраційні дані також наводяться у рядку *Оформ* розділу *Деталі* робочого вікна. Оновлені реєстраційні дані у цьому рядку наводяться після відпрацювання режиму контекстного меню *Оновити список*.

Створювати помітки за ВМД у режимі *Документи/ВМД/Прийняті до митного оформлення* можна за допомогою команди *Помітки* з контекстного меню. У виведеному на екран вікні *Помітки по ВМД №...* з переліку передбачених програмою поміток вибирають потрібну та записують її. Якщо було встановлено хоча б одну помітку зі значенням “1” у графі *Зупин. оформ.*, ця ВМД у графі таблиці-переліку ВМД матиме позначку червоного кольору (оформлення ВМД неможливе). Можна встановити/скасувати тільки ту помітку, на яку має повноваження користувач.

У режимі *Документи/ВМД/Прийняті до митного оформлення* за допомогою команди *Властивості* з контекстного меню є можливість переглянути інформацію про коригування граф ВМД та про дії, що виконувались з ВМД у процесі її митного оформлення.

Способи виведення інформації

Для синхронізації інформації, що міститься в базах даних між віддаленими підрозділами митниці та базою даних митниці, а також відправки документів у ЦБД ДМСУ у програмі

“Інспектор-2006” використовується режим введення-виведення інформації.

Виведення інформації можна здійснити двома способами: просте виведення та черги.

Просте виведення документів — це дія, за якої користувач вибирає документи, що підлягають виведенню, та здійснює їх виведення в указану директорію або відправку засобами ІТК Держмитслужби України “Електронна пошта”. Документи, що підлягають виведенню, можуть бути вибрані одним з таких способів:

- вказівка діапазону дат оформлення документів;
- вказівка діапазону дат останньої модифікації документів;
- вибір конкретного документа;
- формування списку документів до виведення.

Черги — це механізм, за якого документи автоматично ставляться в черги на виведення в місця обміну інформацією. Виведення з використанням черг є рекомендованим механізмом виведення документів, тим більше, що деякі документи — зворотна інформація стосовно аналізу ризиків, платіжні документи — можуть бути виведені тільки за допомогою черг.

Кожен документ, який підлягає виведенню (як результат його оформлення, модифікації або первинного прийняття в базу — залежно від типу документа), автоматично ставиться системою в чергу виведення.

Кожен документ може потрапити одночасно в декілька черг виведення. Наприклад, для розсилки карток учасників ЗЕД для кожного підрозділу митного оформлення створюється своя черга.

Для виведення інформації у будь-якому форматі необхідно попередньо здійснити налагодження місць обміну інформацією. Для налагодження та здійснення будь-якого виведення інформації користувач повинен мати повноваження *Оператор виводу*. Під час використання простого виведення користувач додатково повинен мати повноваження на перегляд відповідного типу документів.

Налагодження черг виведення здійснюється в режимі *Документи/Вивід/Черги виводу*. Для створення черги слід вибрати

з контекстного меню пункт *Додати* (або клавішу INS). У діалоговому вікні слід вказати:

— *Тип черги* (типи черг визначаються схемою інформаційних потоків);

— *Назва черги, примітка* — для зручності та розрізнення черг;

— *Черга поповнюється* — вимкнений прапорець забороняє постановку документів у чергу;

— *Черга виводиться* — вимкнений прапорець відключає автоматичний виведення з черги;

— *У чергу ставляться документи* — можна вибрати *Всі*;

— *При автоматичному виводі виводити не частіше ніж через __хв. від попереднього виводу* — для сервісу автоматичного виведення допустимі такі значення:

а) *більше нуля*: автомат буде виводити таку чергу не частіше, ніж через задану кількість хвилин;

б) *нуль або пусто*: автомат буде виводити чергу щоразу при своєму спрацюванні (у поточній версії — щохвилино);

в) *менше нуля*: така черга автоматично виводитися не буде, її слід виводити в ручному режимі.

Виведення документів, що знаходяться у чергах, можна здійснити такими методами: ручне виведення окремої черги, ручне виведення усіх черг, автоматичне виведення.

Ручне виведення окремої черги виконується в режимі *Документи/Ввід-вивід інформації/Черги виводу*. Необхідно виділити потрібну чергу та натиснути кнопку *Вивести вибрану чергу*, після чого у вікні *Місце виводу* вказати місце для виведення документів з черги: шлях до папки, куди буде занесений файл виведення, або адреса електронної пошти адресата черги.

Ручне виведення усіх черг виконується в режимі *Документи/Ввід-вивід інформації/Черги виводу* натисненням кнопки *Вивести всі активні черги*. У вікні *Вивід всіх документів, що підлягають виводу* за замовчуванням відмічено ті черги, для яких установлено параметр *Черга виводиться*. За необхідності список черг до виведення може бути скорегований. Розпочати виведення документів з черг можна за допомогою клавіші *Вивести*. Ручне виведення усіх черг здійснюється тільки на скриньку ІТК Держмитслужби України “Електронна пошта” адресата.

Автоматичне виведення документів з черг реалізується процесом, який активізується через заданий інтервал часу в автоматичному режимі. Процес здійснює виведення всіх активних черг та відправлення файлів засобами ІТК Держмитслужби України “Електронна пошта”.

Вилучення документів з черг проводиться програмою автоматично без втручання користувача. Для черг, що здійснюють виведення в форматах *cmf* або *imf*, вилучення документа з черги проводиться безпосередньо після його виведення. Для черг, що працюють з форматом *csnmsg*, вилучення документа з черги проводиться тільки після того, як отримано підтвердження з підрозділу-адресата про те, що документ надійшов.

За кожного виведення інформації створюється протокол (*Сервіс/ Налагодження програми /Загальні установки — на закладці Ввід-вивід* установлена відмітка *Зберігати протоколи виводу*). У разі ручного виведення інформації вікно з протоколом відкривається після закінчення виведення. Протоколи виведення можна переглянути в режимі *Документи/Ввід-вивід інформації/ Протоколи виводу*. При цьому можна задати параметри: *Тип виводу* (за окремими документами), *Черга та Дати протоколів*.

Залежно від типу та напрямку передачі інформація має різний формат (табл. 9.2).

Таблиця 9.2. Типи передачі та способи виведення інформації залежно від типу документа

Документ	Тип передачі	Тип виведення	Параметри простого виведення
ВМД в роботі	cmf	Простий + черга	За діапазоном дат, окремий документ, за списком
ВМД оформлені	cmf	Простий + черга	За діапазоном дат, окремий документ, за списком
ВМД всі (в роботі та оформлені)	csnmsg	Простий + черга	За діапазоном дат
Картки відмови	csnmsg	Черга	—

Закінчення табл. 9.2

Документ	Тип передачі	Тип виведення	Параметри простого виведення
ДМВ	cmf	Простий + черга	За діапазоном дат, окремий документ
ДМВ	csnmsg	Простий + черга	За діапазоном дат
МД-1	csnmsg	Простий	За діапазоном дат
Лист про погодження	csnmsg	Простий + черга	За діапазоном дат, окремий документ
Лист про погодження	cmf	Простий + черга	За діапазоном дат, окремий документ
ПВ/ПТП	cmf	Простий + черга	За діапазоном дат, окремий документ
ПИ/ПТП	csnmsg	Простий + черга	За діапазоном дат, окремий документ
Класифікаційні рішення	csnmsg	Простий + черга	За діапазоном дат, окремий документ
Довідки	csnmsg	Простий	За діапазоном дат, окремий документ
Платіжні документи	csnmsg	Простий + черга	Окремий документ
Зворотна інформація щодо аналізу ризиків	csnmsg	Черга	—

Введення інформації з митних підрозділів

Введенню підлягає інформація у форматі *csnmsg*, що була виведена з інших митних підрозділів. Введення інформації доступно тільки користувачам з повноваженням *Оператор вводу*.

Введення документів з інших підрозділів здійснюється за допомогою режиму *Документи/Ввід/Ввід інформації*. У вікні *Ввід інформації* (рис. 9.17) необхідно встановити:

- *джерело інформації*: ІТК Держмитслужби України “Електронна пошта”, папка або файл;
- *спосіб відправлення повідомлень про отримання в підрозділ*, з якого надійшла інформація засобами ІТК Держмитслуж-

Інспектор-2006

Від інформації

Джерело інформації

☐ Вести документи з електронної пошти

☐ Вести документи з указаної папки

☒ Вести документи з указанного файлу

Повідомлення про отримання

☐ Відправляти поштою автору

☒ Складати в папку

Успішно введені файли

☒ Вилучати

☐ Залишати на місці

☐ Складати в папку

Помилкові файли

☒ Вилучати

☐ Залишати на місці

☐ Складати в папку

Введення

Вести інформацію

Додаткові параметри

Параметри

Рис. 9.17. Вікно введення інформації з інших митних підрозділів

би України “Електронна пошта”: відразу автоматично будуть відправлятися поштою адресату або будуть вміщатися в окремому встановлену користувачем папку на диску для відправлення їх поштою вручну;

— *умову обробки вдало введених файлів*: вилучати або зберігати (на місці, звідки вибирались для введення, або в установлену користувачем папку);

— *умову обробки файлів, введених з помилками*: вилучати або зберігати (на місці, звідки вибирались для введення, або в установлену користувачем папку).

За допомогою кнопки *Додаткові параметри* можна вказати кількість днів, протягом яких програма зберігає на сервері некомплектні багатофайлові повідомлення.

Під час введення повідомлень, які були виведені з черг виведення, програма формує повідомлення — відповіді (повідомлення про отримання). Такі повідомлення необхідно відправляти в підрозділ, з якого надійшла інформація, — тільки після їх отримання документи там будуть вилучені з черги.

Процес введення починають натисканням кнопки *Ввести інформацію*. Після завершення введення активізується сторінка *Результати*, на якій розміщуються два вікна.

У першому вікні відображається список сформованих у процесі введення протоколів, серед яких можуть бути такі:

— *загальний протокол* — містить список оброблених файлів із загальною інформацією про кожен з них;

— *поштовий протокол* — формується, якщо введення здійснювалося з поштової скриньки, та призначений для налагодження пошти;

— *протоколи оброблених файлів* — формується для кожного файлу та містить список документів і результати їх обробки.

Результатом обробки документа можуть бути:

— *запис документа в базу даних*;

— *помилка* (рядок виділяється червоним кольором).

Крім того, якщо документ вже існував у базі даних, залежно від налагодження довіри до резюме відправника, можуть бути такі результати введення:

— *документ пропущено*;

— *документ перезаписано*;

— *документ розміщено в карантин*. Рішення про введення таких документів повинен прийняти користувач. Відповідні рядки в протоколі виділено жовтим кольором.

У режимі *Документи/Ввід/Протоколи вводу* користувач з правами *Оператор вводу* може переглянути список усіх протоколів, сформованих під час введення документів, або виконати пошук протоколів за типом та діапазоном дат формування:

— CSNDOC*.csnmsg — протокол прийому документів;

— CSNREPL*.csnmsg — протокол обробки підтвердження про отримання документів.

Обмін інформацією

Під час обміну інформацією програма “Інспектор-2006” використовує її криптографічний захист, вбудований в операційну систему *Windows* та інфраструктуру *Microsoft .NET Framework*.

Такий механізм криптографічного захисту інформації застосовується тільки для повідомлень у форматі програми “Інспектор-2006”.

Захист інформації виконується за допомогою симетричного шифрування. Програмно один раз на етапі формування нової бази даних для митного підрозділу створюється пара ключів — власний криптографічний ключ та його резюме (зовнішній ключ).

Власний ключ дає змогу підписати повідомлення з вашого підрозділу таким чином, що його отримувачі (за допомогою резюме ключа вашого підрозділу) можуть переконатися, що воно справді створено у вашому підрозділі. Криптографічний ключ, створений у підрозділі митної установи, є унікальним.

Резюме вашого ключа дає змогу іншим підрозділам зашифрувати для вашого підрозділу повідомлення таким чином, що ніхто, крім вас, не зможе його прочитати. Адже розшифрувати повідомлення можна лише за допомогою власного ключа вашого підрозділу.

Власний ключ необхідний для захисту інформації в процесі передачі даних між підрозділами митної установи. За допомогою ключів повідомлення шифруються таким чином, що розшифрувати їх може лише той отримувач, кому вони призначені, саме він може перевірити цілісність повідомлення та ідентифікувати відправника.

Для обміну інформацією у захищеному режимі митні підрозділи повинні здійснити обмін своїми резюме та сформувати перелік підрозділів, між якими планується обмін інформацією. Резюме не містить секретної інформації та може бути передано в інший підрозділ.

Налагодження режиму обміну інформацією виконує користувач з повноваженнями *Адміністратора бази даних*, а можливість перегляду надається користувачам з повноваженнями *Оператор вводу* або *Оператор виводу*.

Для передачі резюме вашого ключа в інший підрозділ використовують режим *Сервіс/Передача інформації/Власний ключ* (рис. 9.18). У вікні режиму вибирається посилання *Вивести резюме*, після чого вказується шлях до файлу резюме вашого ключа.

Для отримання резюме власних ключів інших підрозділів, які працюють з іншими екземплярами бази даних програми “Інспектор-2006” та здійснюють обмін інформацією з таким підрозділом, використовують режим *Сервіс/Передача інформації/Сторонні резюме* (рис. 9.18). Для збереження резюме власного ключа іншого підрозділу в панелі режиму вибирається посилання *Ввести резюме*, після чого вказується шлях до файлу резюме. За допомогою контекстного меню командою *Відкрити (F2)* надається можливість перегляду резюме, для якого на вкладинці *Довіра* виставляється позначка “•” для дій над тими типами повідомлень, які будуть прийматися програмою від його власника.

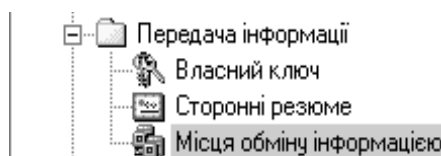


Рис. 9.18. Режими налагодження захисту передачі інформації

Сторонні резюме надають можливість вашому підрозділу визначати автора надісланого повідомлення та шифрувати повідомлення таким чином, щоб його зміг прочитати власник такого резюме.

Для створення переліку місць (адресатів), з якими планується здійснювати обмін інформацією використовують режим *Сервіс/Передача інформації/Місця обміну інформацією (митні адресати)*. У вікні цього режиму за допомогою посилання *Створити місце (адресата) для обміну інформацією* відкривається вікно для заповнення відомостей для місця (адресата) обміну інформацією.

Після обміну резюме між митними підрозділами та створення переліку адресатів, з якими буде здійснюватись обмін інформацією, програма “Інспектор-2006” в автоматичному режимі (без втручання користувачів) виконує криптографічний захист інформації в такому порядку.

Відправник	1. Шифрує інформацію, що виводиться, за допомогою резюме власного ключа одержувача. 2. Додає до повідомлення свій цифровий підпис (ключ) та відправляє одержувачу
Одержувач	1. Одержує пошту та перевіряє підпис відправника за допомогою його резюме. 2. Розшифровує інформацію своїм власним ключем та виконує введення

9.2. Автоматизована система аналізу та управління ризиками

Основні поняття

Митні органи у своїй діяльності зіштовхуються з цілим рядом складних завдань. Головними залишаються забезпечення надходжень до державного бюджету і захист економічних інтересів держави, але ці відповідальні завдання повинні здійснюватися ефективно й дієво, одночасно забезпечуючи підтримку потоку легальних товарів.

В останні роки акценти в здійсненні митної справи у світі зміщуються до застосування таких принципів: завчасний електронний обмін даними, послідовне застосування методів управління ризиками, використання нових технологій неруйнівного контролю під час огляду товарів і тісне співробітництво мит-

них органів між собою та з підприємствами (закріплені Рамковими стандартами Всесвітньої митної організації у 2005 р.).

У світовій практиці все більшої ваги набуває організація митної справи, заснована на управлінні ризиками, що дає змогу оптимально використовувати ресурси митних органів, контролювати здійснення митного оформлення на ділянках, де є найбільший ризик порушення митного законодавства, дозволяючи основній масі товарів і фізичних осіб порівняно вільно проходити через митницю.

Всесвітня митна організація визначає *управління ризиками* як систематичне застосування процедур і методів управління, що забезпечують митні органи необхідною інформацією для вивчення тих переміщень чи вантажів, які несуть у собі ризики. При цьому *ризиком* вважається потенційна можливість недотримання вимог митного законодавства.

У Концепції створення, запровадження і розвитку системи аналізу та керування ризиками Держмитслужби України *управління ризиками* визначається як систематична робота з розроблення та практичної реалізації заходів запобігання і мінімізації ризиків, методики оцінки ефективності їх застосування, а також контролю за застосуванням митних процедур, яка передбачає безперервне оновлення, аналіз і перегляд наявної у митних органах інформації.

Управління ризиками доцільно розглядати як інструмент забезпечення митної безпеки України. **Митна безпека України** визначається як стан захищеності економічних інтересів держави в галузі митної справи, який забезпечує в різних зовнішніх і внутрішніх умовах незалежно від будь-яких загроз:

- переміщення через митний кордон України товарів і транспортних засобів;
- здійснення митного регулювання, пов'язаного з установленням розмірів податків і зборів та повнотою їх справляння;
- застосування митних процедур, заходів митно-тарифного й нетарифного регулювання;
- боротьбу з контрабандою та порушеннями митних правил, а також виконання інших покладених на митну службу завдань шляхом ефективною реалізації митної справи.

Небезпека, загрози, виклики, негативний вплив, ризик, наслідки та шкода є системоутворювальними ознаками митної безпеки.

Загроза — така конкретна чи безпосередня форма небезпеки на стадії переходу її з можливості в реальність, яка характеризується сукупністю несприятливих умов і факторів у відповідних сферах економіки, конкретизується відповідною формою прояву й способом впливу на економічні процеси, наслідки якої можуть заподіяти будь-якої шкоди.

Зовнішні і внутрішні джерела небезпеки, що впливають на стан реалізації митної справи, найчастіше є результатом *суперечностей*, створюються і формуються в самому суспільстві, у зовнішньоекономічних і торговельних сферах, політичних і економічних відносинах, природних та інших явищах. Вони можуть виявлятися у вигляді різних загроз: війни, тривалих нестабільних політичних і економічних станів, протилежних економічних інтересів України й інших держав, не прорахованих прогнозів прийнятих тарифних і нетарифних заходів регулювання, некваліфікованого керівництва митною справою, порушення структурної організації керування митницею, формування негативного відношення суспільства до митниці та ін. Тому важливим є завдання щодо виявлення причин цих загроз з метою їх попередження і досягнення стану безпеки.

У контексті забезпечення митної безпеки **виклик** — це прояв загрози у формі події з негативними наслідками, який потребує відповідного реагування митних органів з метою попередження або зменшення можливої шкоди. **Шкода** — це фактичні або можливі економічні і соціальні втрати, що виникають у результаті різних подій, явищ, дій у митній галузі. Тоді можна визначити **ризик** як кількісну величину митного виклику у вигляді визначеної оцінки діючої небезпеки або ймовірності реалізації потенційної загрози в митній галузі з погляду небажаних наслідків.

Профілювання ризиків є засобом, за допомогою якого митні органи застосовують управління ризиками на практиці. Основним тут є поняття **індикаторів ризиків**, які можна визначити як певні критерії, що разом становлять практичний інструмент для вибірки й виявлення переміщень, що містять потенційну можливість порушення вимог митного законодавства. Власне, під **профілем ризику** прийнято розуміти визначений набір індикаторів ризику, відібраних на основі зібраної, проаналізованої й класифікованої інформації. Крім сукупності ін-

дикаторів ризику, профіль ризику характеризується також наявністю набору заходів з мінімізації ризику.

Профіль ризику найчастіше є документом, що може бути побудований різними способами (та використовуватись в документальному чи автоматизованому вигляді) і повинен містити опис сфери ризику, його оцінку, необхідні заходи з протидії ризику, терміни вжиття таких заходів. Під час розробки профілів ризику слід враховувати також особливості митних органів (пропускну здатність тощо), визначитись з очікуваними результатами й критеріями оцінки ефективності вжитих заходів.

Після розробки профільні характеристики разом з іншою інформацією й оперативними даними будуть забезпечувати основу для цільового виявлення потенційних переміщень вантажів, транспортних засобів або фізичних осіб з високим рівнем ризику.

Дієва система управління ризиками — це циклічний процес, який передбачає аналіз, оцінку ризику — формування профілю ризику — застосування профілю — моніторинг результатів застосування профілю.

Дуже важливим є етап застосування профілів ризику під час митного контролю та митного оформлення. Від його організації залежить як прискорення митних процедур, так і одночасне забезпечення ефективного контролю за дотриманням митного законодавства. Обсяг механізмів контролю, що застосовуються митними органами для забезпечення дотримання законодавства, повинен бути пропорційний рівню оціненого ризику. Рівень ризику визначається в контексті пріоритетів митних органів (забезпечення своєчасності та повноти справляння податків і зборів, перевірка дотримання заборон і обмежень чи інша специфічна сфера).

Процес управління ризиками

Розглянемо загальноприйняті у світі підходи до організації ризик-менеджменту в митній справі.

Процес управління ризиками (рис. 9.19) містить установку контексту управління ризиками, їх визначення, аналіз, оцінку, вживання заходів щодо них, а також моніторинг і перевірку процесу за допомогою оцінки відповідності необхідним вимогам.

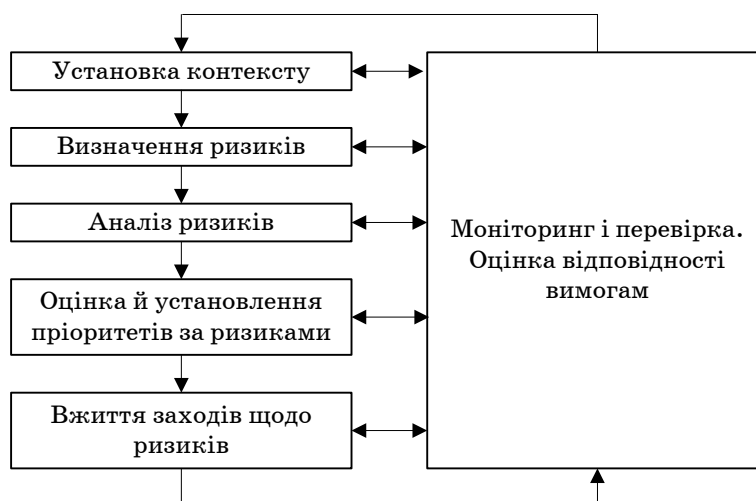


Рис. 9.19. Процес управління ризиками

Етап *установки контексту* передбачає визначення сфер ризику та установлення критеріїв, на основі яких ризики будуть оцінюватися.

Етап *визначення ризиків* передбачає з'ясування того, які ризики, чому і як можуть виникнути. Цей етап вимагає ретельного опрацювання таких питань, як:

- де, коли і як, швидше за все, виникне ризик і хто буде його суб'єктом;
- які небезпеки можуть виникнути і який їх негативний вплив;
- чому виникають можливості для окремого порушення.

На етапі *аналізу ризиків* слід визначити механізми контролю й проаналізувати ризики стосовно ймовірності їх виникнення та наслідків.

Оцінка й установлення пріоритетів за ризиками передбачає розподіл ризиків для визначення пріоритетів управління. Є різні види систем класифікації. Особливо поширена оцінка за високим, середнім і низьким рівнями ризику. Може знадобитися більш детальна система, наприклад, класифікація за рівнями від 1 до 100.

Ризики повинні бути під постійним моніторингом на предмет зміни їх характеру, рівня або значимості.

Вжиття заходів за ризиками. Доцільно проводити моніторинг низькопріоритетних ризиків. Для інших ризиків слід розробити і реалізувати конкретний план управління, що включає урахування ресурсів митних органів (кадрових, фінансових і технічних).

Моніторинг і перевірка — оцінка відповідності вимогам. Щоб залишатися ефективною, будь-яка система управління ризиками повинна проводити оцінку раніше визначених ризиків. Оцінка ефективності має здійснюватися на регулярній основі на всіх етапах, її метою є визначення слабких місць у механізмах контролю й подання рекомендацій з удосконалення.

Також важливо підтримувати елемент несподіванки шляхом проведення випадкових перевірок, оскільки підприємства, що перебувають у постійному контакті з митними органами, можуть знати про методи профілювання чи навіть про самі профільні характеристики. Такі випадкові перевірки можуть бути засобом визначення інших видів ризиків, засобом моніторингу або оцінки їх значимості чи яких-небудь змін у типі ризику.

“Оцінка відповідності вимогам” — термін, що використовується під час застосування техніки статистично обґрунтованої випадкової вибірки з метою визначення того, наскільки торговельні суб’єкти, перевізники, товари тощо відповідають митним правилам і процедурам.

Під час стратегічного використання випадкова оцінка відповідності вимогам і цілеспрямований підхід до застосування заходів контролю можуть забезпечити необхідний баланс для ефективної концентрації ресурсів у сферах, що представляють проблемні для митниці питання. Крім того, результати первісних оцінок відповідності вимогам можуть надати важливу інформацію для вдосконалення методологій оцінки ризиків, простежування тенденцій і питань, що стосуються конкретних галузей економіки.

Індикатори ризиків

У процесі здійснення митної справи індикатори ризиків визначаються за допомогою конкретно виражених критеріїв вибірковості, таких як конкретний код товару, країна походжен-

ня, країна відправлення вантажу, вартість, торговельний суб'єкт, тип транспортного засобу, мета перебування на митній території тощо.

До найбільш вагомих індикаторів ризиків, що стосуються товарів, належать, в основному, митно-тарифне регулювання (при цьому основна увага звертається на товари, які мають значні обсяги переміщення і забезпечують надходження найбільших сум митних платежів; товари, щодо яких застосовуються високі ставки ввізних та вивізних мит; товари групи “прикриття”, щодо яких застосовуються низькі ставки мита і ставки, менші від тих, що застосовуються до товарів, класифікованих у тій самій товарній позиції та/або за своїми характеристиками і зовнішнім виглядом належать до них), походження товарів (товари, які декларуються походженням з країн, з якими Україною укладені угоди про вільну торгівлю; товари, щодо яких є інформація про відсутність виробництва або товари, виробництво яких є нехарактерним для певної країни), вартість товарів (заявлена митна вартість товарів значно відрізняється від ціни ідентичних чи подібних товарів під час їх увезення на митну територію України чи значно завищена під час їх вивезення за межі митної території України).

Стосовно індикаторів ризиків, які належать до діяльності суб'єктів зовнішньоекономічної діяльності, тут аналізуються особливості зовнішньоекономічної угоди (товари переміщуються за контрактами, відмінними від договорів купівлі-продажу, в яких не наведено суттєвих умов угоди; одна зі сторін зовнішньоекономічного договору зареєстрована в офшорній зоні; учасники зовнішньоекономічного договору (контракту) мають ознаки “фірм-одноденки”¹), враховуються дані про попередні порушення митних правил, інформація про протиправну діяльність цих суб'єктів, їх засновників, фактичних власників тощо, отримана від правоохоронних, податкових або інших компетентних органів України та іноземних держав, а також від міжнародних організацій.

¹ Поняття визначено Законом України “Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом” від 6 лютого 2003 р. № 345-IV.

Концептуальний підхід Митної служби України до застосування профілів ризику під час митного контролю та митного оформлення

У Держмитслужбі України застосування профілів ризику під час митного оформлення здійснюється за допомогою спеціального модуля автоматизованої системи аналізу й управління ризиками, імplementованого до автоматизованої системи митного оформлення вантажів. Основне завдання цього модуля — на підставі усіх введених до нього профілів ризику здійснити оцінку ризику ВМД, яка подана до митного оформлення, та видати повідомлення з вказівками необхідних заходів, що слід зробити для перевірки законності зовнішньоекономічної операції посадовій особі, яка здійснює митне оформлення та митний контроль (далі — інспектор).

Дані, які містяться в електронній копії ВМД та інших документах, що подаються разом із нею в електронному вигляді, перевіряються на відповідність індикаторам, що містяться в профілях ризику. Крім індикаторів, кожний профіль ризику обов'язково містить порядок обчислення ступеня ризику (під *ступенем ризику* тут розуміємо числове значення у визначених межах, яке показує ймовірність порушення митного законодавства в конкретному випадку і, відповідно, передбачає здійснення адекватних такому ризику заходів) та перелік форм контролю, які слід здійснити інспектору для перевірки законності цієї зовнішньоекономічної операції.

Процес аналізу здійснюється у два основні етапи: спочатку оцінка ризику за кожним профілем ризику; потім визначення переліку форм контролю в цілому за ВМД.

На першому етапі для кожного профілю ризику спочатку визначається ступінь ризику. Це число визначається по-різному в кожному профілі ризику залежно від його особливостей. Зокрема, ступінь ризику залежить від комбінації індикаторів, які спрацювали, та їх значень. Під час оцінювання значень індикаторів за доцільності застосовуються елементи нечіткої логіки.

Модуль аналізу ризиків повинен враховувати у процесі оцінювання ризику попередню поведінку суб'єкта ЗЕД. У базі даних митного органу (в окремих випадках — централізовано —

наприклад, в центральній базі даних) накопичується інформація про так звані позитивні та негативні історії.

Як показник, *негативна історія* суб'єкта ЗЕД за профілем ризику характеризує наявність за певний період у минулому порушень митного законодавства, пов'язаних із ризиком, описаним у профілі ризику. *Позитивна історія* суб'єкта ЗЕД за профілем ризику характеризує наявність за певний період у минулому фактів митного оформлення, які підтвердили відсутність порушень митного законодавства, пов'язаних із ризиком, описаним у профілі.

Отже, якщо суб'єкт у минулий період (наприклад, за останні 2 роки) порушував законодавство України з питань митної справи і ці факти зафіксовано відповідними документами та занесено до відповідних баз даних, то значення негативної історії для такого суб'єкта буде більше нуля і врахується під час підрахунку ступеня ризику. Значення негативної історії залежатиме від характеру зафіксованого порушення, адже для кожного профілю ризику певні порушення можуть бути більш вагомими, а деякі — взагалі несуттєвими.

Однак наявність негативної історії ще не означає, що у зв'язку з минулими порушеннями суб'єкт ЗЕД постійно підпадатиме під певний профіль ризику і буде підлягати посиленому контролю. Ефект негативної історії за профілем ризику може перекритися значенням позитивної історії, якщо такий суб'єкт за минулий період уже проходив посилену перевірку під час митного контролю та митного оформлення (за результатами спрацювання цього профілю ризику) і порушень не було виявлено. Такі факти теж фіксуються у відповідних базах даних і враховуються у процесі підрахунку ступеня ризику за профілем.

Як уже зазначалося, кожний профіль ризику визначає специфічні для нього форми контролю. Наприклад, для профілю, який спрямований на виявлення ризику подання неправдивих відомостей про країну походження товару, доцільним є підтвердження відповідності заявлених даних про країну походження товарів. Для профілю ризику, що розроблений з метою оцінки ризику декларування певного товару не своїм найменуванням (наприклад, для мінімізації митних платежів чи обходу нетарифних обмежень), доцільно провести митний огляд з

метою ідентифікації товарів. Таким чином, можна сказати, що мета форми контролю залежатиме від характеру можливого порушення, а власне форма контролю (перевірка документів та відомостей, митний огляд чи інші форми митного контролю) — від ступеня ризику.

Після перевірки усіх профілів ризику, визначення форм контролю за кожним профілем здійснюється завершальний етап — формування загального переліку форм контролю за ВМД з відповідними коментарями для вказівки інспектору, на що направлена ця форма контролю.

У результаті, інспектор отримує перелік форм контролю, які необхідно здійснити за такою ВМД, додаткову інформацію про особливості ризику чи мету форм контролю. Після виконання виданих вказівок, інспектор фіксує дані про результати їх виконання — ця інформація використовується згодом для оцінки ефективності впроваджених профілів ризику та розробки нових.

Ще одна особливість, яку слід зазначити, — випадковий вибір форми контролю.

У багатьох країнах, у тому числі в розвинутих державах із значним обсягом міжнародного потоку товарів, є практика так званого випадкового чи відсоткового огляду — коли митний огляд проводиться лише для певного відсотка вантажів, наприклад, доглядається кожний сотий вантаж. Звичайно, такий підхід не гарантує ефективного контролю, особливо, якщо принцип відбору достатньо передбачуваний. Зараз світова практика схиляється до використання більш інтелектуальних методів відбору об'єктів перевірки — застосування управління ризиками, однак присутній і випадковий вибір.

Модуль аналізу ризиків використовує своєрідний підхід до випадкового контролю. Основна його особливість — залежність від обчисленої ризикованості зовнішньоекономічної операції. Такий підхід видається гнучким і зваженим: чим надійніший суб'єкт ЗЕД (адже у процесі підрахунку ступеня ризику враховується його історія), тим менша ймовірність того, що його вантаж підпаде під випадкову форму контролю. Для інспектора такий підхід зручний тим, що вибрана таким чином форма контролю, хоч і випадкова, але корельована з характером можливого порушення. І, щоб передбачити такий випадок,

коли під час аналізу конкретної ВМД не спрацювало жодного профілю ризику (така ситуація може бути і вона ще не означає, що ризику немає), необхідно ввести елемент випадкового вибору за відсутності спрацьованих профілів ризику. У такому випадку ймовірність того, що вантаж буде вибраний для митного огляду, зовсім мала.

Щоб підвищити інформативність роботи модуля аналізу ризиків, результат перевірки ВМД позначається відповідним кольором (табл. 9.3).

Таблиця 9.3. Індикація ВМД за результатами аналізу ризиків

Колір індикації за ВМД	Значення
Зелений	За ВМД модулем аналізу ризиків не виявлено ризику. Зелений колір означає, що в модуля аналізу ризиків немає даних щодо ризикованості зовнішньоекономічної операції. Тому рішення про проведення форм контролю за ВМД приймається інспектором самостійно
Жовтий	За ВМД модулем аналізу ризиків виявлено ризик та сформовано перелік форм контролю. Усі форми контролю передбачають здійснення документальної перевірки та інших заходів, що не потребують огляду вантажу чи транспортних засобів
Червоний	За ВМД модулем аналізу ризиків виявлено ризик та сформовано перелік форм контролю, які передбачають здійснення заходів, що потребують огляду вантажу чи транспортних засобів

Підбиваючи підсумки, слід зазначити, що висвітлені підходи мають на меті підвищити ефективність роботи митних органів України, підняти рівень застосування в митній справі методів аналізу та управління ризиками. З часом підходи до профілювання ризиків будуть вдосконалюватися, змінюватися, однак застосування таких інструментів, як нечітка логіка, не-

гативна та позитивна історії, очевидно, залишатиметься актуальним.

Застосування нечіткої логіки під час оцінювання ризику

Важливим завданням митної служби є гнучке та диференційоване визначення індикаторів ризику на підставі наявного практичного досвіду та науково обґрунтованих розрахунків.

Щодо числових індикаторів ризиків, буває досить складно визначити їх оптимальне значення. Найкращим прикладом такого індикатора є митна вартість товару.

Традиційний спосіб визначення величини ступеня ризику залежно від значення митної вартості (рис. 9.20) передбачає лінійну залежність між цими показниками з різким стрибкоподібним переходом ступеня ризику від 1 до 0 в точці, яка відповідає визначеному значенню митної вартості товару (на рис. 9.20 — 40 грн/кг).

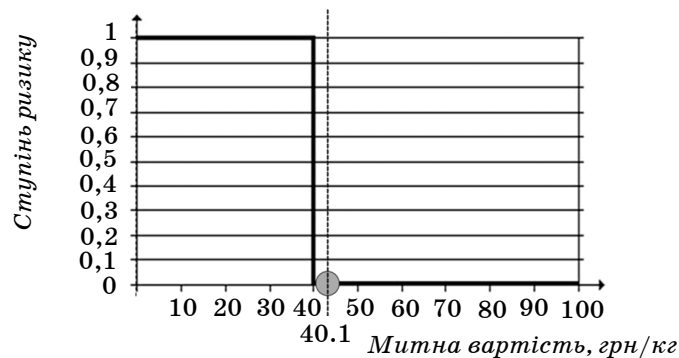


Рис. 9.20. Графік залежності ступеня ризику від митної вартості

Таким чином, для всіх товарів, митна вартість яких не перевищує 40 грн/кг, ступінь ризику завжди буде 1, а для товарів, митна вартість яких становить більше 40 грн/кг, ступінь ризику завжди дорівнює 0. У результаті митне оформлення здійснюється для товарів із митною вартістю близькою до критичної.

Для вирішення цієї проблеми використовується нечітка логіка (рис. 9.21).

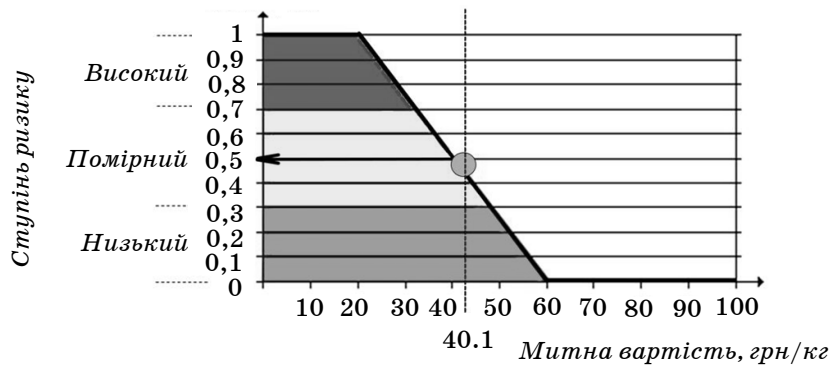


Рис. 9.21. Використання нечіткої логіки

Під час введення нечіткої логіки для визначення ступеня ризику, ризику змінюються від 0 до, наприклад, 0,5 у процесі митного оформлення товару з митною вартістю 40,1 грн/кг.

Використання нечіткої логіки під час визначення ступеня ризику дає змогу підвищити гнучкість його оцінки із застосуванням додаткових параметрів, таких як позитивна та негативна історії. Так, за наявності позитивної історії ступінь ризику зменшується (рис. 9.22).

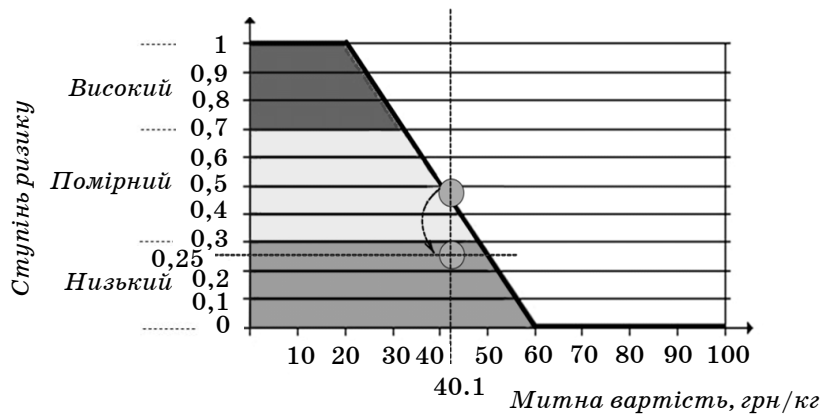


Рис. 9.22. Вплив позитивної історії

У випадку, наведеному на рис. 9.22, за позитивної історії $\Pi_i = 0,25$ ступінь ризику зменшується до 0,25.

За наявності негативної історії ступінь ризику збільшується (рис. 9.23).

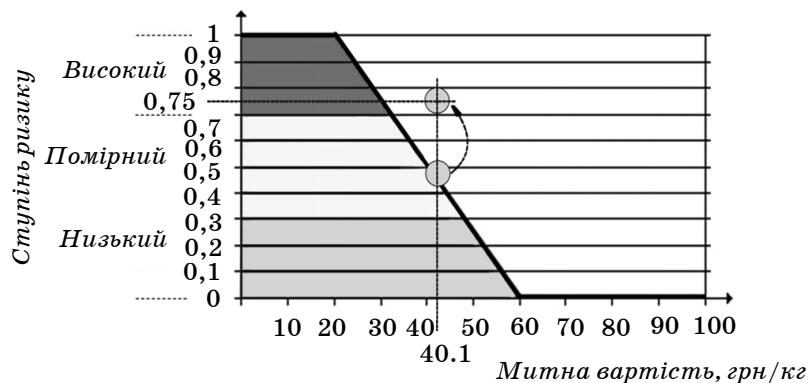


Рис. 9.23. Вплив негативної історії

У випадку, наведеному на рис. 9.23, за негативної історії $H_i = 0,25$ ступінь ризику збільшується до 0,75.

Таким чином, із використанням нечіткої логіки можна досягнути бажаної гнучкості під час врахування таких складних індикаторів, як митна вартість товару.

Підсумки

Перед митними органами України гостро стоїть завдання наповнення державного бюджету. Разом із цим, одним з основних завдань, які ставляться перед митною службою, є сприяння розвитку зовнішньої торгівлі, що тісно пов'язане зі спрощенням митних процедур. Однак лібералізація торгівлі повинна узгоджуватись із захистом економічних інтересів держави. Впровадження в організацію митної справи методів управління ризиками може забезпечити зважений підхід держави у на-

прямі спрощення митних процедур і водночас забезпечення надходжень до держбюджету, забезпечення економічної безпеки держави.

Запитання і завдання для самоконтролю

1. Для чого призначена та які завдання дає змогу вирішувати програма “Інспектор-2006”?
2. На базі якого програмного забезпечення можливе використання програми “Інспектор-2006”?
3. Розтлумачте термін “архітектура клієнт-сервер”.
4. Які параметри роботи програми “Інспектор-2006” встановлюються за допомогою режиму *Сервіс/Налагодження програми/Загальні установки*?
5. У чому полягає призначення профілів та як вони використовуються у програмі “Інспектор-2006”?
6. Які можливості надаються користувачам із повноваженнями *Адміністратор бази даних, Адміністратор SQL-сервера, Оператор виводу*?
7. Як забезпечується розподіл прав доступу під час роботи з програмою “Інспектор-2006”?
8. Яке призначення та застосування режиму *Сервіс/Налагодження програми/Технології проходження ВМД* ?
9. Поясніть зв’язок між режимами *Локальні підрозділи* і *Технології проходження ВМД*.
10. Яким чином налагодити автоматичне формування номерів ВМД у митному підрозділі?
11. Обмін інформацією якого вмісту можна виконати між базами даних за допомогою програми “Інспектор-2006”?
12. Для чого призначений режим введення-виведення інформації у програмі “Інспектор-2006”?
13. Якими способами можна здійснити виведення інформації у програмі “Інспектор-2006”? Надайте характеристику кожному з них.
14. Як виконати налагодження черг виведення інформації у програмі “Інспектор-2006”?

15. Надайте перелік можливих методів виведення черг документів. Як кожний з цих методів можна реалізувати у програмі “Інспектор-2006”?
16. Черги яких документів можна вивести вручну та автоматично? Які типи документів виводяться лише автоматично?
17. Який порядок введення інформації з митних підрозділів?
18. Для чого призначені протоколи введення-виведення інформації?
19. Протоколи якого вмісту формуються у результаті введення інформації з митних підрозділів?
20. Які результати обробки документа можливі внаслідок введення інформації з митного підрозділу?
21. Поясніть, у чому полягає сутність симетричного шифрування. Яке призначення власного ключа та резюме?
22. Як виконується налагодження системи захисту інформації у програмі “Інспектор-2006”?
23. Охарактеризуйте поняття митної безпеки.
24. Що таке ризик у контексті митної справи? Які основні складові процесу управління ризиками?
25. Що таке профіль ризику?
26. Які нормативно-правові акти регулюють застосування системи аналізу та управління ризиками в Держмитслужбі України?
27. Дайте короткий опис побудови автоматизованої системи аналізу та управління ризиками, що застосовується під час митного оформлення в Держмитслужбі України.

Розділ 10

ПРОГРАМНО-ІНФОРМАЦІЙНІ КОМПЛЕКСИ ЄАІС ДМСУ

10.1. Програмно-інформаційний комплекс “Квитанції МД-1”

Призначення

Розробку програмного забезпечення “*Квитанція МД-1*” (далі — режим МД-1) виконано для обліку операцій із застосуванням уніфікованої митної квитанції МД-1 (далі — УМК), Порядок застосування якої затверджений наказом Держмитслужби України “Про затвердження Порядку застосування уніфікованої митної квитанції МД-1” від 4 січня 2005 р. № 1, що передбачає:

- прийняття на зберігання митним органом товарів відповідно до законодавства;
- справляння митним органом з фізичних осіб та підприємств платежів, якщо законодавством не передбачено складання вантажної митної декларації на переміщенні через митний кордон України товари;
- справляння митним органом з фізичних осіб грошової застави у випадках, установлених законодавством.

Режим МД-1 призначений для заповнення уповноваженими особами митного органу бланків УМК і додаткових аркушів, формування в електронному форматі інформації з УМК з можливістю її перегляду, редагування, вилучення, а також для списання коштів для торгового обігу та перегляду інформації списання коштів.

Режим МД-1 дає можливість посадовим особам митних органів передавати електронні копії УМК до центральної бази даних Єдиної автоматизованої інформаційної системи Держмитслужби України та бази даних митного органу.

База даних УМК митного органу використовується митними органами для здійснення контролю за правильністю справляння за УМК платежів і грошової застави, аналізу й прогнозування обсягів надходжень до Державного бюджету України.

Умови застосування та запуск ПІК

Режим МД-1 доступний у навігаторі програми “Інспектор-2006”. Доступ до режиму МД-1 можливий за наявності у користувача повноваження *Перегляд МД-1* або повноваження *Адміністратор бази даних* і містить такі підпорядковані режими: *МД-1* та *Ввід-вивід*.

Робота в режимі МД-1. Підрежим *Створити* призначений для введення в базу даних інформації УМК. На екран виводиться робоче вікно для заповнення полів документа:

- на сторінку *Загальні відомості* заноситься загальна інформація УМК;

- на сторінку *Товари* заноситься інформація про товари. Поля цієї сторінки доступні для занесення інформації тільки для певних типів МД-1.

Кнопка  *Розрахунок загальної суми платежів* на панелі інструментів призначена для перенесення (з підсумовуванням) платежів за товарами з розділу *Нарахування платежів та зборів* сторінки *Товари* у розділ *Подробиці підрахунків* сторінки *Загальні відомості*.

Кнопка  призначена для створення нової МД-1 шляхом копіювання поточної МД-1. У створеній таким чином копії МД-1 поля *Серія*, *Номер* не заповнені, дата у графі *Дата оформлення* замінена на поточну дату, платежі перераховані станом на поточну дату. Для запису нового документа в базу даних необхідно заповнити поля *Серія*, *Номер* та, за потреби, внести зміни в інші поля.

Інші кнопки панелі інструментів цього вікна мають таке саме призначення, що й відповідні кнопки панелі інструментів вікна режиму перегляду ВМД.

Підрежим *Відкрити* призначений для завантаження на екран електронної копії позначеного у переліку документа для перегляду або редагування.

Підрежим *Вилучити* призначений для вилучення з бази даних електронної копії документа.

Підрежим *Списання коштів* (наводиться в меню за наявності у користувача повноважень роботи з платежами) призначений для списання платежів за вказаною МД-1. Під час входження в цей підрежим відкривається вікно з інформацією про ті платежі, які підлягають списанню. Кнопки панелі інструментів цього вікна мають таке саме призначення, що й відповідні кнопки панелі інструментів вікна режиму списання платежів за ВМД.

У процесі входження в режим *Списання коштів* за умови, що списання платежів уже відбувалось, на екран виведеться вікно для редагування списання платежів.

Підрежим *Вивід МД-1 в ЦБД* призначений для виведення у зовнішній файл позначеної у переліку МД-1. На екран виводиться вікно *Вивід МД-1 (не автотранспорт) в ЦБД*, у якому слід указати місце виведення інформації: директорію на диску або адресу електронної пошти. Після натиснення кнопки *ОК* на екрані формується протокол вихідної інформації.

Підрежимами *Вивід в Excel*, *Попередній перегляд*, *Друк списку* призначені для виконання зазначених дій з виведеним на екран переліком документів.

Режим *Ввід-Вивід* призначений для виведення оформлених МД-1 у зовнішній файл або на поштову скриньку для пересилання їх у ЦБД чи інший підрозділ митного органу. Для здійснення введення-виведення інформації користувач повинен мати повноваження *Перегляд МД-1* або *Адміністратор бази даних*.

У робочому вікні режиму надаються такі варіанти виведення:

- *Вивід оформлених МД-1 (крім автотранспорту) в ЦБД*;
- *Вивід інформації по МД-1 в інший підрозділ митниці*.

Після вибору одного з варіантів виводиться вікно *Критерії відбору*, в якому вказується необхідний діапазон дат. За клавішею  послідовно відкриваються вікна *Отримувач повідомлення* (у випадку виведення в інший підрозділ), *Місце виводу* та *Формат виводу* (у випадку виведення в інший під-

розділ) для занесення відповідної інформації. Після натиснення клавіші *OK* останнього вікна відкривається протокол виведення інформації, в якому зазначається ім'я сформованого файлу.

10.2. Програмно-інформаційний комплекс “Аналітична та статистична обробка інформації про порушення суб’єктами ЗЕД чинного законодавства”

Призначення

Програмно-інформаційний комплекс “Аналітична та статистична обробка інформації про порушення суб’єктами ЗЕД чинного законодавства” розроблено для автоматизації підготовки статистичних звітів та аналітичної обробки інформації з питань порушення чинного законодавства і на виконання наказу ДМСУ “Про внесення змін до наказу Держмитслужби від 13 лютого 2002 р. № 96” від 21 серпня 2002 р. № 460.

Формування статистичних звітів та аналітична обробка інформації з питань порушення чинного законодавства зазначеним програмно-інформаційним комплексом базується на наявній в Єдиній автоматизованій інформаційній системі інформації про контрабанду та порушення митних правил, накопиченій в ЄАІС за допомогою програмно-інформаційного комплексу (ПІК) “Боротьба з контрабандою та порушеннями митних правил”, введеного у дослідну експлуатацію з 14 травня 2001 р. наказом Держмитслужби від 28 березня 2001 р. № 217.

ПІК призначено для посадових осіб Департаменту організації боротьби з контрабандою та порушеннями митних правил ДМСУ, регіональних митниць і митниць.

Умови застосування

Програмно-інформаційний комплекс базується на концепції трирівневої мережі з центральним сервером баз даних і серверами ЄАІС Держмитслужби України. Центральний сервер БД і сервери ЄАІС ДМСУ розміщуються в Департаменті інфор-

маційних технологій та митної статистики (далі — ДІТМС). Призначені для користувача процедури зберігаються на web-сервері й запускаються користувачем з робочих станцій (функціональних робочих місць митних органів із застосуванням стандартних засобів операційних систем, наприклад, Internet Explorer Version 3.0 і вище в системі Windows 98/ME/NT/2000/XP). Митні органи повинні мати окрему робочу станцію та засоби оперативного зв'язку каналами супутникового або комутованого зв'язку.

Оперативний доступ до ПІК “Аналітична та статистична обробка інформації про порушення суб'єктами ЗЕД чинного законодавства” в ЄАІС здійснюється каналами супутникового або комутованого зв'язку за адресою: <https://XXX.XX.XX.XXX/>, “Контрабанда”, “Аналітична та статистична обробка інформації про порушення суб'єктами ЗЕД чинного законодавства”.

Доступ до ПІК “Аналітична та статистична обробка інформації про порушення суб'єктами ЗЕД чинного законодавства” надається посадовим особам митних органів України, зареєстрованим в ЄАІС Держмитслужби як користувачі цього ПІК. Права доступу до ПІК надаються згідно з Порядком регламентованого доступу користувачів до ЄАІС Держмитслужби України, затвердженим Наказом Держмитслужби України під грифом ДСК (для службового користування) 2002 р.

Робота ПІК

Робота з ПІК “Аналітична та статистична обробка інформації про порушення суб'єктами ЗЕД чинного законодавства” передбачає можливість формування таких звітів.

- “Інформація про заведення та розгляд справ про ПМП митницею”.
- “Інформація про розгляд судами справ про порушення митних правил”.
- “Довідка про правоохоронну діяльність”, яка включає кілька звітів, а саме:
 - “Предмети, сировина, матеріали, промислові та продовольчі товари, сільгосппродукція, валюта, що затримані у справах про ПМП”;

- “Автомобілі, затримані під час спроби їх незаконного переміщення через митний кордон України”;
- “Дорогоцінні метали, коштовне каміння та вироби з них”;
- “Історичні та культурні цінності”;
- “Зброя, боеприпаси та вибухові речовини”;
- “Наркотики та наркотичні речовини”;
- “Радіоактивні та небезпечні матеріали”.

Формування звітів

Для формування кожного звіту потрібно на головній веб-сторінці ПІК вибрати назву митного органу з довідника, вказати звітний період (початкову та кінцеву дати) і сформувати необхідний звіт. Дата формування вводиться програмно із системної дати.

У ПІК здійснюється аналіз коду користувача. Для користувачів Центрального апарату Держмитслужби доступний весь перелік митних органів. Під час вибору митного органу формується потрібний звіт за ним. Якщо митний орган не вибрано — формується звіт для Держмитслужби.

Для користувачів регіональних митниць доступний перелік митниць свого регіону і звіти формуються за вибраною митницею або для регіону. Для користувачів митниць здійснюється формування звітів для митниці.

10.3. Програмно-інформаційний комплекс “Реєстр дозволів на право відкриття складів тимчасового зберігання”

Призначення

Програмно-інформаційний комплекс “Реєстр дозволів на право відкриття складів тимчасового зберігання” розроблено для автоматизації процесу обліку складів тимчасового зберігання в Єдиній автоматизованій інформаційній системі Держмитслужби України, створення і діяльність яких відбувається відповідно до ст. 99—109 Митного кодексу України та Поло-

ження про склади тимчасового зберігання, затвердженого наказом Держмитслужби від 7 жовтня 2003 р. № 674 і зареєстрованого в Міністерстві юстиції 19 листопада 2003 р. № 1061/8382.

ПІК призначено для ведення Реєстру дозволів на право відкриття складів тимчасового зберігання (далі — Реєстр дозволів) (уведення, редагування, анулювання/скасування дозволів) свого митного органу, перегляду інформації та отримання звіту за Реєстром дозволів будь-якого митного органу посадовими особами регіональних митниць, митниць.

Умови застосування

Програмно-інформаційний комплекс базується на концепції розбудови трирівневої мережі з центральним сервером баз даних і серверами Єдиної автоматизованої інформаційної системи Держмитслужби, розміщеними в Департаменті інформаційних технологій.

Призначені для користувача процедури зберігаються на web-сервері й запускаються користувачем з робочих станцій (функціональних робочих місць митних органів із застосуванням стандартних засобів операційних систем, наприклад, Internet Explorer Version 5.0 і вище в системі Windows 98/ME/NT/2000/XP).

ПІК “Реєстр дозволів на право відкриття складів тимчасового зберігання” в ЄАІС Держмитслужби розміщено в розділі “Митне оформлення”, підрозділах “Митне оформлення”, “Реєстр дозволів на право відкриття складів тимчасового зберігання”. Оперативний доступ до ЄАІС Держмитслужби здійснюється каналами зв’язку за адресами: <https://XXX.XX.XX.XXX/>.

Доступ до ПІК “Реєстр дозволів на право відкриття складів тимчасового зберігання” в ЄАІС Держмитслужби з правом ведення і перегляду Реєстру дозволів за інформацією свого митного органу надається посадовим особам регіональних митниць, митниць, зареєстрованим як користувачі ПІК ЄАІС Держмитслужби, яким надано права доступу до цього ПІК (за відповідними кодами задачі та кодами ролей).

Під час роботи з ПІК на екран виводиться запит імені користувача та пароля. Під час введення зазначених параметрів та їх підтвердження здійснюється перевірка прав доступу користувача до ПІК і виводиться головна web-сторінка ПІК.

Режими ПІК

Робота з ПІК “Реєстр дозволів на право відкриття складів тимчасового зберігання” залежно від прав, наданих користувачу, передбачає виконання таких режимів:

- внесення інформації про новий дозвіл;
- перегляд дозволів;
- редагування, анулювання та скасування дозволів;
- реєстр дозволів від дати початку до дати закінчення періоду.

Для реалізації кожного з режимів на головній web-сторінці ПІК потрібно виконати такі дії: зазначити назву митного органу (програмно наведено назву митного органу користувача ПІК, у разі потреби її можна відкоригувати з довідника) і проставити позначку біля назви необхідного режиму.

Примітка. Під час входу в ПІК програмно здійснюється аналіз коду користувача і визначається належність користувача до певного митного органу.

За наявності помилок у введеній користувачем інформації на екран видається відповідне повідомлення. Порядок дій користувача в таких випадках визначається змістом повідомлення.

У разі повідомлення про помилку слід повернутись до екранної форми, що містить введену користувачем інформацію, візуально перевірити правильність інформації та внести потрібні зміни.

Повідомлення про неправильний формат видається у разі введення символьної інформації в цифрові поля та недотримання розмірності поля. Повідомлення про неправильний формат дати видається під час порушення формату дати.

Якщо видано повідомлення про незаповнене обов’язкове поле, його заповнюють вручну або вибирають потрібне значення з довідника.

Повідомлення “Помилка запису ORACLE, інформація не занесена” видається за наявності у введеній користувачем інформації помилок, що не визначаються ПІК. Правильність інформації в цьому випадку перевіряють візуально.

10.4. Програмно-інформаційний комплекс “Контроль за переміщенням вантажів при транзиті”

Призначення

Програмно-інформаційний комплекс “Контроль за переміщенням вантажів при транзиті” призначено для посилення контролю за доставкою вантажів у митниці призначення з використанням центральної бази даних (ЦБД) Єдиної автоматизованої інформаційної системи Державної митної служби України.

ПІК забезпечує оперативний доступ до ЄАІС службовим особам митних органів, до функцій яких входить оформлення пропуску вантажів і контролю за переміщенням вантажів.

Комплекс використовується службовими особами відділу контролю за переміщенням товарів митного органу під час виконання функцій контролю доставки товарів у митниці призначення і службовими особами пункту пропуску митного органу під час оформлення та пропуску вантажів.

Умови застосування

ПІК “Контроль за переміщенням вантажів при транзиті” базується на концепції трирівневої мережі з центральним сервером баз даних і центральним web-сервером, розміщеними в Департаменті інформаційних технологій і митної статистики Держмитслужби України.

Призначені для користувача процедури зберігаються на web-сервері й запускаються користувачем з робочих станцій (функціональних робочих місць митних органів із застосуванням стандартних засобів операційних систем, наприклад, Internet Explorer Version 3.0 і вище в системі Windows 98/ME/NT/2000/XP).

Оперативний доступ до ПІК “Контроль за переміщенням вантажів при транзиті” здійснюється каналами зв'язку із застосуванням web-серверів “ЄАІС ДМСУ” за адресами: <https://XXX.XX.XX.XXX/>, розділ “Доставка вантажів”, підрозділ “Транзит”.

Доступ до ПК “Контроль за переміщенням вантажів при транзиті” в ЄАІС Держмитслужби з правом введення і перегляду інформації про доставку вантажів надається посадовим особам регіональних митниць і митниць, зареєстрованим як користувачі ПК ЄАІС Держмитслужби, за відповідним кодом завдання “Контроль доставки товарів” та кодом ролі “Відділ контролю доставки”.

Доступ до ПК “Контроль за переміщенням вантажів при транзиті” в ЄАІС Держмитслужби з правом введення інформації про пропуск вантажів надається посадовим особам регіональних митниць, митниць та їх структурних підрозділів, зареєстрованим як користувачі ПК ЄАІС Держмитслужби, за кодом завдання “Контроль доставки товарів” і кодом ролі “Пункт пропуску”.

Посадовим особам регіональних митниць, митниць та їх структурних підрозділів права доступу до ПК “Контроль за переміщенням вантажів при транзиті” надаються згідно з Порядком регламентованого доступу користувачів до ЄАІС Держмитслужби України, затвердженим наказом Держмитслужби України з грифом “ДСК” у 2002 р.

Робота з ЄАІС на робочому місці посадової особи пункту пропуску

На виконання наказу ДМСУ від 8 грудня 1998 р. № 771 посадова особа митниці відправлення у межах своєї компетенції перевіряє правильність заповнення вантажної митної декларації та її електронної копії, за відсутності зауважень присвоює ВМД реєстраційний номер і пропускає вантаж через митний кордон України. Електронна копія ВМД за встановленими правилами передається до ДІТМС у термін, що не перевищує 4 годин з моменту оформлення транзитної ВМД. Після цього інформація про пропуск вантажу вноситься до ЄАІС.

Під час перевезення транзитних товарів, що переміщуються територією України на умовах Митної конвенції про міжнародне перевезення вантажів із застосуванням книжки міжнародного дорожнього перевезення (наказ Держмитслужби від 12 січня 2005 р. № 10), посадова особа митниці відправлення за допомогою програмно-інформаційного комплексу “Автоматизована система митного оформлення товарів та інших предме-

тів” оформлює ці товари одразу, формує в електронному вигляді файл з цією інформацією та передає її засобами електронного зв’язку до ЄАІС.

На робочому місці посадової особи пункту пропуску передбачається виконання таких функцій:

- оформлення транзитних ВМД;
- оформлення транзитних товарів, що переміщуються за операцією МДП у режимі “Транзит автомобільним транспортом на умовах Конвенції МДП” (в’їзд/виїзд);
- перегляд транзитних ВМД за їх номерами й діапазонами дат;
- перегляд інформації про транзит автомобільним транспортом на умовах Конвенції МДП.

Оформлення транзитної ВМД залежно від вибраного режиму має такі особливості:

- в’їзд на митну територію України — умовою оформлення пропуску вантажу в митниці відправлення є наявність транзитної ВМД у ЄАІС;
- виїзд з митної території України — виконання режиму можливе, якщо кількість товару кожного найменування дорівнює кількості товару, пропущеного під час ввезення, за винятком суми підтверджених втрат, якщо такі були, і кількості товарів, пропущених під час частинних вивезень (для переміщення товарів залізницею), якщо такі мали місце;
- прибуття вантажу в митницю призначення — режим застосовується за необхідності, можливе кількарразове його виконання;
- у режимі для залізничного виду транспорту кількість товару кожного найменування, що прибуває, не має перевищувати різниці між кількістю товару такого найменування, пропущеного під час ввезення, та сумою підтверджених втрат, якщо такі мали місце, і кількості товарів за всіма попередніми прибуттями, якщо такі мали місце;
- відмова у пропуску вантажу на виїзді — причину відмови треба зазначати в разі її наявності;
- частковий виїзд вантажу під час транзиту (залізниця) — режим застосовується за необхідності і тільки для ВМД, оформлених на товари, що переміщуються залізничним транспортом;

можливе кількаразове його виконання. Кількість товару кожного найменування, що підлягає частинному вивезенню, не має перевищувати залишку товару цього найменування, тобто різниці між кількістю товару, пропущеного під час ввезення, та сумою підтверджених втрат, якщо такі мали місце, і кількістю товарів, пропущених під час усіх частинних вивезень, якщо такі мали місце.

Примітка. Робоче місце посадової особи пункту пропуску використовується внутрішньою митницею для оформлення прибуття товарів, що переміщуються між митницями в межах митної території України (внутрішній транзит — тип ВМД “ТР 80 ВН”).

Для ВМД, які оформлені на товари, що підпадають під дію “Положення про порядок виконання Україною зобов’язань за Угодою з адаптації Договору про звичайні збройні сили в Європі стосовно надання інформації про транзит звичайних озброєнь і техніки через район застосування або в його межах”, затвердженого постановою Кабінету Міністрів України від 13 грудня 2001 р. № 1663, потрібно вибрати з довідника назву пункту пропуску, через який здійснено ввезення або вивезення.

Такі ВМД доступні для оформлення тільки фахівцям, на яких покладено обов’язки з митного оформлення вантажів, що підпадають під дію дозволу чи висновку Державної служби експортного контролю України.

Робота з ЄАІС на робочому місці посадової особи відділу контролю за переміщенням товарів

Робоче місце посадової особи відділу контролю доставки вантажів передбачає виконання функцій оформлення товарів, що переміщуються з використанням транзитних ВМД, або із застосуванням книжки МДП та перегляду інформації щодо цих переміщень.

Функція “Оформлення транзитних ВМД” включає такі режими:

- запит на зміну режиму;
- дозвіл на зміну режиму;
- порушення справи про контрабанду;
- огляд вантажу та зміна митного забезпечення;

- заява про втрату/вилучення вантажу, зміну транспортно-го засобу та зміну контрольної дати доставки;
- підтвердження втрати/вилучення вантажу, зміни транспортно-го засобу та контрольної дати доставки;
- відмова від підтвердження втрати вантажу, зміни транспортно-го засобу та зміни контрольної дати доставки;
- запит на зміну митниці виїзду;
- дозвіл на зміну митниці виїзду;
- завершення переміщення для ТР ВН — тільки для ВМД;
- зняття з контролю ВМД, за якими немає переміщення;
- прибуття вантажу для внутрішнього транзиту;
- анулювання електронної копії книжки МДП, накладної УІВС, ЦІМ.

Виконання таких режимів веде до зміни стану ВМД (книжки МДП) в ЄАІС.

Примітка. ВМД, оформлені на товари, що підпадають під дію “Положення про порядок виконання Україною зобов’язань за Угодою з адаптації Договору про звичайні збройні сили в Європі стосовно надання інформації про транзит звичайних озброєнь і техніки через район застосування або в його межах”, затвердженого Постановою Кабінету Міністрів України від 13 грудня 2001 р. № 1663, доступні для оформлення тільки фахівцям, на яких покладено обов’язки з митного оформлення вантажів, що підпадають під дію дозволу чи висновку Державної служби експортного контролю України.

Завершення переміщення товарів у режимі транзиту можливе за умови попереднього введення інформації про прибуття вантажу в митницю призначення.

10.5. Програмно-інформаційний комплекс “Митний контроль та митне оформлення транспортних засобів, що переміщуються громадянами через митний кордон України”

Призначення

Програмно-інформаційний комплекс “Митний контроль та митне оформлення транспортних засобів, що переміщуються громадянами через митний кордон України” розроблено для вдосконалення митного контролю та митного оформлення транспортних засобів, що переміщуються громадянами через митний кордон України, згідно з вимогами Правил митного контролю та митного оформлення транспортних засобів, що переміщуються громадянами через митний кордон України, затверджених наказом Держмитслужби від 17 листопада 2005 р. № 1118, та Порядку здійснення контролю за доставкою в митниці призначення транспортних засобів особистого користування, що переміщуються через митну територію України транзитом, затвердженого наказом Держмитслужби від 25 липня 2006 р. № 630.

ПІК призначено для посадових осіб регіональних митниць і митниць, до функціональних обов’язків яких належить здійснення митного контролю та митного оформлення транспортних засобів, що переміщуються громадянами через митний кордон України.

Умови застосування

ПІК “Митний контроль та митне оформлення транспортних засобів, що переміщуються громадянами через митний кордон України” базується на концепції розбудови трирівневої мережі з центральним сервером баз даних і серверами Єдиної автоматизованої інформаційної системи Держмитслужби, розміщеними в Департаменті інформаційних технологій і митної статистики.

Призначені для користувача процедури зберігаються на web-сервері й запускаються користувачем з робочих станцій (функ-

ціональних робочих місць) з використанням стандартних засобів операційних систем, наприклад, Internet Explorer Version 5.0 і вище в системі Windows 98/ME/NT/2000/XP.

ПІК “Митний контроль та митне оформлення транспортних засобів, що переміщуються громадянами через митний кордон України” в ЄАІС Держмитслужби розміщено в розділі “Митне оформлення”, підрозділі “Транспортні засоби”. Оперативний доступ до ЄАІС Держмитслужби здійснюється каналами зв’язку за адресами: <https://XXX.XX.XX.XXX/>.

Доступ до ПІК “Митний контроль та митне оформлення транспортних засобів, що переміщуються громадянами через митний кордон України” в ЄАІС Держмитслужби з правом ведення, перегляду інформації надається посадовим особам регіональних митниць і митниць, зареєстрованим як користувачі ПІК ЄАІС Держмитслужби, яким надано відповідні права доступу до цього ПІК.

Права регламентованого доступу до ПІК надаються посадовим особам регіональних митниць, митниць згідно з Порядком регламентованого доступу користувачів до ЄАІС Держмитслужби України, затвердженим наказом Держмитслужби у 2002 р. під грифом “ДСК”.

Опис роботи програми

Робота з ПІК “Митний контроль та митне оформлення транспортних засобів, що переміщуються громадянами через митний кордон України” залежно від прав, наданих користувачу, передбачає виконання таких режимів:

- доставка в митницю призначення;
- видача Посвідчення на реєстрацію транспортного засобу в органах ДАІ МВС України;
- вивезення за межі митної території України;
- інформація про продовження строку доставки;
- підтвердження отримання інформації про продовження строку доставки;
- інформація про втрату транспортного засобу;
- підтвердження отримання інформації про втрату транспортного засобу;
- інформація про справу про порушення митних правил;
- зворотне вивезення;

- транспортні засоби, для яких строк доставки у митницю призначення не вичерпано;
- транспортні засоби, для яких строк доставки у митницю призначення подовжено та не вичерпано;
- транспортні засоби, для яких наявна інформація про втрату;
- транспортні засоби, для яких наявна інформація про порушення митних правил;
- транспортні засоби, для яких строк доставки у митницю призначення порушено;
- перегляд інформації про ввезення/вивезення транспортних засобів.

За наявності помилок у введеній користувачем інформації на екран видаються відповідні повідомлення. У разі будь-якого повідомлення про помилку слід повернутись до екранної форми, що містить введену користувачем інформацію (за допомогою Internet Explorer), візуально перевірити правильність інформації та внести потрібні зміни.

10.6. Власні розробки митних органів

Автоматизація перевірки митного контролю та митного оформлення за критеріями

Вантажна митна декларація — складний за своєю структурою та інформаційним наповненням документ. Перевірка правильності оформлення декларації потребує високої кваліфікації посадової особи митного органу та значних затрат часу.

З метою більш поглибленого контролю та підвищення якості митного оформлення товарів і транспортних засобів за певними критеріями, а також можливістю оперативно втручатися у процес митного оформлення розроблений програмно-інформаційний комплекс “Критеріальні оцінки оформлення вантажної митної декларації”. З травня 2004 р. почалася дослідна експлуатація ПІК в підрозділах митниць, які здійснюють митне оформлення. Критерії готуються фахівцями митниць на основі нормативних документів, аналізу раніше виявлених по-

милок, довідкової та статистичної інформації з вантажної митної декларації за певний період часу тощо.

ПІК “Критеріальні оцінки оформлення ВМД” призначений для здійснення комплексної перевірки правильності оформлення електронної копії вантажної митної декларації та становить автоматизовану систему підтримки прийняття рішень щодо проведення процедур митного оформлення та їх правомірності. Аналізуючи електронну копію ВМД, програма формує набір рекомендацій для посадової особи щодо можливих порушень під час митного оформлення, за необхідності проведення певних процедур (догляду вантажу працівниками відділу контролю митної вартості та номенклатури, служби боротьби з контрабандою та митної варти, направлення товарів на лабораторне дослідження тощо).

У результаті перевірки ВМД формується перелік зауважень щодо змісту ВМД різного ступеня важкості (помилка, попередження, інформація). Користувач має можливість переглянути довідкову інформацію, пов’язану з перевіркою, ознайомитися з текстами нормативних документів, на основі яких була запроваджена перевірка, та безпосередньо переглянути електронну копію декларації.

Розроблений комплекс призначений для трьох категорій користувачів. По-перше, це працівники, що безпосередньо задіяні у митному оформленні вантажів із застосуванням ВМД. Ця категорія користувачів має змогу отримати вичерпну інформацію про можливі зауваження до заповнення граф ВМД, відповідність оформлення критеріям ризиків. Використання ПІК на етапах митного оформлення ВМД сприяє підвищенню якості митного оформлення, надає довідкову інформацію у зручному вигляді, дає можливість зменшити ймовірність механічних та логічних помилок у ВМД і дозволяє проводити аналітичну роботу щодо характеру помилок.

Друга група користувачів — це керівники підрозділів. Засобами ПІК керівник підрозділу має можливість контролювати якість здійснення митного оформлення своїми підлеглими.

До третьої групи користувачів належать посадові особи підрозділів служби боротьби з контрабандою та митної варти, які

мають змогу контролювати товари, що переміщуються через митні пости, вести аналітичну роботу на основі отриманої інформації з ВМД, оформлених іншими митницями.

Серед реалізованих у ПІК перевірок можна виокремити такі: контроль за застосуванням санкцій Міністерства економіки; контроль інтелектуальної власності; перевірка товарів, суб'єктів зовнішньоекономічної діяльності, транспортних засобів за ВМД на відповідність критеріям та індикаторам ризику; контроль попередніх документів; орієнтування; особливості митного оформлення у межах певного режиму; порядок нарахування платежів та застосування преференцій; контроль документів у гр. 44 тощо. Більшість перевірок базується на довідковій інформації, яка отримується з різноманітних джерел та накопичується у структурованому, зручному для перегляду вигляді.

Особливістю ПІК є оперативність впровадження нових перевірок. Будь-яка інформація після опрацювання завантажується до бази даних відповідно до певного нормативного документа. Реалізована можливість автоматизованого контролю за актуальністю довідкової інформації та алгоритмів перевірки. Після втрати чинності або внесення змін до нормативних документів відбувається актуалізація певних перевірок та довідкової інформації, що базується на цьому документі. Такий механізм значною мірою гарантує користувачеві достовірність та актуальність інформації, яка отримується від ПІК у процесі перевірки ВМД.

Підтримка ПІК організована таким чином, що підрозділи митниці, задіяні у митному оформленні, щомісячно у письмовій формі надають зауваження, пропозиції, технічні завдання для розробки перевірок та впровадження нових критеріїв. Таким чином кожний підрозділ митниці формує власний блок перевірок за профільним напрямом. Для зручності у ПІК реалізований механізм розмежування доступу до перевірок для різних підрозділів митниці. Кожний підрозділ під час перевірки ВМД має доступ тільки до зауважень за власним напрямом роботи.

На сьогодні у програмно-інформаційному комплексі "Критеріальні оцінки оформлення ВМД" реалізовано близько 200 форматно-логічних перевірок та 600 критеріїв.

Використання описаного програмного забезпечення набуває ще більшої актуальності у світлі впровадження нової технології митного оформлення за принципом “єдиного вікна”. Для зазначеної технології особливу увагу необхідно приділяти автоматизації, зменшенню часу та підвищенню якості митного оформлення, впровадженню потужних інформаційних систем підтримки прийняття рішень щодо митного оформлення.

Запитання і завдання для самоконтролю

1. Для чого призначено ПІК “Квитанція МД-1” та які функціональні процеси він автоматизує?
2. Яке програмне забезпечення необхідне для застосування ПІК “Квитанція МД-1”?
3. Збирання й обробку якої інформації забезпечує ПІК “Аналітична та статистична обробка інформації про порушення суб’єктами ЗЕД чинного законодавства”?
4. У роботі яких підрозділів застосовується ПІК “Аналітична та статистична обробка інформації про порушення суб’єктами ЗЕД чинного законодавства”?
5. На яких технологіях базується робота ПІК “Аналітична та статистична обробка інформації про порушення суб’єктами ЗЕД чинного законодавства”?
6. Яке призначення складів тимчасового зберігання?
7. Які функціональні можливості надає ПІК “Реєстр дозволів на право відкриття складів тимчасового зберігання”?
8. Назвіть причини створення ПІК “Контроль за переміщенням вантажів при транзиті”.
9. Виконання яких функцій передбачено на робочому місці посадової особи пункту пропуску із застосуванням ПІК “Контроль за переміщенням вантажів при транзиті”?
10. Яким чином регламентується доступ до ПІК “Контроль за переміщенням вантажів при транзиті”?
11. Які можливості роботи надаються ПІК “Контроль за переміщенням вантажів при транзиті” для посадових осіб відділів контролю доставки вантажів?

12. Для кого призначено та які завдання дає змогу виконувати ПІК “Митний контроль та митне оформлення транспортних засобів, що переміщуються громадянами через митний кордон України”?

13. Які режими роботи підтримує ПІК “Митний контроль та митне оформлення транспортних засобів, що переміщуються громадянами через митний кордон України”?

14. Які підрозділи митної служби використовують ПІК “Митний контроль та митне оформлення транспортних засобів, що переміщуються громадянами через митний кордон України” та як регламентується доступ до нього?

Розділ 11

СИСТЕМИ ПЕРЕДАЧІ ІНФОРМАЦІЇ У МИТНІЙ СЛУЖБІ УКРАЇНИ

11.1. Засоби електронної пошти та їх застосування в ЄАІС Держмитслужби України

Інформаційний обмін у межах митної системи здійснюється за допомогою інформаційно-телекомунікаційного комплексу Державної митної служби України “Електронна пошта” (далі — Система ІТК).

Побудову Системи ІТК на базі програмного забезпечення Lotus Domino/Notes розпочато у 2004 р. та остаточно закінчено у січні 2007 р. Вона є невід’ємною складовою Єдиної автоматизованої інформаційної системи та виконує функції транспортної системи електронного документообігу Державної митної служби України.

Організацію та принципи роботи Системи ІТК визначено в таких документах:

- “Порядок функціонування електронної пошти Державної митної служби України”, затверджений наказом Державної митної служби України “Про затвердження та введення в дію Порядку функціонування електронної пошти Державної митної служби України” від 6 жовтня 2000 р. № 550;

- “Порядок функціонування системи інформаційно-телекомунікаційного комплексу Державної митної служби України “Електронна пошта”, затверджений наказом Державної митної

служби України “Про затвердження Порядку функціонування системи інформаційно-телекомунікаційного комплексу Державної митної служби України “Електронна пошта” та внесення зміни до наказу Держмитслужби України від 6 жовтня 2000 р. № 550” від 29 вересня 2006 р. № 826;

— наказ Держмитслужби України “Про введення в дослідну експлуатацію відмовостійкої системи серверів (кластерів) Головного інформаційно-телекомунікаційного комплексу Держмитслужби України “Електронна пошта” від 1 жовтня 2007 р. № 812.

Структура системи інформаційно-телекомунікаційного комплексу “Електронна пошта”

Структура Системи ІТК ієрархічна та побудована за топологією “зірка” (рис. 11.1).

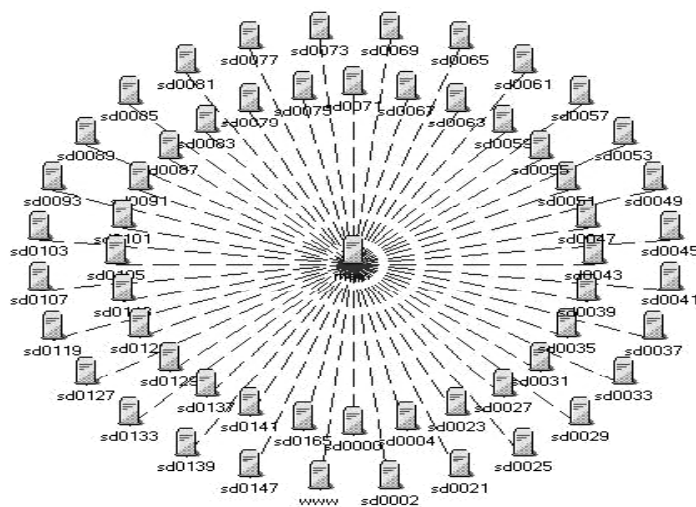


Рис. 11.1. “Зіркова” топологія Системи ІТК “Електронна пошта”

Система ІТК складається з Головного інформаційно-телекомунікаційного комплексу (далі — ГІТК), Регіональних інформаційно-телекомунікаційних комплексів (далі — РІТК) та робочих персональних електронно-обчислювальних машин користувачів.

Головний інформаційно-телекомунікаційний комплекс — це сукупність DNS-серверів, серверів Lotus Domino, пов'язаних між собою локальною обчислювальною мережею Регіональної інформаційної митниці (далі — РІМ). Цей комплекс функціонує в цілодобовому режимі та вимикається лише для проведення регламентних робіт.

До складу ГІТК входять:

- *головний сервер маршрутизації поштових повідомлень* — основний сервер як ГІТК, так і Системи ІТК у цілому, якому за ієрархією підпорядковані всі сервери РІТК. Функціонує в структурі локальної обчислювальної мережі РІМ;

- *сервер віддалених користувачів Системи ІТК* — сервер ГІТК, на якому зареєстровані віддалені користувачі митних органів, спеціалізованих митних установ та організацій, які не мають власного РІТК. Функціонує в структурі локальної обчислювальної мережі РІМ. Доступ до сервера віддалених користувачів здійснюється каналами ВТМ або комутованими каналами зв'язку;

- *сервер для технологічних поштових скриньок і користувачів сторонніх організацій* — сервер ГІТК, на якому зареєстровані технологічні поштові скриньки для пересилання інформації до ЦБД ЄАІС та відповідних ПІКів Держмитслужби України. Також на сервері зареєстровані поштові скриньки користувачів Системи ІТК сторонніх організацій, використовуючи які здійснюється обмін інформацією між Держмитслужбою України та відповідною організацією. Сервер функціонує в структурі локальної обчислювальної мережі РІМ;

- *сервер ЦА Держмитслужби України та РІМ* — сервер ГІТК, на якому зареєстровані користувачі ЦА Держмитслужби, РІМ і технологічні поштові скриньки. Сервер функціонує у структурі локальної обчислювальної мережі РІМ та ЦА Держмитслужби України.

З метою забезпечення безперебійного доступу користувачів та серверів системи ІТК до серверів ГІТК, максимальної працездатності серверів ГІТК, відмовостійкості серверів ГІТК та динамічного перерозподілу інформаційного навантаження відповідно до наказу Держмитслужби України “Про введення в дослідну експлуатацію відмовостійкої системи серверів (клас-

терів) Головного інформаційно-телекомунікаційного комплексу Держмитслужби України “Електронна пошта” від 1 жовтня 2007 р. № 812 побудована відмовостійка (кластерна) система серверів ГІТК. Схематично технічне рішення кластерної системи серверів ГІТК наведено на рис. 11.2.

Регіональний інформаційно-телекомунікаційний комплекс — це сукупність DNS-сервера та сервера Lotus Domino митного органу, спеціалізованої митної установи й організації, пов’язаних між собою локальною обчислювальною мережею відповідного митного органу, спеціалізованої митної установи й організації. Цей комплекс функціонує в цілодобовому режимі та вимикається лише для проведення регламентних робіт. Станом на листопад 2007 р. у Системі ІТК функціонує 65 РІТК.

Користувачами Системи ІТК можуть бути:

- *віддалений користувач* — користувач Системи ІТК, зареєстрований на сервері одного з РІТК або безпосередньо на сервері ГІТК, який здійснює доступ до таких серверів каналами зв’язку відомчої телекомунікаційної мережі або засобами віддаленого доступу;

- *локальний користувач* — користувач Системи ІТК, зареєстрований на сервері одного з РІТК або безпосередньо на сервері ГІТК, який здійснює доступ до таких серверів за допомогою локальної обчислювальної мережі митного органу;

- *користувач сторонньої організації* — користувач сторонньої організації, підключення якого здійснюється на підставі письмового дозволу керівництва Держмитслужби України.

Структура програмного забезпечення системи ІТК

Для віддаленого та локального користувача потрібні: програмне забезпечення Lotus Notes Client або будь-який SMTP/POP3 клієнт (The Bat, Outlook Express тощо), який забезпечує підготовку, відсилення та прийняття електронних повідомлень.

Для роботи серверів ГІТК/РІТК системи ІТК необхідні:

- програмне забезпечення Lotus Domino Server під операційну систему (далі — ОС) Linux або Windows 2000/2003 (у варіантах Server або Advanced Server);

- програмне забезпечення Lotus Domino Administrator, яке власне забезпечує адміністрування серверів ГІТК/РІТК системи ІТК.

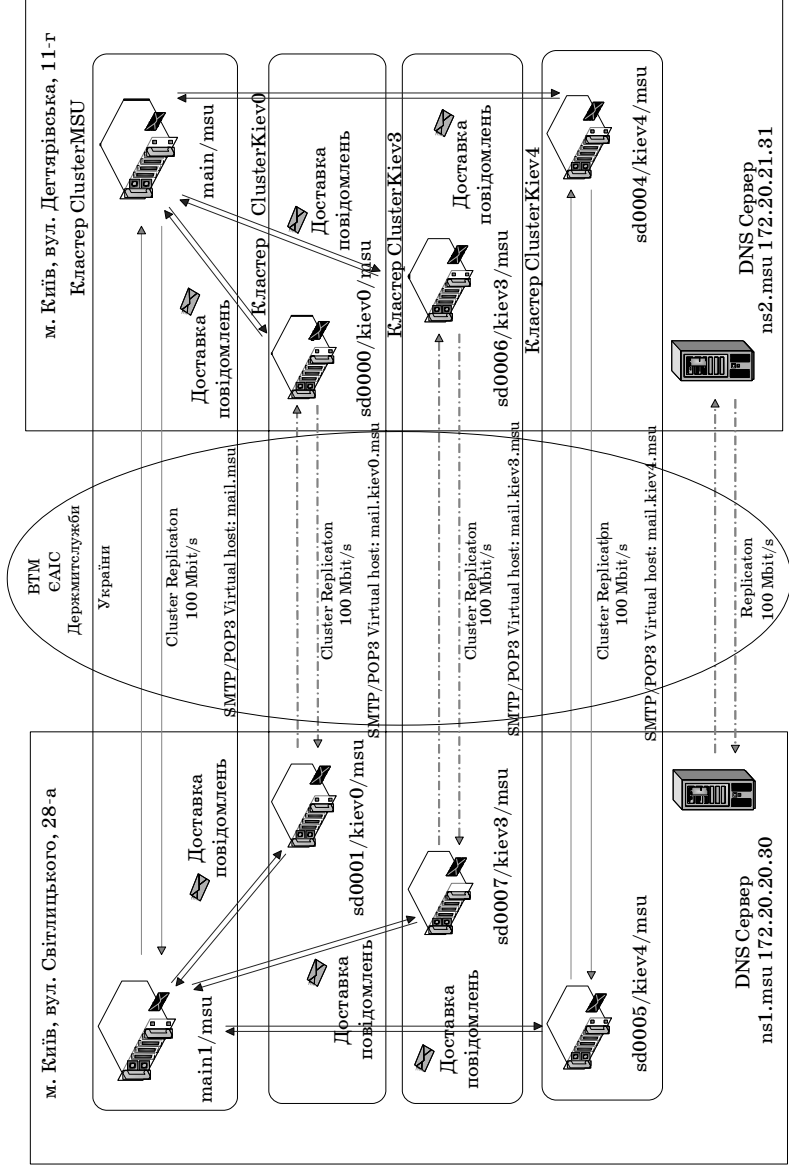


Рис. 11.2. Ескізно-технічне рішення введення в експлуатацію відмовостійкої системи серверів Головного інформаційно-телекомунікаційного комплексу ІТК Держмитслужби України “Електронна пошта” в рамках створення резервного комплексу САІС Держмитслужби

Рекомендовані операційні системи, які потрібно застосовувати під час розгортання РІТК та підключення локальних і віддалених користувачів:

- для серверів РІТК — родини Linux, Windows 2000/2003 (у варіантах Server або Advanced Server);
- для локальних і віддалених користувачів — Windows 2000, Windows NT, Windows XP, Windows 98.

11.2. Відомча телекомунікаційна мережа ЄАІС Держмитслужби України

Відомча телекомунікаційна мережа Єдиної автоматизованої інформаційної системи Держмитслужби України (далі — ВТМ ЄАІС) — телекомунікаційна мережа, що створена Державною митною службою України з метою задоволення потреб у високошвидкісному, надійному, безперебійному та захищеному інформаційному обміні даних та голосу в рамках ЄАІС Держмитслужби України для здійснення процедур митного оформлення та контролю під час переміщення товарів і транспортних засобів через митний кордон України.

До складу ВТМ ЄАІС входять:

- Транспортна мережа супутникового зв'язку Держмитслужби України (далі — ТМСЗ);
- Єдина інформаційно-телекомунікаційна система Державної прикордонної служби України та Державної митної служби України (далі — ЄІТС ДПСУ-ДМСУ);
- Наземні цифрові канали зв'язку Держмитслужби України (далі — НЦКЗ).

ВТМ ЄАІС складається з вузлів, що організаційно-технічно розподіляються на:

- підключені до ВТМ Наземними цифровими каналами зв'язку з використанням технології Frame Relay;
- підключені до ВТМ за допомогою Транспортної мережі супутникового зв'язку Держмитслужби;
- підключені до ВТМ за допомогою станцій супутникового зв'язку, які належать Державній прикордонній службі Украї-

ни та використовуються Державною митною службою, що створює Єдину інформаційно-телекомунікаційну систему Державної прикордонної служби України та Державної митної служби України;

— вузли, які для доступу до ресурсів ЄАІС використовують низькошвидкісний комутований зв'язок (модемне з'єднання) загальнодоступними мережами (телефонна мережа загального користування) або радіодоступ.

ВТМ ЄАІС структурно розподіляється на 3 рівні:

- 1) рівень ядра (CORE LAYER);
- 2) рівень розподілу (DISTRIBUTION LAYER);
- 3) рівень доступу (ACCESS LAYER).

До рівня ядра (CORE LAYER) належить активне мережеве та каналне обладнання, що територіально знаходиться в Департаменті інформаційних технологій та митної статистики (далі — ДІТМС): Cisco 7204 VXR Router, 2 x Cisco 6509 MLS, Cisco AS5350, Cisco 2611XM, Nortell Networks BCN, Axxessit 32xE1 IAD тощо.

В основі рівня розподілу (DISTRIBUTION LAYER) лежать супутникові та наземні цифрові канали зв'язку й активне мережеве та каналне обладнання, що територіально знаходиться в операторів послуги: Nortel Networks Passport, Cisco 2811, Cisco 2611XM, центральна керуюча станція супутникового зв'язку (HUB, Slim, IP-GateWay).

До рівня доступу (ACCESS LAYER) належить мережеве та каналне обладнання, що територіально знаходиться в митному органі: граничний маршрутизатор Cisco 2811 / Cisco 1841 / Cisco 805, DSL-модем “останньої милі” з інтерфейсним кабелем типу DTE V.35, мультиплексор, обладнання станцій супутникового зв'язку, аналогові модеми тощо.

Складові ВТМ ЄАІС Держмитслужби створювалися так:

ТМСЗ — згідно із “Системотехническим проектом по созданию транспортной сети спутниковой связи Государственного таможенного комитета Украины”, затвердженим головою Державного митного комітету України Л.В. Деркачем 23 липня 1996 р.;

— ЄІТС ДМСУ-ДПСУ — на виконання Указу Президента від 9 лютого 2004 № 175/2004, згідно з Протоколами № 1, 2, 3

спільних нарад Держмитслужби, Держприкордонслужби, ЗАТ “УкрСат”, затвердженими головою Держмитслужби, головою Держприкордонслужби, головою Правління ЗАТ “УкрСат” та Договору “Про створення та спільне використання ЄІТС ДМСУ-ДПСУ” від 9 вересня 2004 р. № 850-04;

— НЦКЗ — згідно із “Системотехнічним проектом розвитку ЄАІС III черги “Інгул-2”, затвердженим рішенням Комісії Держмитслужби від 15 квітня 1999 р. і погодженим Комітетом з інформатизації та Державним комітетом зв’язку.

ВТМ ЄАІС функціонує відповідно до вимог:

— Порядку супроводження ВТМ ЄАІС Держмитслужби, затвердженого наказом Держмитслужби від 11 березня 2006 р. № 181;

— Інструкції про спільне використання обладнання супутникового зв’язку в пунктах пропуску через Державний кордон України, затвердженої 15 лютого 2006 р. першим заступником Держприкордонслужби П.А. Шишоліним та заступником голови Держмитслужби П.В. Пашком;

— Порядку використання сервісу відділеного доступу до ЄАІС Держмитслужби, затвердженого наказом Держмитслужби від 25 грудня 2006 р. № 1147.

На жовтень 2007 р. у митній системі функціонує ВТМ ЄАІС Держмитслужби, яка об’єднує цифровими каналами 350 митних підрозділів, забезпечує інформаційний обмін з Федеральною митною службою Російської федерації, Національним банком України, Департаментом ДАІ МВС, Державним казначейством України та складається з:

— 95 вузлів Єдиної інформаційно-телекомунікаційної системи Державної прикордонної служби України та Державної митної служби України;

— 175 вузлів Транспортної мережі супутникового зв’язку;

— 83 вузлів, підключених Наземними цифровими каналами зв’язку.

Запитання і завдання для самоконтролю

1. Які документи визначають організацію та принципи роботи відомчої електронної пошти ДМСУ?
2. За яким принципом побудовано систему інформаційно-телекомунікаційного комплексу “Електронна пошта”?
3. Які користувачі можуть бути підключені до інформаційно-телекомунікаційного комплексу “Електронна пошта”?
4. З яких елементів складається головний інформаційно-телекомунікаційний комплекс та для чого вони призначені?
5. Назвіть правила організації поштових скриньок користувачів у системі електронної пошти ДМСУ.
6. За допомогою яких програмних засобів забезпечується робота інформаційно-телекомунікаційного комплексу “Електронна пошта” ДМСУ?
7. Які вимоги висуваються до користувачів інформаційно-телекомунікаційного комплексу “Електронна пошта”?
8. Які функціональні процеси забезпечує транспортна мережа супутникового зв’язку ДМСУ?
9. На застосуванні яких апаратних засобів і технологій базується робота транспортної мережі супутникового зв’язку ДМСУ?
10. Яким чином відбувається доступ до каналів супутникового зв’язку?

Розділ 12

ЗАХИСТ МИТНОЇ ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ

12.1. Електронна митна інформація. Відповідальність за підготовку, використання та поширення електронної митної інформації

Згідно із Законом України “Про інформацію”, *інформація* — це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі й навколишньому природному середовищі.

Основні принципи інформаційних відносин:

- гарантованість права на інформацію;
- відкритість, доступність інформації та свобода її обміну;
- об’єктивність, вірогідність інформації;
- повнота і точність інформації;
- законність одержання, використання, поширення та зберігання інформації.

Інформацію можна класифікувати за різними критеріями: статистична, адміністративна, масова, інформація про діяльність державних органів, правова та ін.

Від рівня інформованості залежить успішність будь-якої діяльності. Діяльність ДМС України неможлива без сучасної якісної системи інформаційного супроводження. Відповідно до завдань, які виконують митні органи, постає питання оперативної передачі електронної інформації до ДМС України. Обмін електронною інформацією можна здійснювати за допомо-

гою комп'ютерної мережі та відповідного програмного забезпечення. Для виконання вимог Законів України “Про інформацію”, “Про державну таємницю”, “Про захист інформації в автоматизованих системах” і для реалізації заходів щодо вдосконалення системи збирання й обробки зовнішньо-торгівельної та митної статистики згідно з наказом ДМСУ від 8 лютого 1996 р. № 48 затверджено “Положення про електронну інформацію в митній системі України”.

Митна електронна інформація — це така сукупність даних і програм, яка підлягає або може підлягати обробці, передачі та збереженню засобами електронної обчислювальної техніки незалежно від її фізичного та логічного подання на кожному рівні структурного підрозділу митної системи України та яка містить відомості про роботу митних органів або стосується зовнішньоекономічної діяльності.

Джерелом митної інформації є власна інформація Державної митної служби України, яка виробляється в результаті безпосередньої діяльності митниці і митних органів:

- зміст митних документів (декларації, відомості тощо);
- внутрішня документація митних органів (накази, нормативні документи, правила тощо).

Додатковими джерелами інформації може бути інформація, що надходить від інших міністерств, відомств, учасників зовнішньоекономічної діяльності тощо.

Обробка інформації (використання, поширення, зберігання) здійснюється за допомогою технічних і програмних засобів. Митна електронна інформація може переміщуватись, передаватись діючими засобами телекомунікацій на різні рівні митної системи.

Будь-яка митна електронна інформація, що обробляється засобами електронної обчислювальної техніки митної установи, є інформацією з обмеженим доступом, яка за ступенем конфіденційності поділяється на три категорії.

А. Інформація та інформаційно-програмне забезпечення, яке не містить даних, що безпосередньо визначають або зумовлюють характер митної діяльності (технічні дані обладнання, документи стосовно роботи з персоналом, загальносистемне

програмне забезпечення для передачі, обробки та збереження митної інформації, прикладне програмне забезпечення тощо).

Б. Технологічна інформація діяльності митних органів (зміст митних декларацій, провізних відомостей, протоколів порушень митних правил та контрабанди, гарантійних листів та ін.) і нормативно-довідкова інформація (кадри, бухгалтерія тощо).

В. Нормативно-правова інформація суто службового призначення, інформація про зовнішньоекономічну діяльність, групові статистичні бази даних.

Відповідно до Закону України “Про захист інформації в автоматизованих системах” право власності на інформацію, створену в процесі обробки в ЄАІС, належить власникові автоматизованої системи, який здійснив цю обробку, тобто Державній митній службі України.

Митна інформація зберігається на магнітних накопичувачах персональних обчислювальних машин, як внутрішніх (магнітні диски типу вінчестер), так і зовнішніх (оптичні та гнучкі магнітні диски, магнітні стрічки), або у вигляді друкованих документів, які є твердою копією електронної митної інформації.

Під час формування митної інформації використовуються такі чинники: єдині класифікатори на основі міжнародних зразків, період, напрям товаропотоку, країна походження, країна призначення, статистична вартість, кількість, характер угоди, вид митного режиму, одиниці виміру та ін. Після збирання відомостей здійснюється узагальнення й аналіз. На підставі такого аналізу створюються інформаційно-аналітичні довідки з діаграмами й таблицями за певний період, що містять основні показники роботи митних органів. Один з показників роботи митних органів — кількість оформлених вантажних митних декларацій.

Згідно із Законом України “Про науково-технічну інформацію” інформаційні ресурси науково-технічної інформації — це систематизоване зібрання науково-технічної літератури і документації (книги, брошури, періодичні видання, патентна і нормативно-технічна документація, промислові каталоги, конструкторська документація, звітна науково-технічна до-

кументація з науково-дослідних і дослідно-конструкторських робіт, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксовані на паперових чи інших носіях.

Інформаційні ресурси спільного користування — це сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання.

Як і будь-яким ресурсом, інформаційними ресурсами можна управляти. Саме тому прийнято Закон України “Про Національну програму інформатизації” від 4 лютого 1998 р. Головною метою Національної програми інформатизації є створення необхідних умов для забезпечення громадян і суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави.

12.2. Засоби захисту інформації в ЄАІС ДМСУ

Порядок організації захисту інформації під час здійснення митного контролю та митного оформлення товарів і транспортних засобів із застосуванням вантажної митної декларації розроблено відповідно до вимог законів України “Про інформацію”, “Про державну таємницю”, “Про захист інформації в автоматизованих системах”, Порядку організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 2 жовтня 2003 р. № 1561-12, Інструкції про порядок обліку, зберігання й використання документів, справ, видань та інших матеріальних носіїв, які містять конфіденційну інформацію, що є власністю держави, затвердженої постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893, Зводу відомостей, що становлять державну таємницю, затвердже-

ного наказом Служби безпеки України від 1 березня 2001 р. № 52 і зареєстрованого в Міністерстві юстиції України 22 березня 2001 р. № 264/5455 (далі — ЗВДТ), та Розгорнутого переліку відомостей, що становлять державну таємницю в системі митних органів України, затвердженого наказом Держмитслужби України від 17 січня 2002 р. № 22, погодженого Службою безпеки України 15 грудня 2001 р. і зареєстрованого 27 грудня 2001 р. № 32, для захисту секретної та конфіденційної інформації, що є власністю держави, під час митного контролю й митного оформлення товарів і транспортних засобів із застосуванням вантажної митної декларації, яка має гриф обмеження доступу, а також конкретизації дій посадових осіб митних органів, спеціалізованих митних установ та організацій у процесі роботи з документами, що мають гриф обмеження доступу.

Порядок застосовується під час митного контролю й митного оформлення товарів і транспортних засобів, щодо яких оформлюється і подається митним органам вантажна митна декларація з грифом обмеження доступу: “Для службового користування”, “Таємно” або “Цілком таємно”, як у паперовому, так і в електронному вигляді, за всіх митних режимів.

Гриф обмеження доступу паперовому й електронному носіям інформації, а саме вантажній митній декларації, за якою здійснюються митний контроль та митне оформлення товарів і транспортних засобів, відповідно до вимог законодавчих актів з питань охорони інформації з обмеженим доступом надає власник інформації.

У цьому Порядку терміни вживаються в такому значенні:

— *автоматизована система (АС)* — організаційно-технічна система, що реалізує інформаційну технологію й об’єднує засоби обчислювальної техніки та зв’язку, методи і процедури, програмне забезпечення, фізичне середовище, персонал та інформацію, яка обробляється;

— *власник інформації* — фізична або юридична особа, якій належить право власності на інформацію і яка використовує її та розпоряджається нею, визначає правила обробки інформації та доступу до неї, а також встановлює щодо неї інші умови;

— *гриф обмеження доступу* — реквізит матеріального носія інформації, що засвідчує ступінь обмеження доступу до цієї інформації (для службового користування, таємно, цілком таємно).

Інші терміни, що використовуються в цьому Порядку, мають таке саме значення, як і в Митному кодексі України та інших нормативно-правових актах.

Вимоги до забезпечення захисту інформації з обмеженим доступом, що є власністю держави

Перелік посадових осіб митного органу, спеціалізованої митної установи та організації, що залучаються до проведення митного контролю та митного оформлення товарів і транспортних засобів із застосуванням вантажної митної декларації та її електронних копій, які мають гриф “Для службового користування”, “Таємно” або “Цілком таємно”, у тому числі ті, що здійснюють провадження у справах про порушення митних правил, затверджується наказом митного органу, спеціалізованої митної установи й організації.

Митний контроль та митне оформлення товарів і транспортних засобів із застосуванням вантажної митної декларації та її електронних копій, які мають гриф “Для службового користування”, “Таємно” або “Цілком таємно”, здійснюються посадовими особами митного органу, спеціалізованої митної установи й організації, визначеними відповідно до п. 2.1 Порядку організації захисту інформації під час здійснення митного контролю та митного оформлення товарів і транспортних засобів із застосуванням вантажної митної декларації, у зонах митного контролю, на територіях і в приміщеннях підприємств, установ та організацій, що декларують відповідні товари, зберігають їх під митним контролем і повинні мати оформлений у встановленому порядку допуск до державної таємниці та доступ до державної таємниці відповідної форми або до конфіденційної інформації, що є власністю держави, наданий відповідно до вимог нормативно-правових актів з питань охорони інформації з обмеженим доступом, а також необхідні документи для забезпечення роботи з інформацією відповідної категорії.

Порядок митного контролю та митного оформлення товарів і транспортних засобів із застосуванням вантажної митної декларації, яка має гриф обмеження доступу

Митний контроль та митне оформлення товарів і транспортних засобів із застосуванням вантажної митної декларації, яка має гриф обмеження доступу, здійснюються відповідно до вимог Порядку здійснення митного контролю та митного оформлення товарів і транспортних засобів із застосуванням вантажної митної декларації, затвердженого наказом Держмитслужби України від 14 жовтня 2002 р. № 561 і зареєстрованого в Міністерстві юстиції України 7 листопада 2002 р. № 877/7165 (зі змін. і доп.).

Облік і зберігання аркушів вантажної митної декларації, що має гриф обмеження доступу, носіїв електронних копій, анульованих вантажних митних декларацій та їх електронних копій, а також документів з грифом обмеження доступу, що подаються митному органу, спеціалізованій митній установі й організації для митного контролю та митного оформлення товарів і транспортних засобів із застосуванням вантажної митної декларації, яка має гриф обмеження доступу, здійснюються відповідно до вимог нормативно-правових актів з питань діловодства, документів та інформації, яку вони містять.

Видача аркушів вантажної митної декларації, що має гриф обмеження доступу, а також магнітного носія з первинною електронною копією таких вантажних митних декларацій, поводження з ними й документами, що їх супроводжують (крім реєстру документів, аркуша контролю та інших документів, що зберігаються у митному органі), здійснюються в порядку, передбаченому наказом Держмитслужби України від 14 жовтня 2002 р. № 561, з дотриманням вимог нормативно-правових актів у галузі захисту інформації.

Формування бази даних електронних копій вантажних митних декларацій, які мають гриф обмеження доступу

Для формування бази даних електронних копій вантажних митних декларацій з грифом обмеження доступу митними органами, спеціалізованими митними установами та організаціями створюються автоматизовані системи, які мають відпові-

дати вимогам нормативно-правових актів у галузі захисту інформації.

Пересилання носіїв електронних копій вантажних митних декларацій з грифом обмеження доступу здійснюється з дотриманням вимог порядку організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 2 жовтня 2003 р. № 1561-III, а також Інструкції про порядок обліку, зберігання й використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, затвердженої постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893.

Вимоги до організації робочих місць і автоматизованих систем

Митне оформлення товарів і транспортних засобів за вантажними митними деклараціями з грифом обмеження доступу має здійснюватися з дотриманням вимог режиму секретності та конфіденційності у приміщеннях, що відповідають вимогам нормативно-правових актів у галузі захисту інформації.

Робочі місця для роботи з вантажними митними деклараціями, що мають гриф обмеження доступу, а також з магнітними носіями їх електронних копій митні органи створюють самостійно, шляхом укладання договорів з підприємствами, установами або організаціями, які мають відповідні ліцензії, видані Департаментом спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України.

Автоматизовані системи, призначені (виділені) для оброблення електронних копій вантажних митних декларацій, які мають гриф обмеження доступу, повинні бути атестовані в установленому нормативно-правовими актами в галузі технічного захисту інформації (ТЗІ) порядку і мати атестати відповідності для роботи з інформацією з обмеженим доступом відповідної категорії.

Контроль та забезпечення стану захисту інформації з обмеженим доступом під час митного оформлення товарів

і транспортних засобів із застосуванням вантажної митної декларації, яка має гриф обмеження доступу

Забезпечення умов для роботи з інформацією з обмеженим доступом в автоматизованих системах, призначених для оброблення такої інформації, у митних органах, спеціалізованих митних установах та організаціях здійснюється особами, відповідальними за захист інформації з обмеженим доступом.

Контроль за станом захисту інформації з обмеженим доступом, яка обробляється в автоматизованих системах, призначених для оброблення електронних копій вантажних митних декларацій, що містять інформацію з обмеженим доступом, покладається на керівників митних органів, спеціалізованих митних установ та організацій.

Контроль за порядком поводження з документами, які мають гриф обмеження доступу, з електронними носіями, що містять інформацію з обмеженим доступом, а також за порядком доступу до таких документів та інформації здійснюється у порядку, встановленому нормативно-правовими актами з питань забезпечення охорони державної таємниці та конфіденційної інформації, що є власністю держави, уповноваженими комісіями або особами митних органів, спеціалізованих митних установ і організацій відповідно до покладених на них функцій та повноважень.

За порушення законодавства щодо захисту інформації з обмеженим доступом під час митного оформлення товарів і транспортних засобів із застосуванням вантажної митної декларації, яка має гриф обмеження доступу, посадові особи митних органів, спеціалізованих митних установ та організацій несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно із законодавством.

Запитання і завдання для самоконтролю

1. Назвіть основні принципи інформаційних відносин.
2. За якими критеріями класифікується інформація?
3. Що таке електронна митна інформація?
4. На які категорії поділяється інформація з обмеженим доступом?
5. Які чинники використовуються під час формування митної інформації?
6. Що таке інформаційні ресурси спільного користування?
7. Які засоби захисту інформації в ЄАІС ДМСУ?
8. Перелічіть вимоги до забезпечення захисту інформації з обмеженим доступом.
9. Опишіть порядок митного контролю та митного оформлення ВМД, яка має гриф обмеження доступу.
10. Назвіть вимоги до організації робочих місць і автоматизованих систем.

Розділ 13

КОМЕРЦІЙНІ ПРОГРАМНІ ПРОДУКТИ МИТНОГО ОФОРМЛЕННЯ

13.1. Програмні комплекси для декларування товарів суб'єктами зовнішньоекономічної діяльності

Розвиток Єдиної автоматизованої інформаційної системи митних органів України не можливий без оперативного обміну зовнішньоекономічними документами із суб'єктами зовнішньоекономічної діяльності — учасниками ЗЕД. Обмін документами потрібний для швидкого й оперативного митного оформлення, своєчасного збирання та обробки статистичної й оперативної інформації, контролю експортно-імпортних операцій учасників ЗЕД.

Одним з основних завдань програми “Інспектор-2006”, яка нині функціонує в митних органах України, є ефективна обробка інформації, що готується комерційними програмними продуктами типу “Митний брокер”, а в майбутньому — власниками митних ліцензійних складів, транспортними та іншими організаціями.

Формати електронних повідомлень, які застосовуються сьогодні для обміну інформацією між учасником ЗЕД і митницею, підтримують лише вантажні митні декларації та дані щодо розрахунку митної вартості. У майбутньому планується розробка форматів електронних повідомлень, які будуть підтримувати більшу кількість необхідних митниці документів для

проведення митного оформлення, наприклад формалізовані дані з експортного контролю, зареєстрованих контрактів, ліцензій, дозволів тощо.

Коротко зупинимося на технології обміну електронною інформацією між учасником ЗЕД та митницею. *Технологія обміну* передбачає наявність двох суб'єктів обміну — учасника ЗЕД і митниці та об'єкта обміну — електронного повідомлення, яке містить вантажні митні декларації, дані щодо розрахунку митної вартості.

Обмін електронними повідомленнями здійснюється шляхом формування учасником ЗЕД електронного пакета документів (електронної копії вантажно-митної декларації), передачі його в митну установу, використовуючи дискетний або поштовий тракт передачі (електронна пошта) та обробки митною установою електронного пакета документів.

На сьогодні найбільш прийнятним є *дискетний тракт передачі електронної митної інформації*, оскільки він вимагає мінімальних затрат як зі сторони учасників ЗЕД, так і митних установ. Згодом можливий перехід на обмін електронними повідомленнями з використанням електронної пошти. Для цього опрацьовується технологія електронної взаємодії учасників ЗЕД і митниці та запроваджуються алгоритми обробки електронних документів, що надходять засобами електронної пошти, а також технологія, яка передбачає запис учасником ЗЕД електронного пакета документів безпосередньо в центральну базу даних Держмитслужби.

Отже, особа, яка готує документи для оформлення в митному відношенні товарів та інших предметів, повинна володіти елементарними знаннями та навичками роботи на комп'ютері, а саме: вміти перевірити цілісність даних на магнітному носії, перевіряти комп'ютер та магнітні носії на наявність комп'ютерних вірусів, форматовувати дискети, копіювати та знищувати файли.

Програмні продукти типу “Митний брокер” призначені для складання вантажної митної декларації, наступної її перевірки, друкування вантажної митної декларації на бланках встановленої форми та підготовки електронного пакета документів

для митниці та подальшого його виведення на магнітний носій (дискету) у встановленому Держмитслужбою форматі.

Митна інформація, представлена в електронному вигляді, в подальшому використовується митним органом для формування реєстрів до уповноважених банків, інформування податкових інспекцій із зовнішньоекономічних операцій, які проводилися з оформленням вантажної митної декларації. Тому, особі, яка здійснює декларування і готує електронний пакет митних документів, необхідно орієнтуватися в основних питаннях електронного пакета документів зважаючи на митну статистику.

Оскільки електронна митна інформація проходить декілька етапів форматно-логічного контролю (тобто перевірки даних, представлених в цифровому вигляді, які повинні однозначно ідентифікувати суб'єкта ЗЕД, митний режим, спосіб розрахунку, уповноважений банк та ін.), особа, яка здійснює декларування, повинна мати уявлення про код ЄДРПОУ, код платника податку та класифікатори (довідники), які використовуються під час складання вантажної митної декларації.

Основним цифровим параметром, який однозначно ідентифікує учасника ЗЕД, декларанта, особу, відповідальну за фінансове врегулювання зовнішньоекономічної операції, а також уповноважений банк, через який проводиться рух коштів, є *код ЄДРПОУ (ідентифікаційний код з Єдиного державного реєстру підприємств та організацій України, створеного на виконання Постанови Кабінету Міністрів України від 22 січня 1996 р. за № 118)*. Код ЄДРПОУ становить 8-значне ціле число. Перші сім цифр — значущі, остання восьма цифра є контрольною сумою на перші сім цифр коду ЄДРПОУ. Отже, якщо допущена помилка в перших семи цифрах, то контрольна сума не буде збігатися з восьмою, останньою цифрою коду ЄДРПОУ. Якщо помилка у восьмій — також контрольна сума за першими сімома цифрами вкаже на помилку в коді ЄДРПОУ. Алгоритм підрахунку контрольної суми різний для кодів менших ніж 30000000, ніж для кодів, які більше або дорівнюють 30000000.

Код ЄДРПОУ використовується для формування так званого реєстраційного номера (ВМД, гр. 2, 8, 9), а також безпосе-

редньо при заповненні гр. 28, 50. Також, на виконання вимог “Інструкції про порядок заповнення вантажної митної декларації”, затвердженої наказом ДМСУ від 9 липня 1997 р. № 307, у декларацію вноситься обліковий номер платника податків.

Приватні підприємці, тобто фізичні особи без права юридичної особи, не підлягають реєстрації в органах статистики і тому не мають коду ЄДРПОУ.

Для однозначної ідентифікації приватних підприємців використовується податковий номер, який присвоюється приватним підприємцям податковими інспекціями.

Розглянемо можливості програмно-інформаційних комплексів декларування суб'єктами зовнішньоекономічної діяльності на прикладі програмного забезпечення MD Office, QD Pro, Diamond Brige.

13.2. Програмне забезпечення MD Office

Розробник програмного комплексу **MD Office** НВО “Поверхность” пішов нестандартним шляхом, пропонуючи клієнтові можливість вибору окремих компонентів. Модульна організація програмного забезпечення (ПЗ) дає змогу підбирати функціональність офісного пакета відповідно до завдань, що стоять перед користувачем. Вибираючи ту або іншу конфігурацію (набір програм) MD Office, користувач одержує можливість розв'язувати різні комплекси завдань. Маючи повну версію, можна одержати повнофункціональний офісний продукт для діяльності митного брокера. Цей програмний комплекс орієнтований для роботи в середовищі операційної системи Windows. До його складу належить таке.

1. **MD Info** — нормативно-довідкова база MD Office, що містить:

- нормативні документи як митних органів, так і різних міністерств і відомств;
- митні та загальні довідники, що використовуються під час митного оформлення вантажів;

- товарну номенклатуру ЗЕД з поясненнями і примітками та УКТЗЕД;
- тематичні добірки документів;
- потужну пошукову систему;
- міжнародні правила тлумачення комерційних термінів (Інкотермс) тощо.

2. MD Declaration — програма, призначена для заповнення, друку, перевірки й формування електронної копії ВМД. Має великий набір готових мережних рішень, що дає змогу використовувати мережеві ресурси, централізовано зберігати інформацію й підтримувати її цілісність при збоях електроживлення. Включає можливість створення сильної та гнучкої системи безпеки і розмежування прав доступу до бази ВМД, що знижує ризик несанкціонованого доступу. Основні функції програми:

- повна візуалізація бланка ВМД;
- заповнення, друк і формування електронної копії декларації;
- навчальна система з розрахунку фактурної й митної вартості;
- інтелектуальна система пошуку в довідниках;
- перевірка з локалізацією місця помилки;
- система аналізу, контролю та звітів з питань ЗЕД.

Комбінація MD-Declaration і MD-Info дасть можливість створити найпростіший варіант офісного додатка для співробітника, що працює у зовнішньоекономічній сфері.

3. MD Form — програма автоматизованого заповнення документів. По суті, це стандартні шаблони допоміжних документів, заповнення яких необхідне під час зовнішньоекономічних операцій. З їхньою допомогою користувач може швидко скласти будь-який тип зовнішньоекономічного договору, що відповідатиме вимогам чинного законодавства України, а також правильно заповнити понад десяток митних, товаросупровідних і комерційних документів. Застосовуючи цю програму, можна скласти базу даних укладених угод і заповнених документів. Програма формує такі документи:

- декларацію автотранспортних засобів для громадян (МД-7);

- залізничну накладну;
- провізну відомість;
- рахунки-фактури;
- сертифікати про походження товарів та ін.

4. MD Warehouse — програма, призначена для автоматизації обліку товарів на митному ліцензійному складі відповідно до вимог Митного кодексу України. Вона генерує різні форми звітності про діяльність складу. Передбачене введення інформації з електронної копії ВМД. На вимогу видається статистика й аналіз роботи складу. Програма дає можливість підготувати необхідну документацію для роботи з клієнтом (накладні, рахунки-фактури, податкові накладні, договори тощо) з можливістю формування довільних форм документів.

5. MD WareHL — програма автоматизації обліку на торговому складі, що дозволяє вести облік товарів на малій і середній торговельній фірмі. Надає різні форми звітності про діяльність складу, дає можливість підготувати необхідну документацію під час роботи з клієнтом (накладні, рахунки-фактури, податкові накладні, договори тощо), а також вести контроль залишку товарів.

До складу офісного пакета входить також утиліта для налаштування усієї системи і допоміжних програм різного призначення.

MD Declaration

Роботу з MD Declaration організовано за допомогою вікон, які мають одну типову структуру, що полегшує роботу з програмою.

Після запуску програми з'являється вікно, структуру якого зображено на рис. 13.1.

1. Заголовок з номером версії MD Declaration. Праворуч є 3 кнопки управління вікном: згорнути задачу, розгорнути (кнопка відновлення), закрити вікно.

2. Рядок меню програми.

3. Панелі інструментів.

4. Робоча ділянка програми — бланк ВМД. Повністю переглянути ВМД можна за допомогою смуг прокрутки — горизонтальної та вертикальної.

5. Рядок стану, що відображає курси валют на дату створення ВМД та ярлики продуктів MD Office.

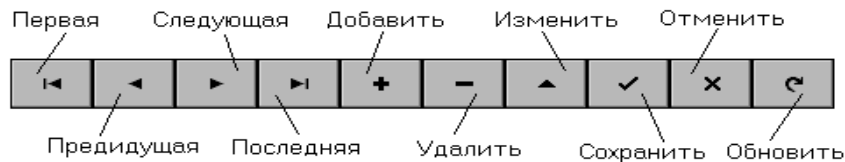


Рис. 13.2. Навігатор

точної. До програми підключено системні довідники, також можна застосовувати довідники користувачів.

Червоними галочками помічено графи, які заповнюються для вибраного типу ВМД.

Заповнення граф, пов'язаних з розрахунками, винесено на допоміжні вікна:

1. “Расчет общей таможенной стоимости” (рис. 13.3).
2. “Расчет таможенной стоимости товара” (рис. 13.4).
3. “Начисление платежей” (рис. 13.5) та ін.

Перевірка декларації

Для перевірки декларації використовують кнопку на панелі інструментів основного вікна програми  — *Перевірка декларації* або [Ctrl+G].

Результатом виконання цієї команди буде список помилок у декларації, виведений у нижню частину основного вікна (рис. 13.6).

Якщо клацнути двічі лівою кнопкою миші по будь-якому рядку зі списку помилок, то програма встановить (перенесе) покажчик курсора в ту графу на бланку ВМД, до якої належить така помилка, для її виправлення.

Під час перевірки відбувається сортування помилок. Можна встановити до показу будь-який вид помилок і виправити їх по одній.

Робота з довідниками

Для полегшення заповнення ВМД програма передбачає роботу з діалоговим вікном “Довідники”. Таке вікно включає довідкову інформацію різного характеру і призначене для вибору необхідного значення для граф ВМД під час її заповнення.

Расчет общей таможенной стоимости

Режим работы: Режим настройки

20. Условия поставки: 08 CIP Київ 30

22. Валюта контракта: 840 24. Валюта расчета: 978 Общий вес груза брутто (кг): 21194.45

Укажите точку перехода груза в собственность:

☒ Территория не резидента ☐ Территория резидента

Не резидент Граница или украинский порт Резидент

Счет - фактура

Наименование вида затрат	Сумма в вал.	Код	Курс	Сумма в грн
Вартість товарів згідно фактури	46547	840	5.3326	248216.5322
Вес Пакування	0	980	1	0
Вес Навантаження	0	980	1	0
Вес Доставка до основного перевізника	0	980	1	0
Вес Перевезення оплачене до вказ. міс	0	980	1	0

22. Общая фактурная стоимость: 248216.53 грн.

Расходы, вычитаемые при определении таможенной стоимости

Наименование вида затрат	Сумма в вал.	Код	Курс	Сумма в грн
Вес Транспортирования від кордону	500	840	5.3326	2666.3
С-ть Страхування від кордону	0	980	1	0

Сумма затрат: 2666.3 грн.

12. Общая таможенная стоимость: 245550.23 грн.

Рис. 13.3. Розрахунок загальної митної вартості

MD-Declaration має два види довідників:

— системні — це ті, які затверджено законодавчими та нормативними актами. До системних довідників належать УКТЗЕД і стандартні довідники, як-от: довідники валют, країн, митниць, умови поставок, характер угоди, процедур і преференцій, документів, способів і видів платежів, видів транспорту та ін. Усі вони працюють за одним принципом;

— користувацькі — ті, що створює користувач у процесі роботи. До них належать довідники учасників ЗЕД, товарної номенклатури користувача, стандартних зобов'язань тощо.

Расчет таможенной стоимости для товара № 1

Цена определяемая отделом тарифов и стоимости. Описание места: Место

35. Вес брутто (кг.) 11.852

38. Вес нетто (кг.) 11.852

Цена по фактуре 25871 840 5.3295 137879.4945

Дополнительная информация о ценах на товар

42. Фактурная стоимость: 137879.49 грн.

45. Таможенная стоимость: 283624.12 грн.

Распределение расходов

	По стоимости			По весу		
	в валюте	в гривнях	в %	в валюте	в гривнях	в %
Для графы 42	0	0.00	0	0	0	0.06
Для графы 45	0	0		0.28	1.49	

Баланс факт. стоим в валюте	0.00 USD	Баланс веса (брутто)	0.00 кг.
Баланс факт. стоим	0.00 грн.	Баланс там. стоим	0.00 грн.

Рис. 13.4. Розрахунок митної вартості товару

Начисление платежей (товар № 1)

Курс доллара США: 5.3329 Курс Евро: 5.763798

Сборы О товаре Пени Ставки Вексель

☐ На территории таможни (не взимается)

☒ Рабочее время 20 \$ 2 час.

☐ Нерабочее время 40 \$

☐ Праздничные дни 50 \$

☐ Отказ от услуг 20 \$

Применить

Платежи по товару:

Вид	Осн. нарахування	Ставка	Сума	СП	Вал
003	2 год	20 \$	213.32	01	980
001	14150.82 x0.05	126 дн.	891.5	01	980
010	14150.82 грн.	0.2 %	28.3	01	980
020	7615.93 грн.	2 %	152.32	08	980
028	7768.25 грн.	20 %	1553.65	01	980

Используется вексель.

Рис. 13.5. Нарахування платежів

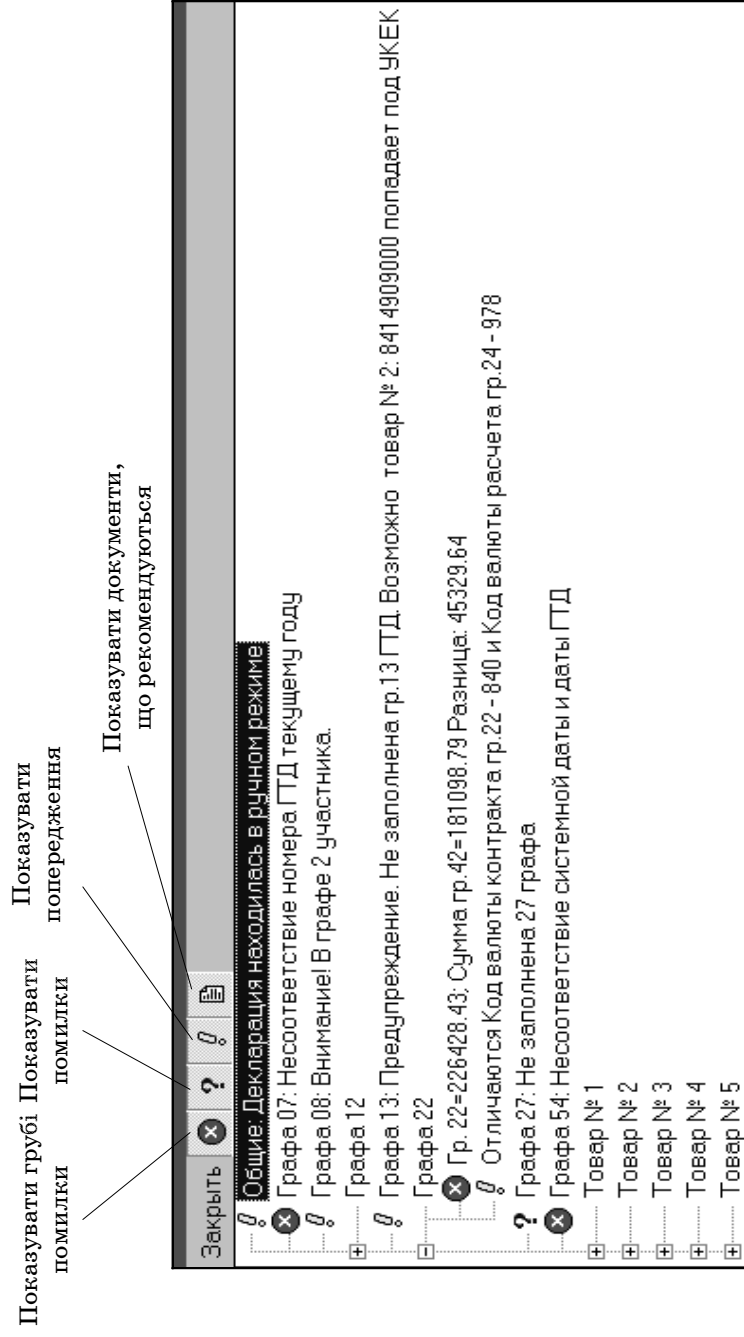


Рис. 13.6. Список помилок

Довідники в програмі викликаються трьома способами:

- 1) натисканням на шапку графі;
- 2) клавішею F2;
- 3) натисканням правої кнопки миші й обранням позиції “Довідники”.

Базою для заповнення ВМД є довідники. Розглянемо роботу довідників на прикладі довідників банків, учасників ЗЕД та УКТЗЕД.

Довідник суб'єкта ЗЕД

Для створення нового суб'єкта ЗЕД слід використовувати пункт меню: *Довідник — Учасники ЗЕД* (рис. 13.7). У вікні відображаються усі юридичні особи, які можуть брати участь у зовнішньоекономічній діяльності. Вся інформація згрупована у відповідні підрозділи — вкладки, які, у свою чергу, містять поля з інформацією. З лівого боку вікна наведено перелік уже наявних (уведених раніше) суб'єктів ЗЕД. Для маніпуляцій з таблицею “Учасники ЗЕД” користуйтеся навігатором на панелі інструментів угорі вікна.

Для того щоб фірма з'явилася на виклик довідника в гр. 14 під час заповнення ВМД потрібно встановити прапорець *Декларант* і занести номер ліцензії на здійснення брокерської діяльності (рис. 13.8). Натиснувши на напис “№ ліцензії”, можна вибрати тип брокерської ліцензії з довідника.

Якщо у введеній фірмі немає коду платника податків, то програма для внутрішніх зв'язків запропонує використати код ЄДРПОУ (додавши перед ним нулі). Цей код використовувати не програма MD-Declaration, але друкуватися й передаватися в електронну копію він не буде.

Для заповнення банківських реквізитів необхідно користуватися робочою панеллю внизу вікна. Заповнюючи ідентифікаційний номер і код МФО банку, можна скористатися відповідними довідниками, натиснувши на шапці “Код МФО”. Код ЄДРПОУ та адресу буде внесено автоматично.

Уважно поставтеся до заповнення реквізиту “Тип рахунку”. Ці дані будуть використані під час формування (розбиття на частини) графі А і друку типу рахунку (“р/р” або “в/р”) у графі 28.

Рис. 13.7. Довідник учасників ЗЕД

☒ Гр.14 Декларант № ліцензії:	10000/0179БМ-00258	выдана:	07.03.2001	15
---	--------------------	---------	------------	----

Рис. 13.8. Графа 14 Довідника учасників ЗЕД

Якщо фірма має стандартні транспортні засоби для заповнення граф 18, 21, необхідно занести їх у закладку “Перевізник”.

Дані для автоматичного заповнення графи 54 (працює зв’язок гр. 14—54) і деякі інші винесено у закладку “Додатково”.

За збереження інформації про учасника ЗЕД відбувається контроль уведеного коду ЄДРПОУ.

Довідник банків

Вікно *Довідник банків* (рис. 13.9) дає змогу вести інформацію про банки учасників ЗЕД, тобто вводити нову інформацію, додавати відомості до наявної, оновлювати інформацію, а також здійснювати пошук необхідного банку.

Рис. 13.9. Довідник банків

Переміщення на полях вікна *Довідник банків* відбувається за допомогою клавіші <Tab> на клавіатурі або за допомогою курсора миші. Заповнення усіх полів вікна *Довідник банків* здійснюється набором символів з клавіатури. Для пошуку (вибору) певного банку (для перегляду інформації й роботи з нею) використовують на панелі інструментів кнопку *Пошук банку*, у результаті чого на екрані з’являється діалогове вікно *Довід-*

ники, що пропонує вибрати потрібний банк зі списку наявних.

УКТЗЕД

Для роботи з довідником УКТЗЕД необхідно вибрати пункт меню *Довідники→УКТЗЕД* або натиснути на шапці гр. 33. У цьому довіднику можна шукати потрібний товар за його назвою (рис. 13.10), за кодом (рис. 13.11), отримати довідку з тарифного і нетарифного регулювання зі списком регламентуючих документів, необхідні платежі, довідку про товар залежно від країни походження та напряму вантажу, отримати інші пояснення (рис. 13.12).

13.3. Програмне забезпечення QD Professional

QD Professional (Quick Declaration professional — QDPro) — програмно-технологічний комплекс митної системи України, призначений для ведення ефективної зовнішньоекономічної діяльності, програма автоматичного заповнення вантажних митних декларацій. Підсистеми **QD Professional** містять: повну нормативну базу, заповнення вантажної митної декларації, мита і режими, українську класифікацію товарів ЗЕД, алфавітно-предметний покажчик товарів, попередній розрахунок угод, потужну інформаційно-довідкову систему з митного законодавства тощо.

Функціональні можливості комплексу:

- повний комплект необхідних довідників із зовнішньоекономічної діяльності (мита, акциз, сертифікація, квотування тощо);
- автоматичний контроль правильності введення інформації під час заповнення декларації;
- автоматичний розрахунок митних платежів з урахуванням усіх вимог законодавства (мито, акциз, ПДВ, митні збори та інші платежі);
- повна перевірка декларації за алгоритмами програмного комплексу “Митний інспектор” і більш детальна за власними алгоритмами;

Поиск по товарной номенклатуре

Наименование товара:

бананы

☒ УКТЗЕД
 ☒ Пояснения к ТНВЭД СНГ
 ☒ Комментарии к тарифу
 ☒ Комментарии к регламентации
 ☒ АПУ
 ☒ Классификационные решения
 ☐ Медицинские препараты

☐ Поиск по результатам поиска

Найдено записей: 2

0803 00

1 Бананы, включаючи плантайны, свіжі або сушені:

1106

2 Борошно, крупа та порошок з сушених бобових овочів товарної позиції 0713, з серцевини сагової пальми або з коренеплодів чи бульбоплодів товарної позиції 0714 або продуктів групи 08:

Рис. 13.10. Пошук товару за назвою

[illegible]

Рис. 13.12. Загальна довідка про товар

- оперативне одержання інформаційно-довідкових та аналітичних матеріалів для мінімізації ризиків під час експортно-імпортних операцій;
- друк декларацій, документів, звітів на принтерах будь-якого типу з можливістю попереднього перегляду, зміни параметрів шрифту, а також з використанням текстового режиму принтера;
- форматування електронної копії декларацій у форматі програмного комплексу “Митний інспектор”;
- читання електронних копій, підготовлених іншими програмами.

QDPro можуть використовувати: учасники ЗЕД, митні брокери, митні ліцензійні склади, міжнародні перевізники, митні органи, юридичні контори, банківські установи.

Структура додатка QD Professional

Системне меню (рис. 13.13) QD Professional з’являється при натисканні однієї з кнопок мишки на іконці, розташованій унизу праворуч на панелі задач .

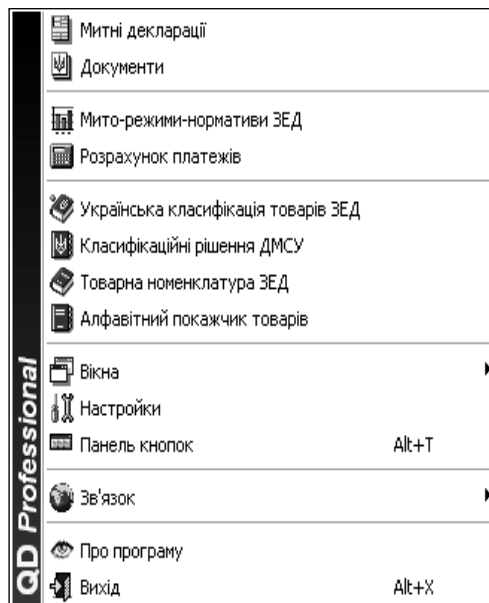


Рис. 13.13. Системне меню програми

Це меню складається з таких частин:

- митні декларації;
- документи;
- мита — режими — нормативи ЗЕД;
- розрахунок платежів;
- українська класифікація товарів ЗЕД;
- класифікаційні рішення ДМСУ;
- товарна номенклатура ЗЕД;
- алфавітно-предметний покажчик;
- вікна;
- налаштування;
- панель кнопок;
- зв'язок;
- про програму;
- вихід.

Вибір кожного з елементів меню зумовлює запуск відповідного модуля.

Кожна з підсистем застосовується для виконання певного кола завдань. Для інформаційно-консультативних цілей використовуються *Документи*, для безпосереднього декларування вантажів — *Митні декларації*.

Кожна з підсистем є інтегрованим середовищем, тобто спирається на модулі більш низького рівня. У кожній підсистемі є своє **головне меню**, подане у вигляді смужки вгорі вікна програми з текстовими заголовками. Вибір будь-якого пункту меню зумовлює розгортання вкладеного списку. Частина пунктів меню в розгорнутому списку містить вкладене меню. Вибір кінцевого пункту меню забезпечує виконання відповідних дій. Звертатися до меню можна за допомогою мишки (ліва кнопка) або за допомогою клавіатури (виклик — клавіші *Alt* або *F10*, стрілки — переміщатися, а *Enter* — робити вибір).

Користувацький інтерфейс QD Professional відповідає вимогам сумісності з Windows і, відповідно, міжнародним стандартам використання.

Структура вікна. Вікно програми складається з рядка заголовка (наприклад, QDPro-документи), головного меню вікна (наприклад: Документи, Товарна номенклатура, Довідники, Допомога) і сцени — спеціальної зони, де містяться різні вікна

(наприклад, вікно *Пошук*). Сцена має кілька зон відображення. Розмір їх можна змінювати. Кожне вікно має свій ярлик у верхній частині зони відображення. Щоб переключитися на інше вікно зони необхідно клацнути лівою кнопкою мишки на відповідному ярлику. За замовчуванням уся робота з документами ведеться у двох зонах — лівій і правій. За смугою головного меню йде панель інструментів, що містить кнопки основних функцій для роботи з таким модулем. У будь-якій частині програми можна викликати додаткове меню — спливаюче (контекстне меню, яке викликається правою кнопкою мишки), воно з'являється за вимогою, а в інший час його не видно. Спливаючі меню, як правило, контекстно залежні, тому важливо, над яким елементом вікна меню було активізовано.

Система QDPro-документи

Така система є інтегрованим пакетом, що забезпечує зручний і швидкий механізм роботи з документами, товарною номенклатурою і різними довідниками для ведення і планування зовнішньоекономічної діяльності.

База документів містить звід необхідних законів, постанов і указів, листів Державної митної служби України, регіональних митниць та ін. База документів постійно оновлюється і містить актуальну інформацію з митного законодавства.

Програма QD Professional має швидку і потужну пошукову систему. Пошук документів виконується за різними параметрами, включаючи номер документа, діапазон дат, тип документа, фрагмент назви, слова з тексту тощо.

Вікно програми ***QDPro-документи*** (рис. 13.14) поділяється на 4 частини:

1. Головне меню: Документи, Товарна номенклатура, Кодекси України, Довідники, Допомога.
2. Зона пошуку: Пошук, Каталог, Добірки.
3. Зона відображення документів: Список документів, Робота з документами.
4. Панель режимів: переключення між вікнами.

Під режимом у програмі розуміється набір вікон, з'єднаних логічно і візуально тематикою змісту. Переключення режимів відбувається неявно — виклик вікна з новою темою переключає поточний режим.

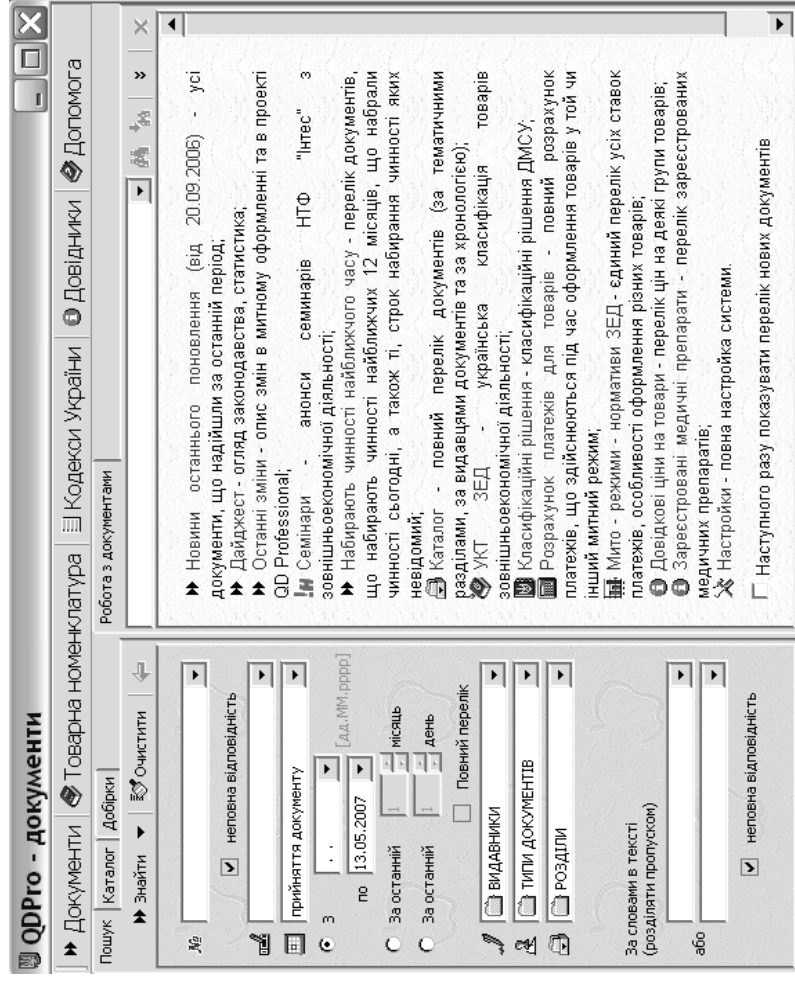


Рис. 13.14. Вікно програми QDRPro-документи

Для впорядкування потоку нормативних актів кожен документ належить до однієї або декількох тематичних груп. Усі теми (розділи) зведено в деревоподібну структуру *рубрикатора*. Потрібно знати, що рубрикатор відповідає сприйняттю структури митної нормативної бази працівниками митниці й у багатьох випадках є ключем до розуміння суті документа. Для кожного розділу рубрикатора є його короткий опис та окрема роз'яснювальна стаття. Щоб перейти в ознайомлювальний режим слід натиснути спеціальну кнопку в правому верхньому куті вікна. Після цього можна мишкою (або стрілками клавіатури) переміщатися по рубрикатору і читати короткий опис. *Рубрикатор* — складова *Каталогу*, який відображає повний список документів або результати пошуку і містить: *Розділи* — перелік тематичних груп документів, *Видавці* — дає змогу вибрати видавців документа зі списку, *Хронологія* — розбиття документів за роками і місяцями підписання.

Для огляду документів з певної тематики використовується *Каталог*, а для специфічних питань застосовуються *Добірки*. Результати пошуку, переліки документів з каталогу і добірок відображаються як *Список документів*.

Крім основної функції — можливості увійти в текст — список дає можливість сортувати елементи за різними критеріями (датой прийняття, набрання чинності, за номером) та поміщати кожен з них у кейс. *Кейс* — це сховище посилань на тексти, наповнюється користувачем за його розсудом (спливаюче меню — Кейс). Дає змогу заводити папки і наповнювати їх посиланнями, а як список документів — увійти в текст виділеного елемента.

Інший спосіб запам'ятати потрібний документ — це залишити в ньому *закладку*. У тексті закладки виділяються різними кольорами, залежно від типу, і позначаються коментарями користувача. Список закладок дає можливість знайти потрібний документ за таким коментарем. *Список документів* — це перелік документів, що задовольняють заданий запит, наприклад, *Пошук*, відображення *Новин* або вибір одного з розділів *Каталогу*.

Головне меню програми *QDPro-документи* подано на рис. 13.15.

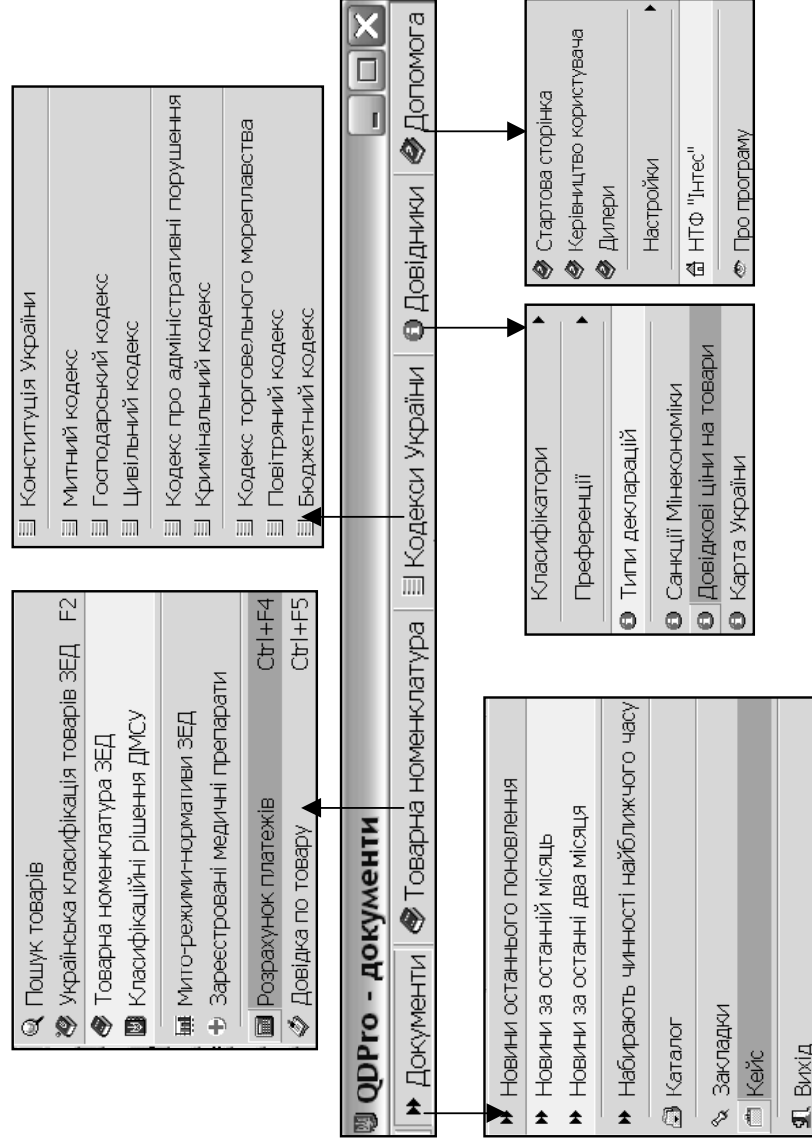


Рис. 13.15. Головне меню програми QDPPro-документи

QD Professional має засоби для ідентифікації товарів і подальшої роботи з ними. Пошук коду товару за його описом здійснюється одночасно в декількох джерелах: УКТЗЕД, ТН ЗЕД, ТН ЗЕД СНД та ін. Спираючись на код товару, система дає можливість одержати вичерпну *довідку про товар*. Загальна довідка містить як тарифне (мито, акциз), так і нетарифне регулювання переміщення такого товару через митний кордон у режимі імпорту, експорту і транзиту.

Накладаючи додаткові умови на довідку відповідно до майбутнього посилання, можна врахувати такі параметри, як напрям переміщення вантажу, митний режим, країну походження (відправлення) тощо.

У QD Professional подано переліки преференцій, довідкові ціни на товар, санкції Міністерства економіки до українських підприємств і нерезидентів України, а також усі необхідні класифікатори.

Довідкова інформація територіального змісту пов'язана з *картою України*. Це митні установи, пункти пропуску на кордоні, митні ліцензійні склади, місця прибуття автотранспорту та ін.

Пошук документів

Під час вибору вкладки *Пошук* (рис. 13.16, а) розкривається підменю: *Знайти (Повний пошук)*, *Пошук у знайденому* (рис. 13.16, в). Вікно пошуку має ряд полів введення, наповнення яких є складеним ключем для пошуку. Чим більше полів введення заповнено, тим конкретніше завдання на пошук, тим точнішим буде його результат.

Можна задавати такі атрибути пошуку:

- *Номер документа.*
- *Назва документа.*
- *Тип дати.*
- *Діапазон дат:*

1) з — по (граничні дати);

2) за останній < > місяць (дає змогу вказати кількість найближчих місяців);

3) за останній < > день (дає змогу вказати кількість найближчих днів).

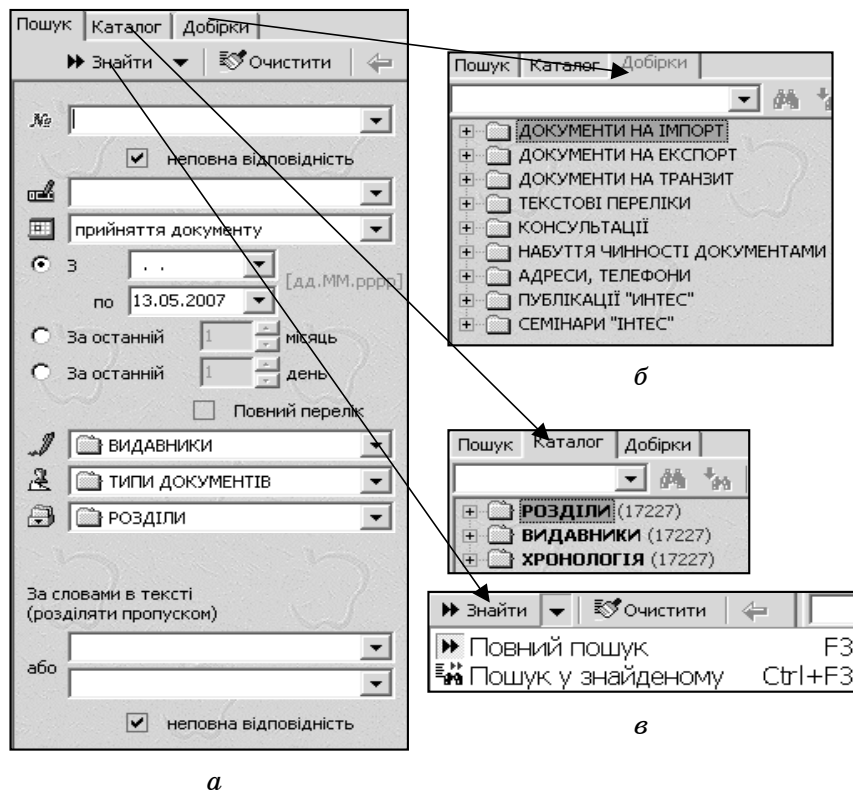


Рис. 13.16. Пошук, Каталог, Добірки

- Видавці.
- Типи документів.
- Розділи.
- За словами в тексті.

Запуск процедури пошуку виконується натисканням кнопки *Знайти* на панелі керування або за допомогою клавіші *Enter*. Очищення полів введення здійснюється за допомогою кнопки *Очистити*.

Якщо потрібно скоротити отриманий список за допомогою додаткових умов пошуку, можна використовувати пошук у знайденому (фільтр). Для цього у вікні пошуку потрібно зміни-

ти стан кнопки *Знайти* (повний пошук, *F3*) на *Фільтр* (пошук у знайденому, *Ctrl+F3*). Задавши нові параметри пошуку і натиснувши кнопку *Фільтр*, одержимо скорочений список.

Добірки (рис. 13.16, б) містять багато аналітичних матеріалів, статей, зведених таблиць, згрупованих за темами. Це ряд готових рішень, що не потребують аналізу нормативної бази. Наприклад, добірка *Документи на імпорт* містить відомості про всі документи, необхідні для імпорту товарів. *Добірки*, як і *Каталог*, мають деревоподібну структуру. Однак, на відміну від *Каталогу*, його елементи посилаються не на списки документів, а на тексти.

Система QDPro-декларації

Система *QDPro-декларації* складається з довідника типів декларацій, довідника митних процедур, довідника митних платежів, довідника способів платежів тощо. За допомогою цієї програми можна вводити нову декларацію, редагувати, друкувати, поєднувати декларації, перекомпоновувати декларації, здійснювати пошук декларацій і товарів, створювати електронну копію, вибирати зі списків різні довідники тощо.

Виклик програми *QDPro-декларації* здійснюється через системне меню (рис. 13.13), пункт *Митні декларації*. Після завантаження вікно програми має вигляд, поданий на рис. 13.17.

Декларації подано у вигляді списку, в якому відображається така інформація: номер ВМД (гр. 5), дата заповнення ВМД, тип декларації, дані про відправника (експортера), дані про одержувача (імпортера), кількість товарів і кількість аркушів декларації, митна й фактурна вартість, код митної установи/остання цифра року (з гр. 7).

Крім даних з основного списку, про кожну декларацію може надаватися додаткова інформація з платежів, а також дані стосовно товарів декларації. До кожної декларації можна додати примітки особистого характеру.

Відомості, що містяться в примітці, не впливають на формування електронної копії, ніде не друкуються і мають інформаційний характер. У нижній частині вікна винесено курси валют, використані в цій декларації.

Головне меню програми *QDPro-декларації* складається з таких пунктів: *Декларації*, *Друк*, *Вид*, *Довідники*, *Установки*, *Довідка* (рис. 13.18).



Рис. 13.17. Вікно програми QDPro-декларації

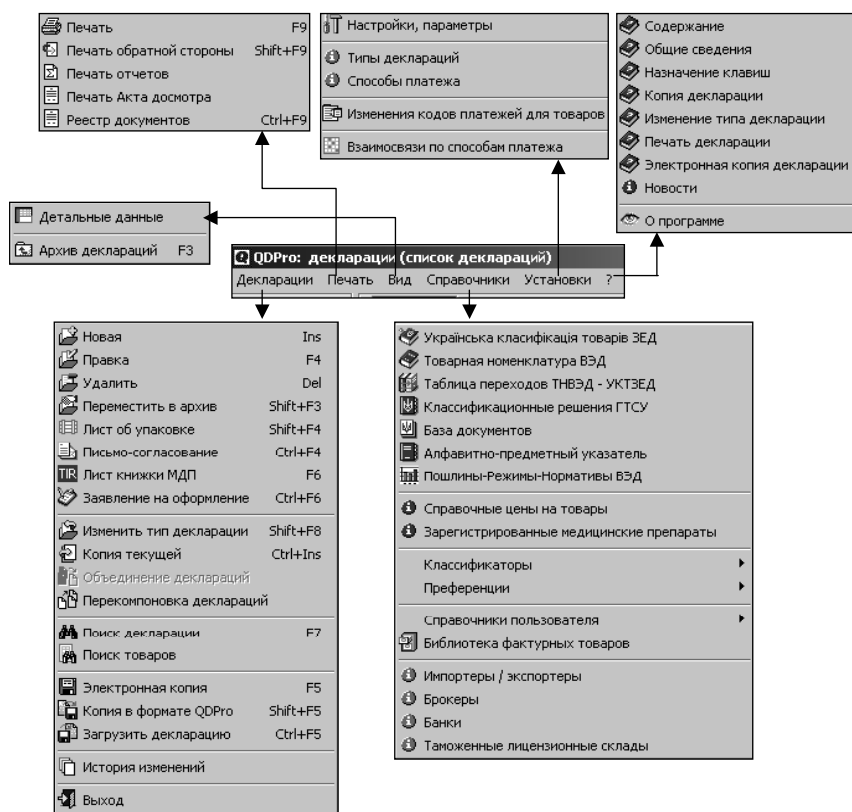


Рис. 13.18. Головне меню QDPro-декларації

Доступні функції з меню можна викликати через спливаюче (контекстне) меню або за допомогою функціональних клавіш унизу вікна, чи за допомогою гарячих клавіш.

Створення та редагування декларацій

Програма QDpro заповнює ВМД відповідно до “Положення про вантажну митну декларацію”, затвердженого Кабінетом Міністрів України. Для створення нової ВМД у вікні *QDPro: декларації* (рис. 13.18) необхідно вибрати пункт меню *Декларації* → *Нова* і вказати тип декларації. Відкривається вікно бланка ВМД, графі якого необхідно заповнити. Для різних типів

декларацій є різні вимоги щодо заповнення окремих граф (наказ № 307 “Інструкція про порядок заповнення ВМД”). Графи, що заповнюються для одного типу ВМД, можуть не заповнюватися для іншого. Інформаційний контроль декларації проводиться під час її заповнення і виходу з режиму заповнення ВМД.

Для редагування декларацій передбачене вікно (рис. 13.19), що умовно ділиться на чотири функціональні частини:

- головне меню і панель кнопок (верхня частина форми);
- вікно навігації за графами декларації (ліва частина форми, може бути “виключена”);
- сторінка даних декларації;
- панель призначення функціональних клавіш.

Декларация №1 тип: [ЕК 10] Режим заполнения: автомат

Декларация Товары Вид Правка Переход Справочники Установки ?

Заполненные графы [ЕК 10]

А. Розрахункові рахунки декларанта

Б. Виділення / експорт

В. Одержувач / імпортер

Г. Кількість специфікацій

Д. Всього товарів

Е. Довідковий номер

Ж. Особа, відп. за фін. врегул.

З. Торговельна країна

И. Експортний контроль

К. Країна відправлення

Л. Країна призначення

М. Транспортний засіб при відправленні

Н. Контейнер

О. Транспортний засіб на кордоні

П. Умови поставки

Р. Характер угоди

С. Вид транспорту на кордоні

Т. Вид транспорту в межах країни

У. Місце завантаження / розвантаження

Ф. Фінансові та банківські відомості

Х. Митниця на кордоні

Ц. Платежі

Ч. Код товару

Ш. Опис товару

Щ. Код країни походження товару

Ъ. Преференція

Ы. Проходження

Э. Вага бруто

Ю. Вага нетто

Я. Кофта

Аб. Підсередній документ

Ав. Код додаткової одиниці виміру

Аг. Фактурна вартість товару

УНІФІКОВАНИЙ АДМІНІСТРАТИВНИЙ ДОКУМЕНТ

2. Відправник / експортёр

3. Дод. арк.

4. Специф.

5. Товарів

6. Місць

7. Довідковий номер

8. Одержувач / импортер

9. Особа, відп. за фін. врегул.

10. Країна імп. признач.

11. Торговельна країна

12. Загальна нитт. варт.

13. Країна походження

14. Декларант / представник

15. Країна відправлення

16. Країна призначення

17. Країна призначення

18. Трансп. засіб відправлення

19. Конт.

20. Умови поставки

21. Трансп. засіб на кордоні

22. Валюта та факт. вартість

23. Курс валют

24. Характ. угоди

25. Вид трансп. на кордоні

26. Вид трансп. в країні

27. Місце завантаження

28. Фінансові та банківські відомості

29. Митниця на кордоні

30. Місце огляду товару

Курс USD 5,3315 Курс EUR

Загальна вага (брутто)

Розподіл Валюта Курс Сума

Загальна вартість товарів в валюті контракту 840 USD 5,3315 26611,34

Додаткові витрати (згідно фактури)

Транспортування

Рис. 13.19. Вікно заповнення декларації

У вікні редагування декларацій доступні такі функції: налаштування вікна редагування, вибір режиму роботи, властивості заповнення гр. 44, контроль декларації під час виходу з редагування, список заповнюваних граф декларації, розмір вікна редагування, контроль декларації, формування електронної копії ВМД, друк ВМД, перегляд платежів за декларацією, перегляд і редагування списку товарів декларації, перерахунок декларації, перегляд добірки документів, вибір даних з довідників.

Графи декларації, що не заповнюються, підсвічуються темним кольором, і курсор уведення з клавіатури не встановлюється у поле даних графи.

Перегляд платежів за декларацією

Для перегляду підсумкового списку платежів за такою декларацією (гр. 47, В) передбачено вікно (рис. 13.20), у якому відображаються всі типи платежів, суми до оплати і спосіб платежу.

Щоб викликати таке вікно, можна скористатися опцією меню *Платежі*, функціональною клавішею *F8* або відповідною кнопкою на панелі інструментів.

ПЛАТЕЖИ ПО ДЕКЛАРАЦИИ № 1
Валюта контракта: USD Курс: 5.3315 грн

Декларация

Тип декларации	ЕК.10
Дата декларации	10.09.2003
Фактурная стоимость	141878.36 грн
Таможенная стоимость	144544.11 грн
Количество товаров	1

Платежи

код платежа	название платежа	сумма	СП
010	Митне оформлення товарів та інших предметів	289.09 грн	01
ВСЕГО:		289.09 грн	

Рис. 13.20. Перегляд платежів

Перерахунок декларації

Під час внесення або зміни даних у деяких полях декларації може виникнути ситуація, коли необхідно виконати розрахунок усіх платежів за даною декларацією, а також митної і фактурної вартості товарів декларації з урахуванням додаткових витрат (транспортування, страхування, пакування тощо). Для таких цілей у програмі передбачено режим перерахунку декларації.

Для процедури перерахунку декларації можна скористатися опцією меню *Перерахунок*, функціональною клавішею [Shift + F2] або відповідною кнопкою на панелі інструментів.

Перегляд і виправлення списку товарів декларації

Для роботи з товарами декларації, крім основної панелі товарів на сторінці даних декларації, передбачене додаткове вікно (рис. 13.21), у якому всі товари декларації подано у вигляді списку. Щоб викликати це вікно, можна скористатися опцією меню *Товари і вартість*, функціональною клавішею F9 або відповідною кнопкою на панелі інструментів. У цьому вікні можна додавати і видаляти товари, вносити виправлення в дані про товари. При цьому під списком товарів виводиться довідкова сумарна інформація про товари, а також аналогічна інформація про основну частину декларації. У разі розбіжності суми фактурної вартості або ваги числа виділяються відповідно синім (недобір) або червоним (перебір) кольором. Таким чином, можна послідовно збалансувати вартість, кількість місць і вагу кожного товару в декларації із загальною фактурною вартістю (гр. 22), кількістю місць за декларацією (гр. 6) і загальною вагою товарів за декларацією (вказується як розрахункова величина в гр. 22).

Шукати товар можна за назвою і кодом, скориставшись пошуком за УКТЗЕД (рис. 13.22), та шляхом одержання загальної довідки (рис. 13.23).

Контроль декларації

Для перевірки заповнення декларації передбачено відповідне вікно *Перевірка заповнення декларації* (рис. 13.24), яке викликається з меню *Декларація — Контроль декларації*. У цьому вікні відображається список усіх помилок, допущених під час заповнення декларації. Якщо контроль здійснюється в ре-

Товары в декларации									
№	Товар Код	Фактурная стоимость		Таможенная стоимость	мест	Вес		СТС	
		В валюте	В гривнах			брутто	→ нетто		
1	4104221000	26611,34	141878,36	144544,11	13	12840		12580	
1	Сумма по товарам	26611,34	141878,36	144544,11	13	12840		12580	
	По основной части	26611,34	141878,36	144544,11	13				
31. Вантажні місця та опис товару									* - СТС - справка-расчет таможенной стоимости
ШКТЯНИЙ НАПІВФАБРИКАТ ДУБЛЕНИЙ із сливки сировини ВРХ "ВЕГ-ЕЛУ" коэф. волог. 1.0 Зматун. 11266шт. 12580кг, 7603,24 м2, 13палет Виробник ЗАТ "Чинбар", Україна 3. 0									31. Тип места Повне місце
Контейнер									31. Количество товара 41. Допол. единица измерения
47. Начисление пошлин и таможенных платежей									36. Преференц. 000 000 000
Ставка									37. Процедура 10 00 50
Вид Основы начисления									34. Код страны происх. ☒ подтвержд. происхождения
Сумма									Валюта СП

31. Вантажні місця та опис товару	ШКТЯНИЙ НАПВФАБРИКАТ ДУБЛЕНИЙ ІЗ СПІЛКА СИРОВИНИ ВРХ "ВЕТ-БЛУ" КОЕФ. ВОЛОГ. 1.0 2штатун. 11266шт. 12580кг, 7603,24 м2, 13палет Виробник ЗАТ "Ци́нар", Україна 3. 0											
31. Тип міста	Повне місце										▼	
31. Кількість товару											41. Доповн.єдниця измерения	
36. Преференц.	000	000	000	000	000	000	000	000	000	000	000	34. Код страны проищ.
37. Процедура	10	00	00	50	804	804	804	804	804	804	804	34. Код страны проищ.
38. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	38. Подтвержд.
39. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	39. Подтвержд.
40. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	40. Подтвержд.
41. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	41. Подтвержд.
42. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	42. Подтвержд.
43. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	43. Подтвержд.
44. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	44. Подтвержд.
45. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	45. Подтвержд.
46. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	46. Подтвержд.
47. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	47. Подтвержд.
48. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	48. Подтвержд.
49. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	49. Подтвержд.
50. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	50. Подтвержд.
51. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	51. Подтвержд.
52. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	52. Подтвержд.
53. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	53. Подтвержд.
54. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	54. Подтвержд.
55. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	55. Подтвержд.
56. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	56. Подтвержд.
57. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	57. Подтвержд.
58. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	58. Подтвержд.
59. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	59. Подтвержд.
60. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	60. Подтвержд.
61. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	61. Подтвержд.
62. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	62. Подтвержд.
63. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	63. Подтвержд.
64. Подтвержд.	000	000	000	000	000	000	000	000	000	000	000	64. Подтвержд.
65. Подтвержд.	000											

Рис. 13.21. Товари в декларації

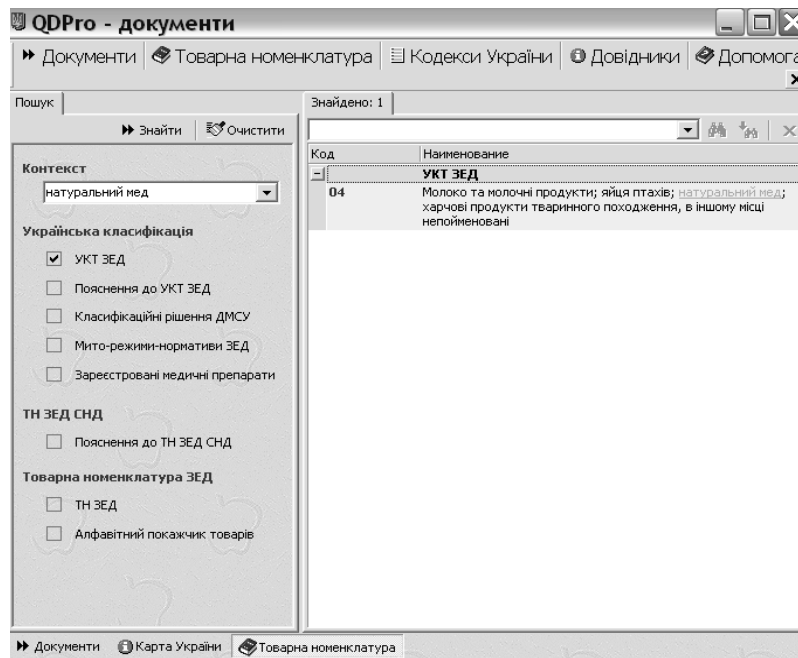


Рис. 13.22. Пошук товару за назвою

жимі виправлення декларації, то під час виявлення помилок можна переміститися безпосередньо в графу, в якій є помилка. Для цього необхідно встановити покажчик на помилку і натиснути клавішу *Enter* або двічі клацнути мишею. При цьому графа, в якій виявлено помилку, стає поточною й одержує курсор уведення з клавіатури.

QDPto - документи

ДокументиТоварна номенклатураКодекси УкраїниМіжнародні конвенціїДовідникиДопомога

ПошукУКТ ЗЕДДовідка по товару 0409 00 00 00Знайдено: 1

0408Яйця птаці без шкаралупи та яєчні жовтки, свіжі, сушені, варені у воді або на парі, форовані, морожені або консервовані іншим способом, з доданням чи без додання цукру чи інших пасолодуювальних речовин:

0409 00 00 00Мед натуральний

0410 00 00 00Харчові продукти тваринного походження, в іншому місці не зазначені

Група 05Інші продукти тваринного походження, не включені до інших угруповань

Розділ II (06-14)Продукти рослинного походження

Розділ III (15)Жири та олії тваринного або рослинного походження; продукти їх розщеплення; готові харчові жири; воски тваринного або рослинного походження

Розділ IV (16-24)Готові харчові продукти; алкогольні та безалкогольні напої; оцет; потион та його замінники

Розділ V (25-27)Мінеральні продукти

Розділ VI (28-38)

ДОВІДКА ПО ТОВАРУ 0409 00 00 00

на 14.05.2007 р. (останнє поновлення БД 09.02.2007)

УКТ ЗЕД

Мед натуральний

Додаткова одиниця виміру відсутня

Основна одиниця виміру кг (код 186)

ІМПОРТ

Митні та інші платежі

Ввізне мито

Являє собою податок на переміщення товарів через митний кордон України. Див. додатково преференції по миту

Пільгова ставка	0,8 EUR за кг
Повна ставка	0,8 EUR за кг
Діє	з 17.08.2005

Підстава:

Закон України ВР № 2775-IV від 07.07.2005

Коментарі:

Мед натуральний

ДокументиКарта УкраїниТоварна номенклатура

Рис. 13. 23. Загальна довідка про товар

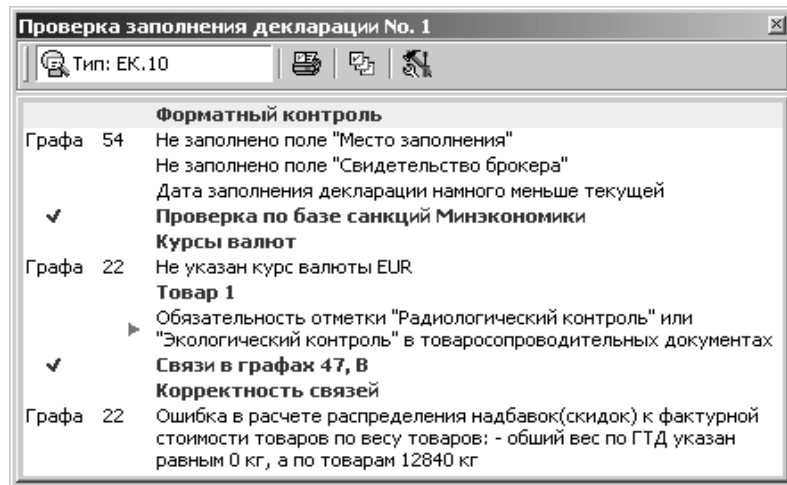


Рис. 13.24. Перевірка заповнення декларації

13.4. Програмне забезпечення Diamond Bridge

Митно-брокерська програма ***Diamond Bridge*** (TM Eugenia) є програмним продуктом нового покоління для здійснення зовнішньоекономічної діяльності, побудована на найсучасніших інформаційних технологіях, зокрема:

- 1) системі управління базами даних Microsoft SQL Server;
- 2) програмному середовищі Microsoft .Net Framework.

Використання цих технологій дає можливість:

- забезпечення надійного доступу до даних незалежно від кількості користувачів системи, яка може варіюватися від одного до багатьох десятків і сотень;
- швидкого доступу до них;
- віддаленої роботи через мережу Інтернет;
- гнучкого розмежування прав доступу користувачів до окремих модулів системи;
- надійного збереження даних з можливістю їх відновлення в разі апаратних збоїв станом на момент такого збою;
- отримати зручний стандартний інтерфейс для застосувань Windows з можливістю одночасної роботи з багатьма документами, кожен з яких відкривається у своєму вікні;

- легкої інтеграції системи з іншим програмним забезпеченням (бухгалтерського, управлінського, складського обліку тощо);

- створити сучасні протоколи зв'язку з інформаційними системами митниці.

Виходячи з можливостей, що надаються користувачеві, програмне забезпечення Diamond Bridge створює умови для роботи з усіма інформаційними ресурсами, необхідними для супроводження зовнішньоекономічної діяльності, серед яких:

- тексти нормативних документів з питань митної справи;
- нормативно-довідкова система з усіма необхідними класифікаторами;
- створення, перевірка, друк та виведення на митницю всіх типів документів: ВМД, ДМВ, транспортних накладних, облікових карток, ПТП, платіжних документів, контрактів, пакувальних відомостей та багато інших;
- підсистема митного обліку;
- все необхідне для електронного декларування та обміну електронними документами з митницею;
- гнучка система звітності й розширеного пошуку.

13.4.1. Підсистема роботи з нормативними документами з питань митної справи

Пошук текстів нормативних документів може здійснюватися за такими критеріями: номер або його частина, діапазон дат документа або його прийняття в базу даних, назва або її частина, типи, видавники, наявність або відсутність у папках (системних або власних папках користувача), за словами в тексті або їх частинами (рис. 13.25).

Для пошуку за словами використовується контекстний індекс, що дає можливість радикально збільшити швидкість пошуку. Крім того, можливий подальший пошук серед знайдених документів та серед прочитаних користувачем за останні три дні.

Папки документів мають ієрархічну структуру (рис. 13.26).

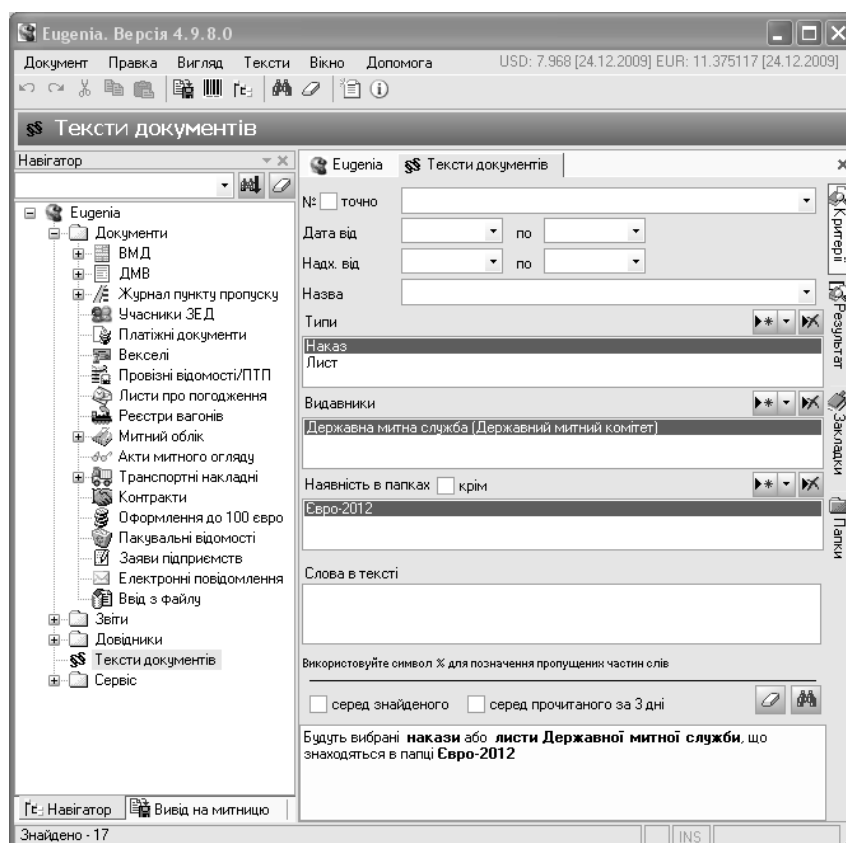


Рис. 13.25. Критерії пошуку текстів нормативних документів

За результатом пошуку видається список документів (рис. 13.27).

Користувач має можливість відкрити як один конкретний документ, так і декілька одночасно в окремих вікнах (рис. 13.28).

Основні можливості для роботи з текстом документа:

- перегляд інформації про документ (рис. 13.29);
- пошук всередині тексту;
- перегляд редакцій документа;
- розміщення його у власних папках;

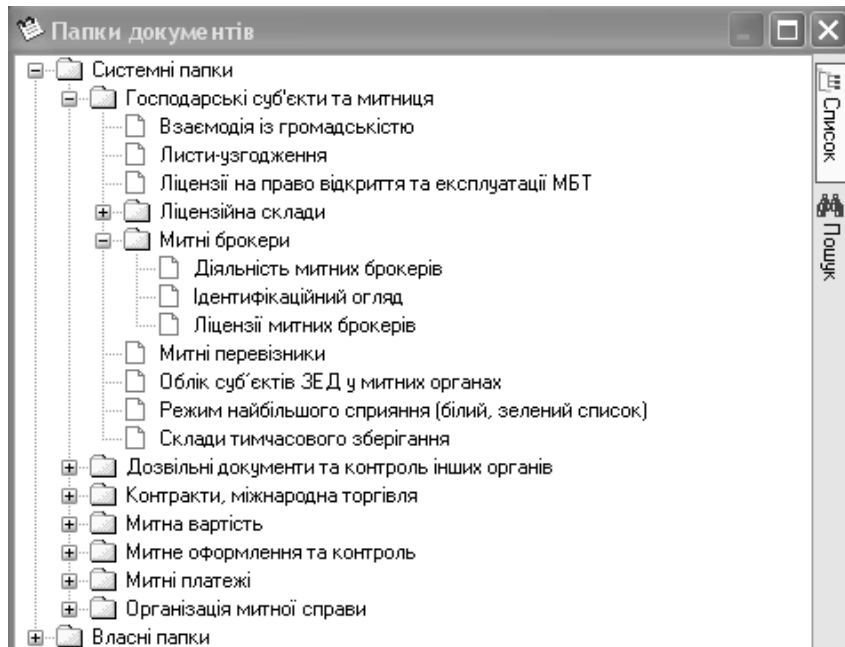


Рис. 13.26. Структура папок документів

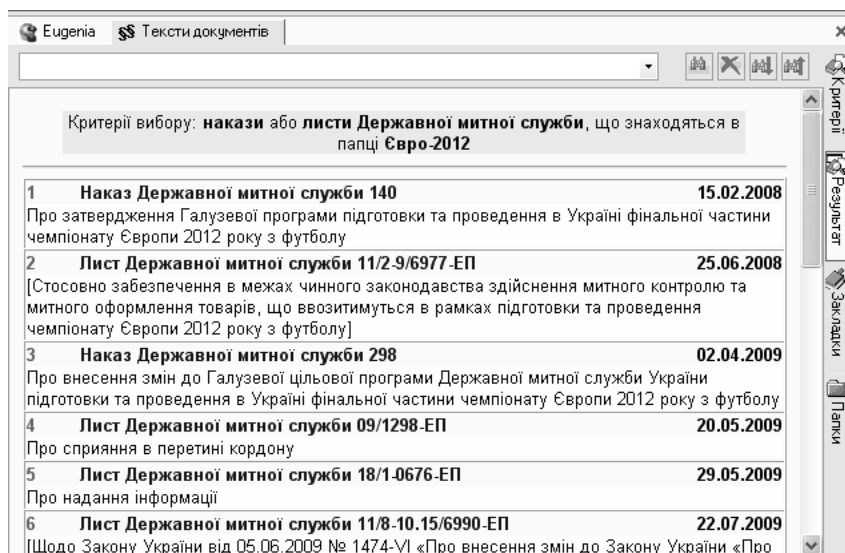


Рис. 13.27. Зразок результату пошуку документів

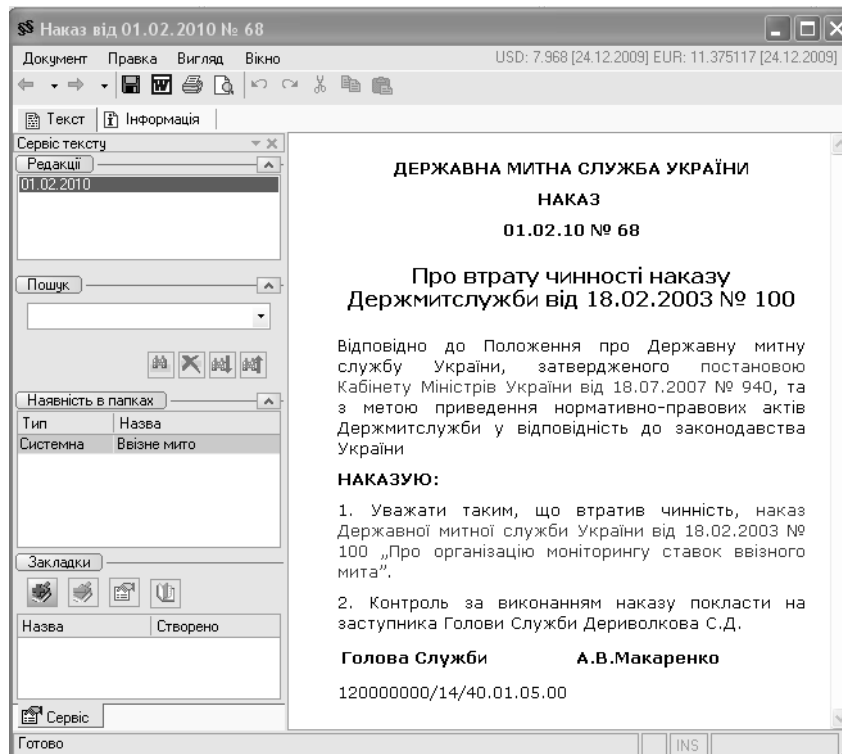


Рис. 13.28. Зразок відкритого документа

Інформаційна карта документа	
Назва	Про затвердження Інструкції про порядок заповнення вантажної митної декларації
Дата набрання чинності	09.07.1997
Дата втрати чинності	-
Тип	Наказ
Видавець	Державна митна служба (Державний митний комітет)
Номер	307
Дата	09.07.1997

Рис. 13.29. Інформація про документ

- створення закладок в документах та приміток до них, в тому числі таких, що посилаються на інші документи;
- навігатор для роботи з великими за структурою документами (рис. 13.30).

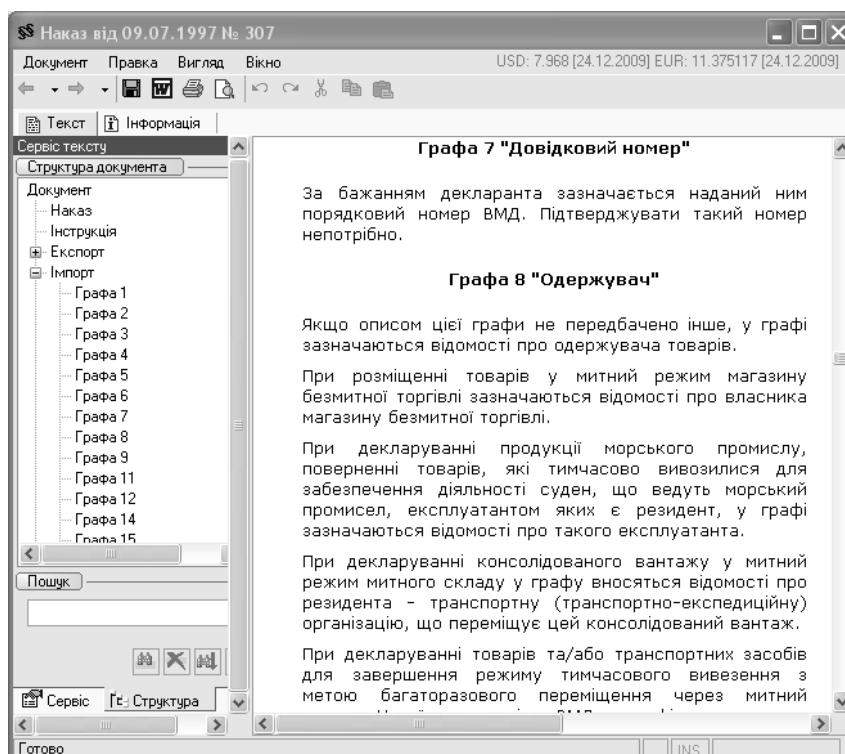


Рис. 13.30. Використання навігатора

- друк, збереження на диск та вивід у формат Microsoft Word;
- перегляд заходів нетарифного регулювання та інших контрольних процедур, що встановлюються або скасовуються документом (рис. 13.31);
- перегляд посилань на цей документ, а з нього на інші документи з можливістю фільтрації списку (рис. 13.32).

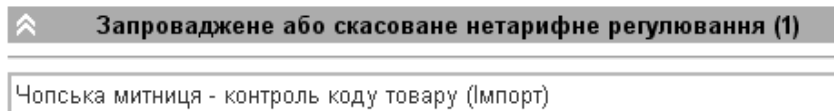


Рис. 13.31. Заходи нетарифного регулювання

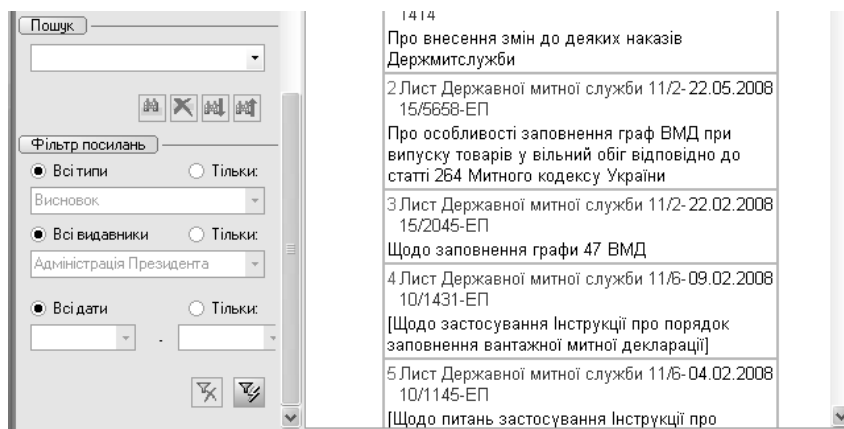


Рис. 13.32. Перелік посилань на документ

13.4.2. Робота з класифікаторами та іншою нормативно-довідковою інформацією

Програма Diamond Bridge містить усі класифікатори, що використовуються при підготовці митних документів (рис. 13.33) та велику кількість інших нормативно-довідкових матеріалів. Користувач має можливість роботи одночасно з кількома класифікаторами в окремих вкладках або вікнах програми (рис. 13.34).

Більшість довідників часово-залежні, тобто можуть бути відображені станом на будь-яку дату. У всіх класифікаторах забезпечено можливість пошуку, сортування (в тому числі за декількома колонками) та фільтрації. За кожною позицією кла-

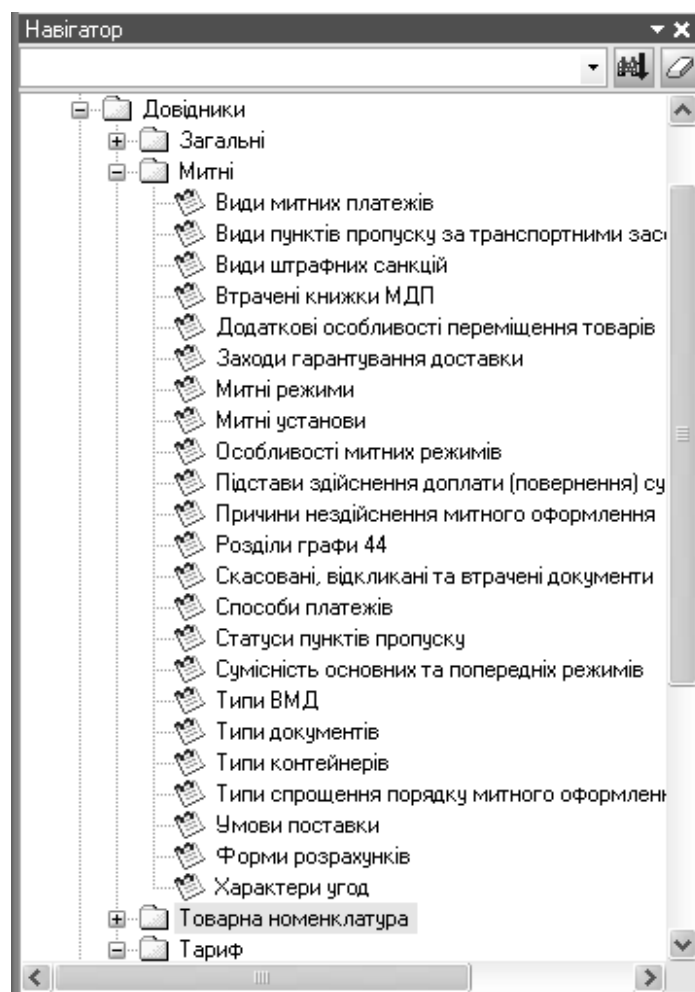


Рис. 13.33. Класифікатори програми Diamond Bridge

сифікатора наявне посилання на документ введення та, за наявності, скасування. Класифікатори можуть бути роздруковані та виведені в Excel. Там, де це потрібно, наявні можливості розширеного пошуку (рис. 13.35).

особи платєжів Митні режими Митні установи Особливості митних режимів

Назва = Станом на 30.04.2010

Категорія

G. Особливості тимчасового ввезення (вивезення)

Код	Назва	Сумісність з осно
GA	Багаторазове переміщення товарів та/або транспортних засобів через митний кордон (як в Україну, так із України)	0,31,32
GB	Зворотне ввезення товарів (транспортних засобів), тимчасово вивезених за межі митної території України згідно із законодавством на підставі інших, ніж вантажна митна декларація, документів	0
GC	Зворотне вивезення товарів (транспортних засобів), тимчасово ввезених на митну територію України згідно із законодавством на підставі інших, ніж вантажна митна декларація, документів	0
GD	Тимчасове ввезення з умовним повним звільненням від оподаткування морських і річкових суден, інших плаваючих засобів, повітряних суден, які ввозяться з метою ремонту, устаткування й матеріалів, призначених нерезидентами для будівництва та ремонту морських і річкових суден, інших плаваючих засобів та повітряних суден	31

Підстави

Документ введення Наказ Державної митної служби від 12.12.2007 № 1048 "Про затвердження відомчих класифікаторів з питань митної статистики, які використовуються в процесі оформлення митних декларацій, і порядку їх

Діє з 01.01.2008

Документ виведення

Діє до

Рис. 13.34. Використання кількох класифікаторів одночасно

Умови пошуку

Код

Назва Яр

Шукати

Очистити умови

— Стосується тільки пунктів пропуску

Категорія ПП

Вид транспорту 1 - автомобільний

Суміжна країна

Особливість

☒ Обмежити кількість результатів до: 100

Код	Назва
102030200	П/п „Нові Яриловичі - Нова Гута”
506011400	П/п „Малоярославець 1 - Чадир-Лунга”

Довідник

Пошук

Рис. 13.35. Можливості розширеного пошуку

Окремі класифікатори організовані за ієрархічним принципом (рис. 13.36).

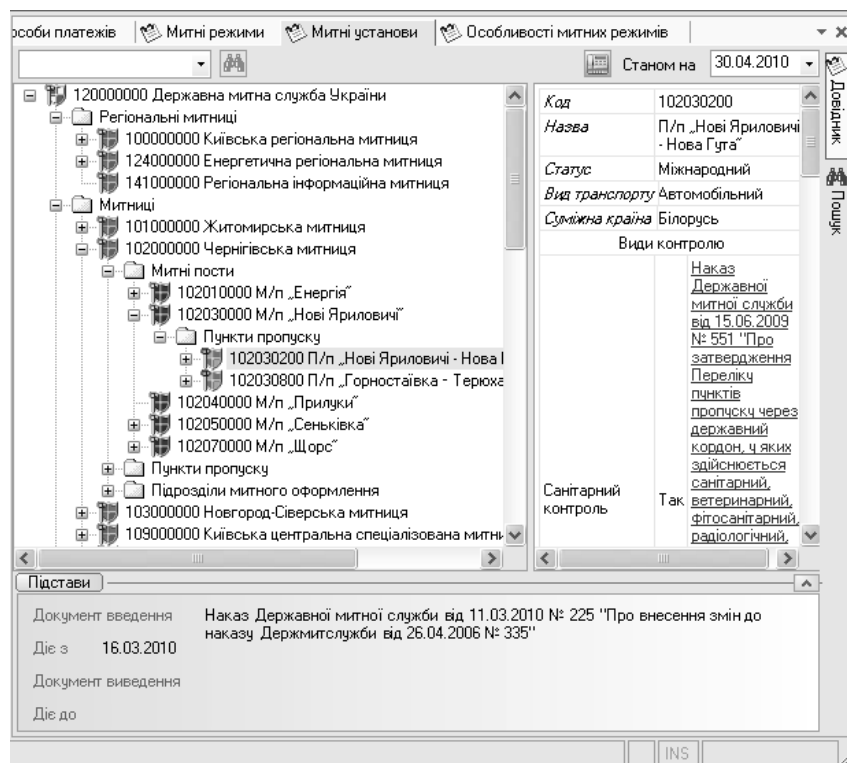


Рис. 13.36. Класифікатор з ієрархічним принципом

Широкі можливості надає, зокрема, довідник УКТ ЗЕД. Серед цих можливостей:

- пошук і розширений пошук товарів;
- перегляд приміток і пояснень до УКТ ЗЕД;
- перегляд довідки за товаром;
- наявність двох альтернативних форм перегляду: звичайна та ієрархічна (рис. 13.37, а, б).

Довідка стосовно товару, що може бути викликана як з УКТ ЗЕД, так і з багатьох інших частин програми, де використовується код товару, надає таку інформацію:

Надпорядковані рівні		
[4412] Фанера клеєна, панелі фанеровані та аналогічні матеріали з шаруватої деревини: -фанера клеєна, яка складається винятково з листів деревини, кожний лист завтовшки не більш як 6 мм;		
Код	Назва	Дод. од.
4412 13	що має хоча б один зовнішній шар деревини тропічних порід, зазначених у примітці 1 до товарних підпозицій цієї групи:	
4412 14 00 00	інша, що має хоча б один зовнішній шар з деревини листяних порід	113
4412 19 00 00	інші	113

a

Товарна номенклатура		
Станом на 30.04.2010		
Елементи УКТ ЗЕД		Дод. од.
4409 10 18 00	інші	
4409 20	з листяних порід:	
4410	Плити деревностружкові та подібні (наприклад, з орієнтованою стружкою (OSB) та вафельні плити) з деревини або з інших здерев'янілих матеріалів, просочені або не просочені смолами або іншими органічними зв'язувальними речовинами:	
4411	Плити деревноволокнисті з деревини або з інших здерев'янілих матеріалів з доданням або без додання смол або інших органічних сполучних речовин:	
4412	Фанера клеєна, панелі фанеровані та аналогічні матеріали з шаруватої деревини:	
>>>	фанера клеєна, яка складається винятково з листів деревини, кожний лист завтовшки не більш як 6 мм:	
4412 13	що має хоча б один зовнішній шар деревини тропічних порід, зазначених у примітці 1 до товарних підпозицій цієї групи:	
4412 14 00 00	інша, що має хоча б один зовнішній шар з деревини листяних порід	м3
4412 19 00 00	інші	м3
>>>	інші, що мають хоча б один зовнішній шар з деревини листяних порід:	
>>>	інші:	
Деревина пресована у вигляді блоків, плит, блоків		
Підстави		
Документ введення	Закон від 31.05.2007 № 1109-V "Про внесення змін до Закону України "Про Митний тариф України""	
Діє з	01.01.2008	

б

Рис. 13.37. Звичайна та ієрархічна форми перегляду

- код, назва товару за УКТ ЗЕД, додаткова одиниця виміру;
- тарифне регулювання;
- заходи нетарифного регулювання та контролю;

- довідкові ціни;
- класифікація товарів;
- посилання на тексти документів, що стосуються розглядуваного товару.

Крім того, наявний зручний навігатор за довідкою та можливість перегляду змін, що внесені в регулювання щодо товару за період, який цікавить користувача. Можлива фільтрація інформації за напрямом переміщення, митницею та видами регулювання.

З цього ж вікна може бути викликана форма порівняння ставок мита на товари, що знаходяться поруч в УКТ ЗЕД (рис. 13.38).

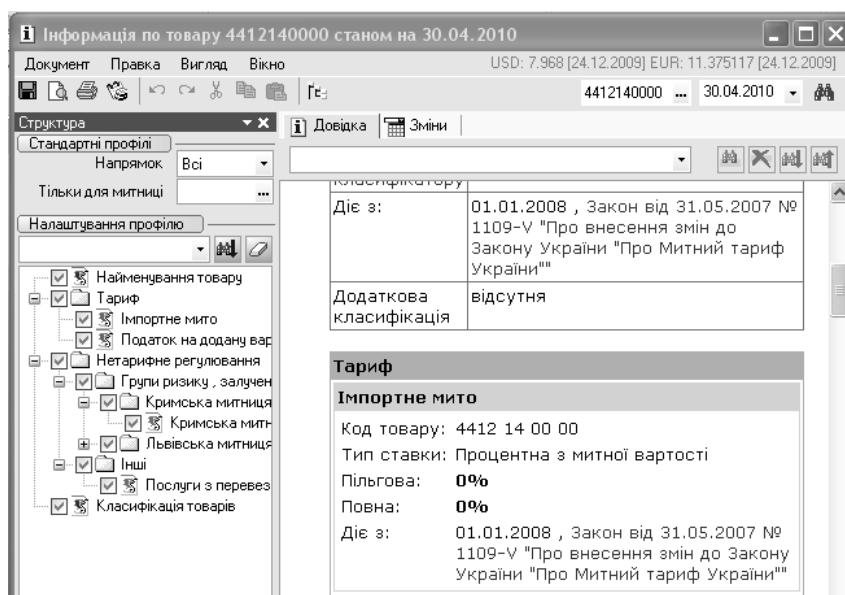


Рис. 13.38. Порівняння ставок мита

У режимі “Нетарифне регулювання” нетарифне регулювання та інші контрольні заходи можуть бути проаналізовані не тільки в розрізі коду товару за УКТ ЗЕД, але і виходячи з виду регулювання або документа введення/скасування (рис. 13.39).

Критерії пошуку

Вид регулювання: Дозвіл УКПЕК на експорт, імпорт та транзит

Код товару: ... Станом на: 05.05.2010

Документ: ... ☒ введення ☒ виведення

Результати пошуку

Код від	Код до	Примітка
2804501000		2.С.4. [1С225] Бор, збагачений ізотопом бор-10 (10В) відносно в
2804501000		6.А.1. [9А010.а - 9А010.с, 9А110] Композитні структури, шарув
2804501000		1.С.11.б. Бор або карбід бору чистотою 85 відсотків або вище т
2804501000		9.А.10.а. "Компоненти" та структури, кожна з яких вагою понад
2804501000		9.А.10.б. "Компоненти" та структури, спеціально призначені для
2804501000		4.С.2.е. е) бор (САС 7440-42-8) та його сплави у формі частинок
2804509000		6.С.2.а. Хімічно чистий первинний телур (Те) з рівнями чистоти
2805120000		2.С.5. [1С227] Кальцій, що має усі такі характеристики: а) вміст
2805199000		2.С.9. [1С233] Літій, збагачений ізотопом літій-6 (6Li) відносно в
2808000000		Примітка 2. 10) рідинні окислювачі, що містять у своєму складі і
2808000000		1.С.13.а. ^{xx} 2) азотна кислота з концентрацією вище ніж 95 відсо
2808000000		4.С.4.а.5. 5) інгібована червона димляча азотна кислота [IRF
2810001000		2.С.4. [1С225] Бор, збагачений ізотопом бор-10 (10В) відносно в

2.С.4. [1С225] Бор, збагачений ізотопом бор-10 (10В) відносно вмісту цього ізотопу у природному борі, а саме: елементарний бор, сполуки, суміші, що містять бор, вироби з них, відходи або металобрухт з будь-чого, зазначеного вище

Рис. 13.39. Режим нетарифного регулювання

Аналогічний механізм застосовується для аналізу тарифу: ввізного/вивізного мита, акцизу, антидемпінгового/компенсаційного/спеціального мита (рис. 13.40).

Довідник курсів валют може актуалізуватися безпосередньо з веб-сайта НБУ.

13.4.3. Робота з вантажними митними деклараціями

Програма Diamond Bridge містить розвинений інтерфейс для підготовки, перевірки, друку та виводу на митницю вантажних митних декларацій. Списки ВМД розділено за статусами: які перебувають у роботі, оформлені, анульовані. Як і в усіх інших списках, у списках ВМД доступні фільтрація, пошук, сортування, друк та вивід в Excel. Зі списків здійснюєть-

регулювання Ставки антидемпінгового, спеціального та компенсаційного мита (ІМ)

Критерії пошуку

Код товару ... Станом на 05.05.2010 Вид Всі

Результати пошуку

Код товару	%	фікс.	Примітка
2918 11 00 00	31.80000		молочна кислота походженням з Китайської Наро
2918 11 00 00	0.00000		
3102 30 90 00	9.76000		добрива мінеральні або хімічні, азотні: нітрат амон
3102 30 90 00	10.78000		добрива мінеральні або хімічні, азотні: нітрат амон
3102 30 90 00	11.91000		добрива мінеральні або хімічні, азотні: нітрат амон
3605 00 00 00	11.30000		сірники, крім піротехнічних виробів товарної позиц
4304	179.70000		антидемпінгове; продовжено згідно листа від 18.0
4411 11 90	68.75000		антидемпінгове
4411 11 90	0.00000		Застосування антидемпінгових заходів не розповс
4411 11 90 00	31.58000		Плити деревноволокнисті (ДВП) мокрого способу
5208 22 16 90		0.57000	тканини бавовняні, з вмістом бавовни 85 мас. % а
5208 22 19 00		0.57000	тканини бавовняні, з вмістом бавовни 85 мас. % а
5208 22 96 90		0.57000	тканини бавовняні, з вмістом бавовни 85 мас. % а

Тільки для країн: **Китай**

Тип ставки: **Процентна з митної вартості**

Мито: **31.8%**

Примітка: **молочна кислота походженням з Китайської Народної Республіки**

Підстави

Документ введення: Рішення Міжвідомчої комісії з міжнародної торгівлі від 28.05.2009 № АД-203/2009/4402-36 "Про застосування остаточних антидемпінгових заходів щодо імпорту в Україну молочної кислоти п

Діє з: 07.07.2009

Документ виведення: Рішення Міжвідомчої комісії з міжнародної торгівлі від 28.05.2009 № АД-203/2009/4402-36 "Про застосування остаточних антидемпінгових заходів щодо імпорту в Україну молочної кислоти

Діє до: 07.07.2014

INS

Рис. 13.40. Механізм аналізу тарифу

ся створення, відкриття, вивід ВМД на митницю та інші дії над ВМД та супутніми документами (рис. 13.41).

Дії над ВМД доступні через контекстне меню списку ВМД та головне меню форми (рис. 13.42).

ВМД може бути створена:

- з чистого аркуша;
- копіюванням вибраної раніше створеної ВМД;

Тип	Ре	Особ	Вн. №	Митн.	Рік	Номер	Подано
IM	40	4		100000019	2010	288	27.04.2010 10:31:37
EK	10	287		0	2010	287	17.04.2010 12:31:37
TP	ПП	282		300080003	2010	282	15.04.2010 17:12:56
IM	51	281		0	2010	281	07.04.2010 10:58:18
IM	51	280		0	2010	280	07.04.2010 10:56:51
EK	10	1218		300080001	2010	279	22.03.2010 11:45:09
TP	ПЛГ	58		300000005	2010	277	17.03.2010 10:18:26

Рис. 13.41. Дії над ВМД

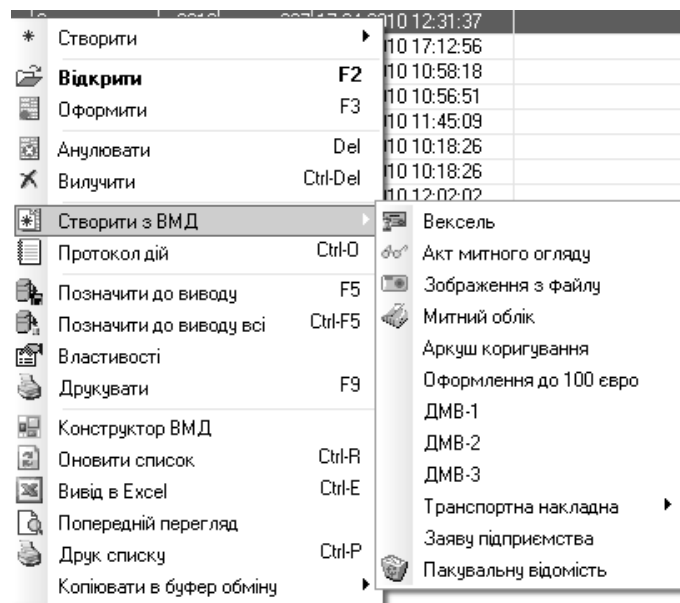


Рис. 13.42. Меню для роботи з ВМД

- через конструктор ВМД шляхом об'єднання інших ВМД або їх розділення на дві чи більше нових ВМД;
- з документів митного обліку.

Тип ВМД обирається при створенні, але може бути змінений у будь-який момент у графі 1.

Вся робота з ВМД відбувається у окремому вікні. Одночасно може бути відкрито декілька вікон ВМД. Інформація у вікні ВМД розділена на логічні розділи — вкладки: Головна, Товар, Інвойс. Крім того, по краях форми знаходяться допоміжні вкладки — Навігатор, Транспортні засоби, Учасники ЗЕД, Доповнення, Друк, Список помилок, Графа В, Список товарів та ін. (рис. 13.43).

Редагування ВМД * - Eugenia

Документ Правка Вигляд Товар Перехід Вікно Допомога

ВМД: 7.968 [24.12.2009] EUR: 11.375117 [24.12.2009]

1

Головна Товар Інвойс

УНІФІКОВАНИЙ АДМІНІСТРАТИВНИЙ ДОКУМЕНТ (УАД)

1. Тип декларації: А. Митний орган відпр./експ./призн.

2. Відправник/експортер: DE

Тестове електронне попереднє повідомлення

Тестове електронне попереднє повідомлення

Регистр №: - /

3. Дод. зрк: 2

4. Відвант спецфрм: 0 / 0

5. Товарів: 3

6. Місць: 282

7. Довідковий номер

8. Одержувач/импортер: UA

Тестове електронне попереднє повідомлення

Тестове електронне попереднє повідомлення

Регистр №: 00 110 00 - 21 / 0000000017

9. Особа, відповідальна за фінансове врегулювання

Регистр №: - /

14. Декларант/представник: UA

Тестове електронне попереднє повідомлення

Тестове електронне попереднє повідомлення

Регистр №: 00 110 00 - 21 / 0032836226

11. Торг. країна

12. Митна вартість

13.

15. Країна відправлення: DE Німеччина

17. Країна призначення

20. Умови поставки

Список помилок

INS

Рис. 13.43. Інформація у вікні ВМД

Для зручності використання раніше створеної інформації товари ВМД можуть бути “перетягнуті” мишкою з навігатора однієї ВМД в іншу. Крім того, існують режими простого і складного пошуку товарів у раніше створених ВМД, звідки вони можуть бути додані в поточну ВМД по одному або разом.

З метою забезпечення ефективної роботи зі створення ВМД з різних інформаційних джерел доступні майстри введення з Excel:

- товарів ВМД (включаючи графи 40, 44 та електронний інвойс);
- транспортних засобів;
- окремо граф 40 та 44.

Введення можливе з будь-яких програмних засобів, що підтримують роботу з таблицями, — Microsoft Office Excel, Microsoft Office Word, Open Office тощо.

Забезпечено також можливість розширеного редагування електронного інвойсу одночасно за всіма товарами в окремому вікні *Редактор інвойсу* (рис. 13.44).

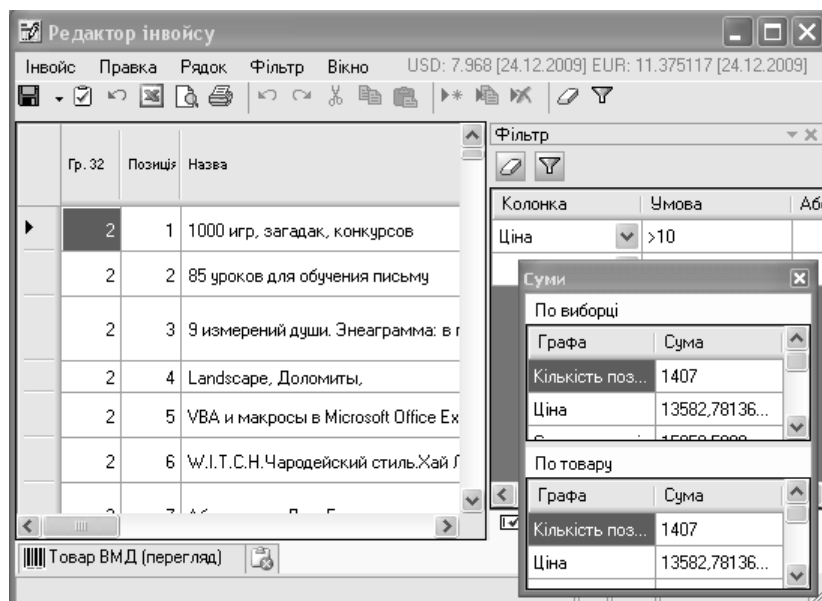


Рис. 13.44. Вікно *Редактор інвойсу*

У цьому вікні доступна фільтрація позицій інвойсу за будь-якими критеріями, отримання сум за товаром та за вибіркою, налагодження колонок, двосторонній обмін даними з Excel в режимі Ctrl-C/Ctrl-V.

Після підготовки ВМД здійснюється її перевірка на наявність помилок. Перевірка ВМД у програмі Diamond Bridge є найбільш повною, максимально наближеною до ПЗ “Інспектор-2006” і здійснюється за понад 950 критеріями (рис. 13.45).

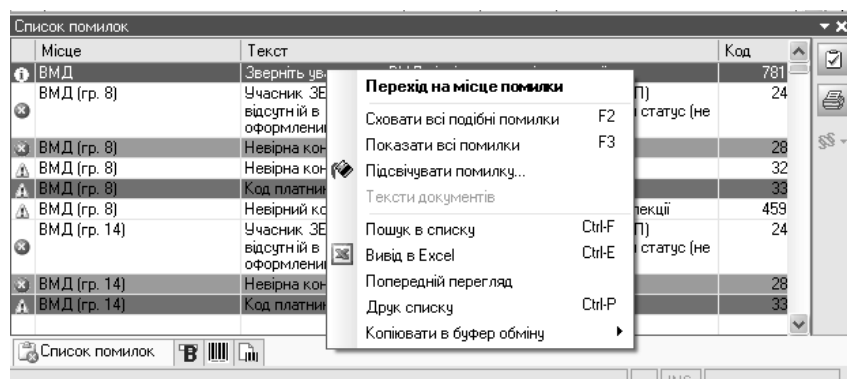


Рис. 13.45. Перевірка ВМД на наявність помилок

У панелі списку помилок зазначаються не тільки суть та місце помилки, а й її рівень. Крім того, користувач має можливість здійснювати додаткову кольорову підсвітку окремих категорій помилок.

Для додаткового опрацювання інформації, що міститься у ВМД, “просунутими” користувачами можуть бути викликані окремі вікна розширеного аналізу:

- тарифу за ВМД;
- нетарифного регулювання;
- країни походження;
- подібних та аналогічних товарів;
- документів графи 44.

Виведення на митницю ВМД та інших документів здійснюється в пакетному режимі: разом з електронною копією ВМД (або електронною ВМД) в одному файлі містяться електронні копії всіх необхідних документів, які на стороні митниці так само пакетом вводяться в базу даних (рис. 13.46).

Тип	Ре	Особ	Вн. №	Митн.	Рік	Кр	Отримув
ВМД	40		271	300000030	2010	UA	ТОВ "Тре
ДМВ	40		270	302000010	2010	UA	СПД-ФО
	40		269	302000010	2010	UA	СПД-ФО
	40		268	302000010	2010	UA	СПД-ФО
	40		267	302000010	2010	UA	СПД-ФО
	40		ййцц	300070010	2009	UA	ТОВ "Він
	40		12	300070010	2010	UA	ТОВ "Він

Рис. 13.46. Виведення на митницю

Перед виведенням користувач ще раз попереджується про наявність у ВМД грубих помилок, через які її не буде прийнято на митниці. При електронному декларуванні електронні документи підписуються електронним цифровим підписом і можуть бути безпосередньо відправлені на поштову скриньку Регіональної інформаційної митниці, через яку здійснюється прийом ЕВМД. При цьому всі вхідні й вихідні підписані ЕЦП електронні повідомлення зберігаються в базі даних і за необхідності можуть бути повторно переглянуті або вивантажені на диск.

13.4.4. Модуль “Митний облік”

Модуль “Митний облік” є інтегрованою підсистемою програми Diamond Bridge. Він призначений для ведення обліку товарів, які розміщені на склад тимчасового зберігання, митні режими тимчасового ввезення/вивезення, митного складу, магазину безмитної торгівлі тощо. Інформація в цьому модулі

може бути створена з ВМД, і навпаки, ВМД можуть створюватися на основі інформації з модуля “Митний облік”. За необхідності здійснюється передача інформації на митницю (рис. 13.47).

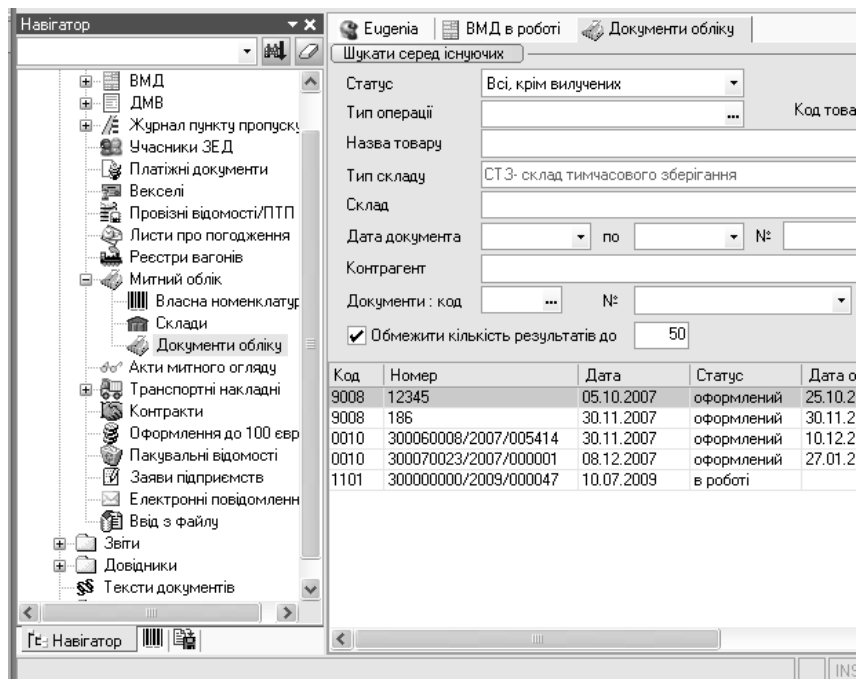


Рис. 13.47. Інформація щодо ВМД з модуля “Митний облік”

Модуль також містить систему звітності, необхідну для всебічного контролю складського обліку, в тому числі звіти про:

- наявність товарів на складі станом на визначену дату;
- прихід за період;
- розхід за період;
- рух товарів за період.

Крім того, наявні спеціалізовані форми звітності, затверджені Держмитслужбою для окремих типів складів.

13.4.5. Звіти програми Diamond Bridge

Програма Diamond Bridge містить систему звітності, необхідну для максимально повного використання інформації, накопиченої декларантами в базі даних (рис. 13.48, 13.49).

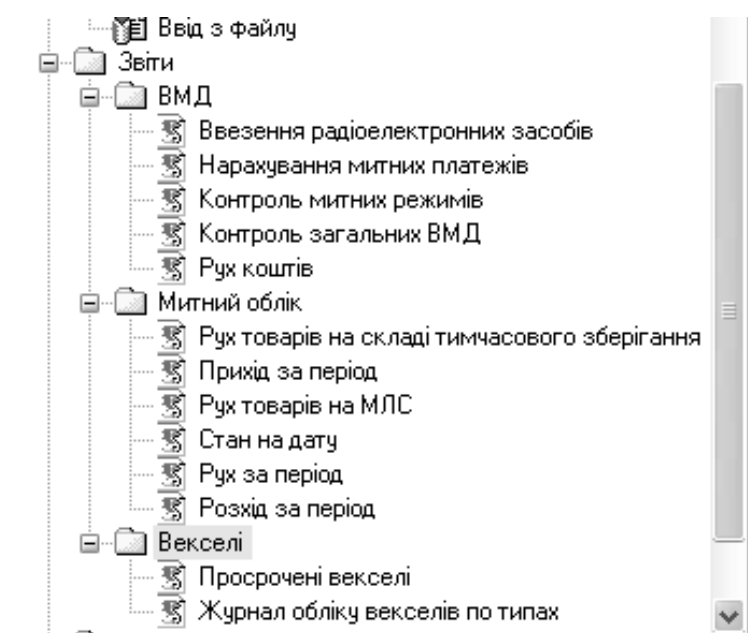


Рис. 13.48. Звіти програми Diamond Bridge

Більшість звітів також містить розшифровку кожної поданої в них суми (рис. 13.50).

Крім того, модуль розширеного пошуку ВМД дає можливість формування вибірок та звітів у широкому діапазоні форматів надання інформації.

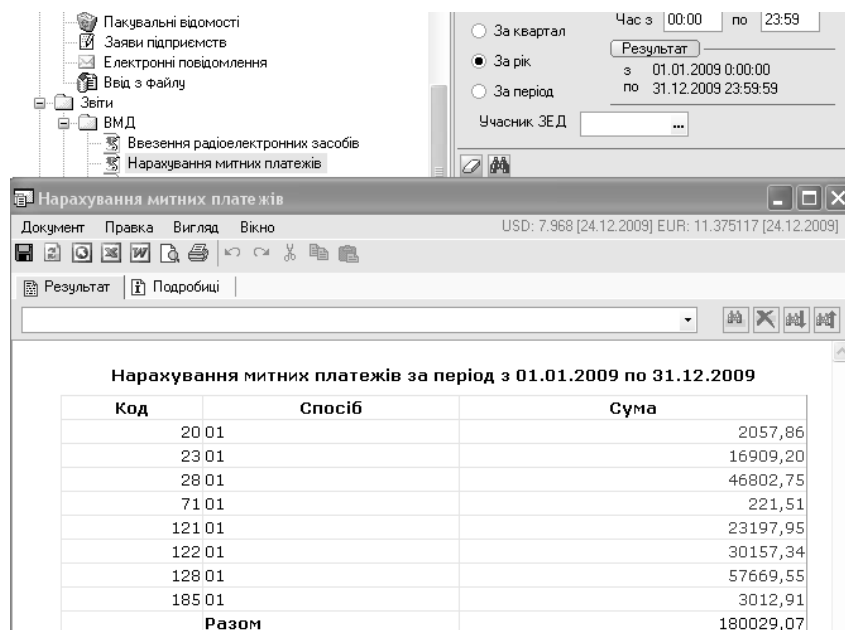


Рис. 13.49. Використання системи звітності за програмою Diamond Bridge

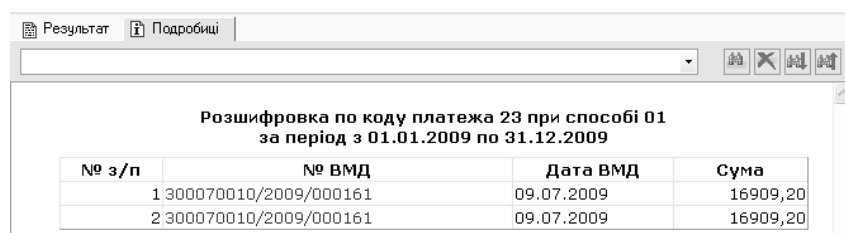


Рис. 13.50. Інформація бази даних

13.4.6. Адміністрування програми Diamond Bridge

Адміністрування програми спрямоване на вирішення таких завдань:

- загальне налагодження системи під вимоги конкретної митниці та запити користувачів;
- розмежування прав користувачів на окремі модулі та дії;
- сервіс бази даних (створення резервних копій, відновлення індексів тощо). Такі адміністративні завдання можуть також виконуватися в автоматичному режимі;
- налагодження прийняття/передачі інформації, в тому числі з використанням ЕЦП;
- ведення довідників регулярної інформації, що використовується при заповненні документів;
- створення власних додаткових правил перевірки ВМД;
- введення поновлень програми (можливе також в автоматичному режимі).

Отже, програмне забезпечення Diamond Bridge є найсучаснішим з технологічного погляду інформаційно-технічним рішенням для автоматизації роботи декларантів та ведення зовнішньоекономічної діяльності, а з погляду користувача — найбільш повним засобом задоволення найвибагливіших його потреб. Можна сказати, що це перше програмне забезпечення, яке дозволяє зробити те, чого хоче декларант, так, як це вимагає митниця і диктують вимоги сучасного електронного світу.

Запитання і завдання для самоконтролю

1. Розкрийте поняття електронного декларування.
2. Яку роль відіграють інформаційні технології у митній справі відповідно до Міжнародної конвенції про спрощення та гармонізацію митних процедур (Кіотська конвенція, 1999 р.)?

3. Який порядок виконання процедури електронного декларування?
4. Назвіть особливості призначення програмно-інформаційного комплексу “Інспектор-2006”.
5. Які особливості призначення пакета MD Office?
6. Назвіть складники пакета MD Office.
7. Розкрийте можливості MD Declaration.
8. Які види довідників використовуються в пакеті MD Office?
9. Яке призначення пакета QD Professional?
10. Назвіть функціональні можливості пакета QD Professional.
11. Яка структура додатків пакета QD Professional?
12. Назвіть можливості системи QD Pro-документи.
13. Які критерії пошуку документів та особливості роботи з ними?
14. У чому полягає робота з довідковою системою пакета QD Professional?
15. Яке призначення та функціональні можливості QD Pro-декларація?
16. Опишіть роботу з текстами документів у програмі Diamond Bridge.
17. Опишіть роботу з класифікаторами в програмі Diamond Bridge.
18. Опишіть роботу з ВМД в програмі Diamond Bridge.
19. Опишіть роботу з модулем “Митний облік” у програмі Diamond Bridge.
20. У чому полягає технологічна інноваційність програми Diamond Bridge? Які можливості відкривають ці нові технології?
21. Які переваги й недоліки програми Diamond Bridge порівняно з іншими програмними продуктами?

Розділ 14

СТВОРЕННЯ ЕЛЕКТРОННОЇ МИТНИЦІ — ГОЛОВНИЙ НАПРЯМ ПОДАЛЬШОГО РОЗВИТКУ ЄАІС ДМСУ

14.1. Концепція створення Електронної митниці

Тенденції світового розвитку встановлюють нові завдання зі спрощення митних процедур та процедур логістики при поставчанні товарів для ввезення та вивезення з території країни, зменшення ризиків порушення безпеки мешканців, для чого необхідно створювати електронні інформаційні системи, які будуть функціонально сумісні з аналогічними системами різних країн, будуть доступні, керовані, безпечні, об'єднані та контрольовані.

Європейська спільнота визначає, що шлях до цього — зменшення відмінностей між митними процедурами країн світу, та називає механізм реалізації такого завдання “Електронною митницею”. Держави — члени ЄС прийняли рішення діяти в рамках структури “Електронної Європи” та затвердили Рішення Ради Європейського Союзу щодо простого та безпаперового середовища для митних адміністрацій та суб'єктів зовнішньоекономічної діяльності.

Аналогічні завдання під час втілення новітніх технологій у митну справу ставлять митні адміністрації багатьох країн СНД, Азії та Америки. Вони відрізняються лише за строками реалізації та окремими деталями. Тому “Електронна митниця”

— це не тільки утворення декількох країн. Це — майбутнє митної спільноти світу.

Україна поетапно просувається до створення сучасної власної інформаційної системи. Постановою Кабінету Міністрів України від 24 лютого 2003 р. № 208 встановлено, що одним з пріоритетних завдань розвитку інформаційного суспільства є надання громадянам і юридичним особам інформаційних та інших послуг шляхом використання електронної інформаційної системи “Електронний Уряд”, яка забезпечує інформаційну взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій.

Закон України “Про електронні документи та електронний документообіг” встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів.

Сьогодні створено всі передумови для формування і розвитку інформаційного суспільства в Україні. Розроблена законодавча база, успішно розвиваються інформаційно-телекомунікаційні технології, зростає парк сучасних засобів обчислювальної техніки. Цей процес має глобальний характер, немислиме входження і нашої країни до світової інформаційної спільноти.

До характерних рис і ознак інформаційного суспільства належать:

- формування єдиного інформаційно-телекомунікаційного простору України як частини світового інформаційного простору;

- повноправна участь України в процесах інформаційної і економічної інтеграції світової спільноти;

- становлення і в подальшому домінування в економіці нових технологічних принципів, що базуються на масовому використанні сучасних інформаційних технологій, засобів обчислювальної техніки і телекомунікацій;

- створення і розвиток ринку інформації і знань як чинників виробництва на додаток до ринків природних ресурсів, праці і капіталу, фактичне задоволення потреб суспільства в інформаційних продуктах і послугах;

- зростання ролі інформаційно-телекомунікаційної інфраструктури у системі суспільного виробництва;
- підвищення рівня освіти, науково-технічного і культурного розвитку за рахунок розширення можливостей систем інформаційного обміну на міжнародному, національному і регіональному рівнях;
- створення ефективної системи забезпечення прав громадян і соціальних інститутів на вільне отримання, розповсюдження і використання інформації як найважливішої умови демократичного розвитку.

Роль інформаційних технологій у митній справі відображена в Міжнародній конвенції про спрощення і гармонізацію митних процедур (Киотська конвенція, 1999 р.), яка:

- передбачає максимальне практичне використання інформаційних технологій;
- розглядає інформаційні технології як один з принципів митного оформлення, реалізація якого повинна сприяти спрощенню і гармонізації митних процедур;
- встановлює стандартні правила використання інформаційних технологій для вдосконалення митного контролю.

Митна служба України як один з основних інститутів держави бере участь у формуванні і розвитку інформаційного суспільства, розпочавши втілення новітніх технологій у митну справу ще в 1992 р. У 2005 р. почався новий етап цієї роботи з розробки принципів побудови системи “Електронна митниця” та її часткової реалізації.

Враховуючи провідну роль митниці в зовнішньоекономічній діяльності, інформаційна складова діяльності митної служби повинна бути домінуючою.

Наріжним каменем, на якому базується вищенаведена система, є “Електронна митниця”, складовими якої повинні бути такі підсистеми: електронне декларування; електронний документообіг; аналіз ризиків і керування ними; контроль за транзитом; єдина міжвідомча автоматизована система збору, збереження й обробки інформації, у тому числі від різних відомств; автоматизоване здійснення усіх видів державного контролю; уніфікована база нормативних і довідкових документів, які використовуються в митних цілях; інформаційне забезпечен-

ня постаудиту та правоохоронної діяльності. Отже, замість придатка до митних процедур вона повинна стати ядром, стрижнем не тільки митних технологій, а ще й інструментом керування та контролю митної діяльності, тобто головним механізмом забезпечення митної справи.

У рішеннях Європейського Союзу “Електронна митниця” є базою для створення “єдиного вікна”, яке зобов’язані використовувати інші відомства, що задіяні у митній справі. Тому і на митні органи України повинні бути покладені додаткові обов’язки з координації дій міністерств та відомств у цьому напрямі, затвердження яких має бути закріплене відповідними рішеннями уряду.

Об’єднувальний стрижень митної служби — це інформаційні механізми, які є запорукою посилення авторитету та могутності митниці. Інші шляхи — це крок назад.

Такий підхід потребує змін на рівні не тільки інформаційних підрозділів, а й управлінської ланки центрального апарату Держмитслужби України.

Митна безпека держави визначається як стан захищеності національних інтересів, забезпечення та реалізація яких покладені на митні адміністрації країни, що дає можливість незалежно від будь-яких зовнішніх і внутрішніх загроз забезпечити здійснення митної справи. Тоді базою для оцінки митної безпеки України може стати оцінка якості виконання митної справи, яка, у свою чергу, визначається розрахунково-програмними способами через організаційно-технічні системи в рамках “Електронної митниці”.

Враховуючи завдання, покладені Президентом і Урядом України на митну службу, які спрямовані на наближення митних правил України до світових норм і стандартів, Держмитслужбою України розроблено Концепцію створення системи “Електронна митниця”.

Метою Концепції є визначення стратегії створення багатофункціональної комплексної системи “Електронна митниця” (далі — Електронна митниця) на базі Єдиної автоматизованої інформаційної системи (далі — ЄАІС) ДМСУ як одного з механізмів забезпечення митної безпеки України.

Концепція передбачає визначення принципів побудови Електронної митниці, основних положень з формування її інформаційно-телекомунікаційного забезпечення, етапів впровадження, а також створення передумов для інтеграції України у світову інформаційну спільноту.

Концепція ґрунтується на вимогах Конституції України, законодавства України, міжнародних митних конвенцій та враховує досвід інших країн.

14.2. Обґрунтування та мета створення Електронної митниці

Істотне збільшення рівня прозорості та підзвітності операційної діяльності органів державної влади можливе тільки за умови електронізації в процесі адміністративного реінжинірингу базових інститутів державного адміністрування (тобто при переході до інтенсивного використання інформаційно-телекомунікаційних технологій у їх діяльності). До таких інститутів належать державний (нефінансовий) облік, розкриття інформації держави для громадян, внутрішній і зовнішній інформаційний контроль, незалежний аудит інформаційних систем, інструменти державного управління, управління адміністративними процесами, проектами та програмами, управління адміністративним персоналом тощо.

Дуже коротко “Електронний уряд” (ЕУ) можна охарактеризувати як “інформаційну взаємодію органів державної влади і суспільства з використанням інформаційно-телекомунікаційних технологій”. У моделі ЕУ виділяються чотири чітко виражені сфери відносин: між державними службами і громадянами (G2C — government — to — citizen), державою і приватними компаніями (G2B — government — to — business), державними організаціями та їх співробітниками (G2E — government — to — employee) і, нарешті, між різними державними органами і рівнями державного управління (G2G — government — to — government).

За наявності інститутів ЕУ чиновник буде менше зв'язаний регламентами, вільний у виборі відповідних засобів для виконання своїх обов'язків на благо громадян.

Отже, ЕУ має такі основні цілі:

- оптимізація надання урядових послуг населенню і бізнесу;
- підвищення ступеня участі всіх виборців у процесах керівництва і управління країною;
- підтримка і розширення можливостей самообслуговування громадян;
- зростання технологічної обізнаності і кваліфікації громадян;
- зниження дії чинника географічного місцезнаходження.

Створення Електронної митниці, спрямоване на зміцнення митної безпеки України, забезпечить оперативне отримання актуальної і достовірної інформації про наміри щодо здійснення зовнішньоекономічних операцій, створення умов для прискорення процедур митного контролю та митного оформлення, поліпшення соціального й інформаційного обслуговування населення, сприятиме вдосконаленню інформаційної інфраструктури ДМСУ.

Проектування і впровадження Електронної митниці повинні здійснюватися на базі діючої ЄАІС з урахуванням міжнародних стандартів і з максимальним використанням науково-технічного потенціалу держави.

Враховуючи необхідність спрощення процедури митного оформлення та митного контролю товарів і транспортних засобів, а також загальносвітові тенденції щодо поступового переходу до уніфікації оформлення вантажних митних декларацій та їх контролю, передбачається створення та використання виключно машинозчитуваних документів, для чого повинні застосовуватися відповідні програмно-апаратні засоби.

Відкритість і багаторівнева структура Електронної митниці мають забезпечувати можливість розширення її взаємодії із зовнішніми користувачами — центральними органами виконавчої влади, органами місцевого самоврядування, підприємствами, установами та організаціями на будь-якому рівні системи і в будь-який час.

При цьому слід урахувати особливості державного управління, серед яких основними з погляду впливу на структуру Електронної митниці, є:

- неоднорідність інформації, що зберігається у базах даних;
- наявність у базах даних розподіленої інформації;
- наявність великої кількості інформаційних потоків, різних за структурою та інтенсивністю;
- велика кількість внутрішніх та зовнішніх користувачів;
- різні вимоги щодо захисту інформації та програмно-апаратного забезпечення.

Електронна митниця як інформаційно-аналітична система загальнодержавного значення повинна стати моніторинговою підтримкою у формуванні організаційного механізму забезпечення управління у митній справі, відстеження динаміки співвідношень експортного та імпортного потенціалу країни тощо.

Ведення довідкових систем і формування баз даних спеціального призначення повинні забезпечити можливість організації інформаційного обслуговування різноманітних запитів користувачів Електронної митниці, що потребують аналізу й узагальнення, як на державному, так і на регіональному рівнях. Цьому має сприяти створення інтегрованих баз даних центрального і регіонального рівнів, де будуть концентруватися інформаційні ресурси Електронної митниці.

Електронна митниця забезпечуватиме задоволення потреб юридичних та фізичних осіб, як резидентів, так і нерезидентів України, у своєчасному оформленні документів, які подаються до митного оформлення, та верифікацію внесених даних, а також буде використовуватися в системі управління митною справою.

Електронна митниця повинна функціонувати в режимі реального часу, бути доступною кожному авторизованому користувачеві та орієнтуватися на використання визнаних міжнародних форматів документів, що подаються до оформлення в електронному вигляді.

Держави — члени ЄС протягом 2005—2006 рр. прийняли рішення діяти в рамках структури “Електронної Європи” та

затвердили Рішення Ради щодо простого та безпаперового середовища для митниці та торгівлі.

ЄС розробив Багаторічний стратегічний план упровадження “Електронної митниці”, яким пропонується:

- об’єднати наявні системи контролю за експортом, імпортом та транзитом в єдину систему;
- увести систему єдиного обліку суб’єктів ЗЕД з реєстрацією тільки в одній державі;
- надати суб’єктам ЗЕД можливість використання місць єдиного електронного доступу для оформлення зовнішньоекономічних операцій;
- проводити усі фактичні перевірки товару в один час і в одному місці;
- забезпечити обмін електронною інформацією між усіма органами та суб’єктами, задіяними в зовнішньоекономічних операціях (у тому числі з трьома країнами). Митниця буде діяти для цих органів та агентів як “єдине вікно”;
- відбір товарів для митного огляду на прикордонних та внутрішніх пунктах митного оформлення (ПМО) проводити на основі автоматизованого аналізу ризиків;
- збір, повернення, звільнення від платежів здійснювати вповноваженим суб’єктом у місці, де він зареєстрований і де містяться його документи;
- збір, повернення, звільнення від платежів здійснювати вповноваженим суб’єктом у митному органі за його вибором;
- запровадити безпаперове середовище для митниці та торгівлі, подання митної декларації в електронному вигляді зі свого місця розташування незалежно від країни відправлення або ввезення товарів;
- проводити електронний обмін інформацією між митними пунктами пропуску на території усього ЄС, де вона необхідна для митних процедур.

Цей план розрахований на впровадження до 2013 р.

Для реалізації в Україні такого плану, головною метою якого є використання інформаційних технологій замість паперових, необхідно внести зміни до Митного кодексу та інших нормативно-правових актів.

Основною метою створення Електронної митниці є:

- технологічне забезпечення безперервного потоку, накопичення та обробка електронної інформації між митними адміністраціями держав, органами державної влади України та суб'єктами зовнішньоекономічної діяльності;
- створення та технічна підтримка організаційно-технічних систем для функціонування всеохоплюючих автоматизованих процедур оцінки якості виконання митної справи;
- підвищення ефективності митного контролю та митного оформлення шляхом формування єдиної державної автоматизованої системи митного контролю та митного оформлення на підставі відомостей, що подаються до митних органів юридичними та фізичними особами виключно в електронному вигляді;
- створення режиму “єдиного вікна”;
- забезпечення органів державної влади, інших державних органів та органів місцевого самоврядування актуальною і достовірною статистичною інформацією;
- підвищення ефективності управління ДМСУ та взаємодії з органами державної влади;
- виключення дублювання заходів з ведення обліку окремих операцій, що здійснюються органами виконавчої влади, органами місцевого самоврядування, іншими організаціями, з метою раціонального використання бюджетних коштів;
- участь у формуванні державних інформаційних ресурсів;
- спрощення порядку звернення юридичної та/або фізичної особи до митних органів і отримання інформації, що їх стосується;
- зменшення кількості адміністративних зобов'язань;
- підвищення ефективності боротьби з контрабандою, шахрайством, організованою злочинністю і тероризмом;
- забезпечення повноти сплати податків та зборів;
- захист інтелектуальної власності та культурної спадщини;
- підвищення контролю за ввезенням небезпечних вантажів;
- забезпечення обміну інформацією з митними службами закордонних держав;
- забезпечення контролю за додержанням передбачених законом заборон та обмежень щодо переміщення окремих товарів через митний кордон України.

14.3. Основні завдання, які вирішує Електронна митниця

Основними завданнями Електронної митниці є:

- автоматизація процесів митного контролю та митного оформлення товарів, предметів і транспортних засобів, що переміщуються через митний кордон України;
- забезпечення функціонування системи електронного документообігу;
- забезпечення функціонування системи аналізу ризиків;
- сприяння захисту прав інтелектуальної власності в процесі зовнішньоекономічної діяльності шляхом ведення відповідних автоматизованих систем;
- забезпечення інформаційної взаємодії митної служби України з правоохоронними органами та іншими органами державної влади України в межах двосторонніх угод або спільних наказів про обмін інформацією;
- формування банку даних Електронної митниці;
- забезпечення інформаційної безпеки під час формування і функціонування банку даних Електронної митниці;
- накопичення інформації в результаті проведення митного контролю та митного оформлення товарів, предметів і транспортних засобів, що переміщуються через митний кордон України;
- забезпечення інформаційної взаємодії та співпраці відповідно до укладених Україною міжнародних договорів;
- проведення єдиної науково-технічної політики під час створення Електронної митниці.

Електронна митниця як автоматизована система обліку зовнішньоекономічних операцій юридичних та фізичних осіб повинна забезпечувати виконання таких функцій:

- накопичення інформації про зовнішньоекономічні операції юридичних та фізичних осіб у відповідних базах даних (на центральному та регіональному рівнях);
- взаємодія з іншими зовнішніми інформаційними системами;

- уведення інформації про можливу зовнішньоекономічну операцію юридичної або фізичної особи безпосередньо з первинних документів, включаючи їх відцифрований образ;
- хронологічне накопичення інформації про зовнішньоекономічні операції юридичних та фізичних осіб;
- формування аналітичних звітів про експортно-імпортні операції країни;
- дотримання необхідного рівня технічного захисту інформації.

Власником Електронної митниці є ДМСУ, яка володіє, користується і розпоряджається основними структурними компонентами Електронної митниці, необхідними для забезпечення її функціонування.

Власник Електронної митниці:

- реалізує державну політику з питань реєстрації, ідентифікації та обліку зовнішньоекономічних операцій юридичних та фізичних осіб, забезпечує оформлення та видачу відповідних документів Електронної митниці;
- здійснює керівництво та контроль за роботами, пов'язаними зі створенням, веденням і забезпеченням функціонування Електронної митниці;
- визначає організаційні та методичні засади ведення Електронної митниці.

Уповноваженою особою Власника Електронної митниці для виконання робіт із створення, ведення і забезпечення функціонування Електронної митниці є Регіональна інформаційна митниця (далі — РІМ).

14.4. Напрями створення Електронної митниці

Основні напрями створення Електронної митниці як подальшого інформаційно-технічного розвитку ЄАІС ДМСУ такі.

1. *У сфері розвитку системи технічних та програмних комплексів автоматизації технологічних процедур митного контролю та митного оформлення:*

- вдосконалення системи автоматизованого контролю за переміщенням товарів і транспортних засобів відповідно до заявлених митних режимів;

- розвиток та вдосконалення процесів автоматизації митного оформлення товарів, транспортних засобів та громадян;

- розвиток та вдосконалення процесів автоматизації митного оформлення товарів, транспортних засобів, що переміщуються через митний кордон України;

- подальша автоматизація процесів митного контролю;

- вдосконалення системи аналізу ризиків та її інтеграція з автоматизованими системами митного оформлення;

- вдосконалення системи обліку учасників ЗЕД в напрямі її взаємодії з інформаційними системами органів державної влади України;

- створення автоматизованої системи адміністрування митних платежів як складової АСМО;

- вдосконалення автоматизації процесів виявлення та обліку порушень митних правил;

- розробка автоматизованої системи формування, збору, обробки та накопичення інформації для формування митної статистики (показники діяльності митних органів);

- створення автоматизованої системи застосування передбачених законом заборон та обмежень щодо переміщення окремих товарів через митний кордон України.

2. У сфері розвитку системи електронного документообігу:

- впровадження електронного цифрового підпису для усіх працівників митних органів;

- ведення та постійне оновлення Рубрикатора нормативних документів;

- створення електронної бібліотеки Митної служби України;

- побудова системи електронного документообігу та електронного декларування на базі системи ІТК “Електронна пошта”;

- поетапне впровадження системи електронного документообігу в ДМСУ, інтегрованої в систему електронного документообігу органів державної влади.

3. У сфері накопичення та адміністрування відомчих інформаційних ресурсів:

- модернізація архітектури ЄАІС та баз даних в напрямі забезпечення відмовостійкості (створення резервного інформа-

ційного центру), цілісності, несуперечності, достовірності, актуальності та доступності інформації;

- розробка єдиної інформаційної моделі ЄАІС ДМСУ з використанням механізмів системної інтеграції об'єктів інформаційно-технічної інфраструктури;

- модернізація та вдосконалення механізмів доступу до інформаційних ресурсів органів державної влади України;

- зміна системи накопичення статистичних показників та формування БД статистичних показників ;

- розвиток та вдосконалення функціональних підсистем ЄАІС для автоматизації діяльності структурних підрозділів ДМСУ.

4. У сфері телекомунікацій:

- організація каналів зв'язку між центральними офісами митних органів та їх віддаленими підрозділами шляхом подальшої розбудови ВТМ на базі сучасних технологій передачі даних на засадах отримання послуг у телекомунікаційних операторів України;

- організація міжнародних каналів зв'язку для реалізації угод з інформаційного обміну на базі сучасних технологій передачі даних на засадах отримання послуг у телекомунікаційних операторів;

- створення системи відомчого телефонного зв'язку та системи передачі відеозображення у складі ВТМ на базі сучасних технологічних рішень;

- модернізація та оснащення митних органів сучасними обчислювальними мережами, засобами обробки та передачі інформації.

5. У сфері розвитку систем захисту інформації:

- побудова комплексної системи захисту інформації (в подальшому — КСЗІ) шляхом упровадження типових рішень КСЗІ на різних рівнях обробки та збереження інформації на об'єктах інформаційної діяльності;

- організація та проведення атестації об'єктів інформаційної діяльності митних органів відповідно до вимог законодавства у сфері захисту інформації.

14.5. Принципи побудови багатофункціональної комплексної системи “Електронна митниця”

Принципами побудови Електронної митниці є:

- законність;
- достовірність, цілісність та доступність інформації;
- єдність форматів даних, технічних і технологічних параметрів;
- уніфікованість документів;
- багаторівневість зберігання та доступу до інформації.

Електронна митниця повинна функціонувати в єдиному інформаційному середовищі зі ступеневою системою обробки інформації та доступу до неї.

За основу створення Електронної митниці слід брати структурний принцип побудови, що забезпечує модульну організацію і поетапне нарощування її функціональних можливостей. Це допоможе сконцентрувати технічні та фінансові ресурси ЄАІС на розв’язанні завдань поетапного переходу від діючого механізму подання документів (вантажної митної декларації) до митного оформлення до механізму електронного декларування і одночасно започаткувати проектування, створення і впровадження програмно-технічних комплексів для автоматизації обробки всіх типів документів, які повинні надаватися як суб’єктом ЗЕД, так і іншими органами виконавчої влади виключно в електронному вигляді.

Основою Електронної митниці є інтегрована база даних та телекомунікаційне середовище.

Інтегрована база даних Електронної митниці формується на базі центральної бази даних ДМСУ, центрів обробки даних митних органів.

Передбачається функціонування резервного комплексу збереження та обробки даних, який з міркувань безпеки повинен бути територіально віддаленим від інтегрованої бази даних, розміщеної в приміщенні РІМ.

Відповідно до організаційних та економічних умов створення, а також враховуючи необхідність гарантування безпеки інформації, Електронна митниця повинна формуватися відповідно до таких засад:

- забезпечення повного циклу збирання, обробки, відображення, реєстрації, зберігання та розподілу інформації;
- використання обладнання з високою надійністю, реалізація принципу розподілених обчислень для підвищення надійності Електронної митниці;
- оперативність забезпечення зовнішніх користувачів Електронної митниці необхідною інформацією, надання її в зручному для сприйняття вигляді, надання допомоги в проведенні аналізу та виробленні можливих варіантів рішень з використанням сучасних інтерфейсів і процедур прийняття рішень;
- відповідність технологічного обладнання, що використовується в Електронній митниці, державним та міжнародним стандартам;
- єдність загальнодержавного і відомчих інформаційних просторів, захист національного інформаційного ресурсу під час забезпечення взаємодії із зовнішніми інформаційно-аналітичними системами.

Програмно-технічний комплекс Електронної митниці повинен базуватися на проектних рішеннях, які опрацьовано під час створення ЄАІС ДМСУ:

- робота з великими обсягами даних;
- підвищена стійкість до відмов, резервування даних, відновлення даних у разі їх руйнування;
- підтримання гетерогенного середовища даних;
- захист інформації як на рівні доступу до баз даних, так і під час її циркуляції в мережах;
- підтримання одночасної роботи з інформацією різних категорій;
- підтримання цілісності баз даних;
- спільна обробка та зберігання різних типів даних;

— формування інформації державною мовою, латинськими літерами для транслітерації українського алфавіту, відповідних форматів дат.

Уведення в дію Електронної митниці повинне передбачати максимальне використання програмно-апаратних комплексів вузлів ЄАІС ДМСУ.

Це суттєво зменшить витрати та прискорить процес уведення в дію Електронної митниці, дасть змогу поетапно оптимізувати програмно-апаратний комплекс як за продуктивністю об'єднання, так і за його вартістю.

14.6. Структура та інфраструктура Електронної митниці

В основу проектування і формування Електронної митниці повинні закладатися системотехнічні принципи, що були основою під час створення ЄАІС Держмитслужби України, у тому числі мережева архітектура, відкритість, системне управління тощо.

Застосування сучасних технологій обробки інформації з потужним програмно-апаратним комплексом Регіональної інформаційної митниці надає широкі можливості для вибору оптимальних технологій обробки даних для кожного типу документів Електронної митниці, спрощення технологічних схем обробки даних.

При цьому забезпечується принципова можливість спільного функціонування програмно-технічних компонентів, розроблених самостійно співробітниками митних органів та офіційно придбаних у різних виробників.

Важливими умовами існування Електронної митниці повинні бути ліцензійна чистота програмних і технічних засобів, їх відповідність нормам і вимогам технічного захисту інформації, уніфікація протоколів обміну інформацією.

Структура Електронної митниці повинна забезпечувати централізований моніторинг і управління центральною та резервною базами даних ДМСУ, вузлами ВТМ, серверами, робо-

чими станціями, програмно-технічними комплексами, телекомунікаційним обладнанням, а також взаємодію із зовнішніми системами.

Функціонально Електронна митниця складається з окремих підсистем, які працюватимуть на різних рівнях і взаємодіятимуть.

Передбачається поступове введення в експлуатацію та подальший розвиток цих підсистем.

Підсистема електронного декларування та електронного документообігу

Підсистема електронного декларування та електронного документообігу — це сукупність програмно-апаратних засобів та інформаційно-телекомунікаційних комплексів, що забезпечує взаємодію підсистем декларанта (брокера) і митного органа, а також співробітників різних митних органів під час здійснення процедур митного контролю та митного оформлення вантажів.

Головними перевагами електронного декларування є прискорення митних процедур, підвищення вірогідності відомостей, заявлених у декларації, і усунення “людського фактора”, тобто зведення до мінімуму безпосередніх контактів посадових осіб митних органів і учасників ЗЕД.

Підсистема аналізу ризиків і керування ними

Підсистема аналізу ризиків і керування ними становить комплекс програмних засобів, які дають можливість в автоматичному режимі аналізувати інформацію, яка надходить в електронній копії вантажної митної декларації, що, у свою чергу, допоможе підвищити ефективність митного контролю й одночасно реалізувати принцип вибіркової у цій сфері.

Підсистема контролю за транзитом

Підсистема контролю за транзитом повинна забезпечувати можливість в автоматичному режимі отримувати та передавати інформацію про транзитні вантажі до нової комп’ютерної транзитної системи (NCTS), яка використовується в усіх країнах — членах Європейського Союзу, тобто забезпечувати організацію сумісності діючої (вдосконаленої) в митних органах України системи щодо контролю за переміщенням вантажів із загальноєвропейською системою.

Єдина міжвідомча автоматизована система збору, збереження й обробки інформації

Комплексний аналіз інформації повинен забезпечувати Операційний центр, головне завдання якого — безперервний моніторинг усієї інформації, що надходить, її аналіз з використанням системи керування ризиками й оперативне керування митними органами ДМСУ.

Збір і аналіз повинні здійснюватись від обробки попередньої інформації до результатів постконтролю протягом усього переміщення товарів.

З метою забезпечення цілісності даних, оперативності надання користувачам Електронної митниці необхідної довідкової інформації повинне забезпечуватися ведення бази даних нормативно-довідкової інформації. Нормативно-довідкова інформація має надаватися центральними органами виконавчої влади та установами, які згідно з відповідними нормативними актами відповідальні за її підтримання в актуальному стані.

14.7. Інформаційна безпека Електронної митниці

Інформаційна безпека Електронної митниці повинна забезпечуватися шляхом створення Комплексної системи захисту інформації (далі — КСЗІ), яка включає програмно-технічні засоби підсистеми захисту інформації, та шляхом здійснення інженерно-технічних, правових та організаційних заходів.

Метою створення КСЗІ ЄАІС Держмитслужби України є реалізація єдиної політики інформаційної безпеки в Держмитслужбі України, що дасть змогу здійснювати автоматизовану обробку інформації з обмеженим доступом в Держмитслужбі України відповідно до нормативних і законодавчих актів України в галузі захисту інформації.

Наявність спільних технічних рішень щодо реалізації складових ЄАІС Держмитслужби України визначає необхідність використання спільних рішень щодо захисту інформації та створення єдиної для інформаційно-телекомунікаційної систе-

ми КСЗІ. Впровадження єдиної КСЗІ дає можливість забезпечити реалізацію єдиної політики безпеки інформації в інформаційно-телекомунікаційній системі Держмитслужби України та спадкоємність рішень щодо захисту інформації, які будуть розроблятися надалі.

КСЗІ ЄАІС Держмитслужби України повинна будуватись за модульним принципом.

Поділ КСЗІ ЄАІС Держмитслужби України на модулі забезпечує:

- розробку і впровадження спільних для інформаційних систем модулів КСЗІ та їх використання для усіх інформаційних систем, що входять до складу інформаційно-телекомунікаційної системи;
- мінімізацію витрат та часу в процесі упровадження захисту інформації в інформаційних системах, які існують та будуть створюватись в подальшому, шляхом розробки (за необхідності) лише окремого модуля, що враховує особливості конкретної інформаційної системи;
- достатність заходів і засобів захисту та виключає їх надлишковість;
- можливість модернізації без припинення функціонування ЄАІС.

Вибір заходів і засобів захисту кожного модуля повинен здійснюватись відповідно до єдиної політики безпеки інформації в ІТС, чим забезпечуватиметься їх узгоджена взаємодія.

Сукупність модулів КСЗІ ЄАІС на окремому об'єкті інформаційної діяльності утворює компонент КСЗІ, що забезпечує можливість проведення державної експертизи у сфері захисту інформації згідно з діючими нормативними документами у сфері захисту інформації.

До КСЗІ як централізованої системи управління інформаційною безпекою ЕМ належать модулі КСЗІ:

- телекомунікаційної системи (локальні обчислювальні мережі, відомча телекомунікаційна мережа тощо);

- автоматизованого робочого місця;
- загального прикладного програмного забезпечення;
- Основного комплексу ЄАІС Держмитслужби України;
- Резервного комплексу ЄАІС Держмитслужби України;
- інформаційної системи n ;
- інформаційної системи $n+1$.

Інформаційна безпека під час використання ЄАІС Держмитслужби

Організаційні заходи — це сукупність процесів чи дій, що ведуть до утворення й удосконалення взаємозв'язків між окремими частинами єдиного об'єкта. Одним з важливих напрямів організаційних заходів є чітка організація системи діловодства і документообігу.

Багатогранність сфери організаційного захисту інформації вимагає створення спеціального відділу безпеки, що забезпечує і направляє реалізацію всіх організаційних заходів. Його штатна структура, чисельність і склад визначаються реальними потребами Держмитслужби України, ступенем конфіденційності циркулюючої інформації і загальним станом безпеки.

Метою створення підрозділу захисту інформації Держмитслужби України є організаційне забезпечення завдань керування КСЗІ в ЄАІС та здійснення контролю за її функціонуванням.

Політика інформаційної безпеки (ІБ) Держмитслужби України

Політика ІБ Держмитслужби України є головним зведенням правил, рекомендацій, положень, інструкцій, актів та наказів Держмитслужби України, які регламентують порядок дотримання інформаційної безпеки під час використання та обробки засобами ЄАІС інформації, що потребує захисту.

Політика інформаційної безпеки ДМСУ спрямована:

- на забезпечення рівня інформаційної безпеки в ЄАІС Державної митної служби України, що відповідає нормативно-правовим актам у цій сфері;
- обґрунтування доцільності вибору заходів захисту інформації;
- розробку регламенту створення, придбання, застосування сертифікованих програмно-апаратних засобів забезпечення технологічних процесів Держмитслужби України;

- забезпечення інформаційної безпеки в кожному з об'єктів інформаційної діяльності Держмитслужби України;
- розроблення планів реагування та відновлення післяаварійних ситуацій для усіх функціональних галузей з метою забезпечення безперервності роботи;
- забезпечення відповідності КСЗІ нормативно-правовим актам у сфері захисту інформації, що має бути прийнято та затверджено в установленому законодавством порядку.

Рівні інформаційної безпеки

До політики інформаційної безпеки *вищого рівня* належать положення, які стосуються питань забезпечення захисту інформації в ЄАІС Держмитслужби України в цілому та вирішення питань, що визначають стратегічні рішення та напрями розвитку інформаційної безпеки.

До *середнього рівня* політики інформаційної безпеки зараховують питання, що визначають загальний порядок поводження з інформаційними, програмними та технічними ресурсами і є важливими для різних автоматизованих систем, що входять до складу ЄАІС Держмитслужби України.

До *нижчого рівня* політики інформаційної безпеки належать завдання, що стосуються окремих аспектів функціонування ЄАІС Держмитслужби України та визначають регламент робіт з тими чи іншими функціональними сервісами ЄАІС Держмитслужби України.

Завдання, що повинні вирішуватись для забезпечення інформаційної безпеки ресурсів ЄАІС Держмитслужби України

Метою адміністративних завдань забезпечення є досягнення правильної і надійної роботи інформаційних систем шляхом виконання правил експлуатації ЄАІС та покладання відповідальності за їх недотримання (за необхідності з використанням додаткових заходів).

Вимоги до засобів керування інформаційної безпеки:

- надійність засобів керування безпекою забезпечується поділом ролей і обов'язків адміністраторів;
- наявність як мінімум інспектора із захисту інформації, адміністратора бази даних, адміністратора автоматизованої інформаційної системи, користувачів;

- контроль питань перерозподілу і додавання посадових обов’язків, пов’язаних з інформаційною безпекою;
- засоби адміністрування, що належать до інформаційної безпеки, повинні контролюватися на предмет їхнього несанкціонованого використання, модифікації, знищення;
- у системі повинні використовуватися механізми захисту під час реєстрації нових користувачів;
- повинен бути встановлений граничний час пасивності користувачів, після якого вони виключаються з числа легальних користувачів;
- системний адміністратор повинен мати можливість проводити аудит дій одного чи вибраної групи користувачів;
- засоби проведення аудиту повинні бути захищені від неавторизованого використання, модифікації, знищення;
- повинен існувати захисний механізм, що забезпечує доступ тільки авторизованого персоналу до виконання функцій адміністратора.

Аспекти, пов’язані з безпекою, повинні бути враховані на стадії набору персоналу та включені до посадових інструкцій і договорів та підлягати контролю протягом усього часу роботи такого співробітника. Про порушення режиму інформаційної безпеки необхідно негайно повідомляти адміністративними каналами. Усі співробітники повинні бути ознайомлені з процедурою повідомлення про різні типи інцидентів (порушення безпеки, загроза безпеці чи збій).

14.8. Етапи впровадження Концепції “Електронна митниця”

Впровадження Концепції розраховано на 2007—2013 рр.

Перший етап (2007 р.) упровадження Електронної митниці в Україні потребував низки послідовних кроків, спрямованих на:

- створення законодавчого підґрунтя для застосування інформаційно-телекомунікаційних технологій у взаємовідносинах як між контрольними органами та учасниками ЗЕД, так

і між самими контрольними органами, що є необхідною умовою для гарантування безконфліктного функціонування Електронної митниці;

- створення оптимальної структури інформаційного наповнення електронних систем, призначених для підготовки рішень (приписів), та надання цьому наповненню юридичного значення, що є необхідною умовою для впевненості контролюючих органів у прийнятті максимально об'єктивних рішень щодо поводження з товарами та транспортними засобами;

- аналіз стану та оптимізацію нормативно-правової, методологічної бази в частині автоматизації діяльності митної служби;

- удосконалення та подальший розвиток автоматизованих систем, що функціонують у митній службі, базуються на сучасних інформаційно-телекомунікаційних технологіях й направлені на технологічне забезпечення безперервного потоку, накопичення та обробки електронної митної інформації, впровадження механізму електронного декларування (впровадження приймання в електронному вигляді попередніх повідомлень (далі — ЄПП) на рівні центральної бази даних від суб'єктів ЗЕД, з якими укладено угоди про подачу митних документів в електронному вигляді і які користуються режимом сприяння);

- розвиток відомчої телекомунікаційної мережі для передачі даних, голосу, відеозображення та інтеграцію її з іншими аналогічними мережами органів державної влади;

- забезпечення захисту інформації в інформаційно-телекомунікаційних системах митних органів;

- модифікацію структури інформаційного наповнення ЄАІС до стану, що забезпечує об'єктивність підготовки рішень (приписів) на рівні митних органів;

- збільшення рівня забезпеченості митних органів сучасними інформаційно-телекомунікаційними засобами та упорядкування практики застосування технічних засобів митного контролю, надавши їй властивостей системності та передбачуваності.

На другому етапі (2008—2010 рр.) передбачається:

- створення системи адміністрування (у тому числі міжвідомчого) процесів, що відбуваються під час підготовки, видан-

ня, доведення рішень (приписів) та контролю за їх дотриманням, що є необхідною умовою для мінімізації часу проходження митних формальностей (для учасників ЗЕД) та раціоналізації дій контролюючих органів;

- створення системи оперативного виконання рішень, які потребують певного фізичного поводження (огляду, затримання, обмеження руху тощо) з товарами та транспортними засобами, що є необхідною умовою для недопущення несанкціонованого поводження з товарами та транспортними засобами, щодо яких виникає необхідність безпосереднього фізичного втручання;

- впровадження відомчої нормативно-правової бази ДМСУ шляхом створення та інформаційного наповнення корпоративної бази (на рівні центрального апарату), а також створення та інформаційного наповнення локальних баз даних (на базі інформаційного комплексу “Ліга : Корпорація”);

- впровадження системи електронного цифрового підпису (ЕЦП);

- створення та впровадження відомчої КСЗІ;

- подальше вдосконалення програмного забезпечення функціонування механізму електронного декларування (розробка програмного забезпечення локального рівня, що дасть змогу приймати повідомлення від суб’єктів ЗЕД як на рівні центральної бази даних (з подальшим інформуванням відповідного пункту митного оформлення), так і на рівні безпосередньо пункту митного оформлення;

- розвиток ВТМ у напрямі збільшення кількості її вузлів, її загальної пропускної спроможності та впровадження системи відомчого телефонного зв’язку і системи передачі відеозображення;

- розвиток інформаційно-телекомунікаційного комплексу “Електронна пошта” як інфраструктури транспортної системи електронного документообігу Держмитслужби України;

- створення та введення в дію у повнофункціональному режимі резервного центру обробки даних Електронної митниці;

- виконання робіт щодо гармонізації документів Електронної митниці відповідно до вимог Європейського Союзу (запровадження Єдиного уніфікованого документу (SAD));

— організація сумісності діючої (вдосконаленої) в митних органах України системи контролю за переміщенням вантажів із загальноєвропейською системою NCTS;

— уведення в дію засобів централізованого управління та адміністрування Електронної митниці.

На третьому етапі (2010—2013 рр.) передбачається:

— завершення впровадження системи аналізу ризиків як складової автоматизованої системи митного оформлення товарів і транспортних засобів як на рівні центрального апарату, так і на рівні митного органу (пункту митного оформлення);

— впровадження системи електронного документообігу між усіма ланками системи управління митними органами (на рівні: суб'єкт ЗЕД — пункт митного оформлення, пункт митного оформлення — адмінприміщення митного органу, митний орган — центральний апарат ДМСУ, пункт митного оформлення, митний орган — РІМ, і також у зворотному напрямку).

14.9. Очікувані результати реалізації Концепції

У результаті реалізації Концепції очікується:

— створення законодавчої бази з питань функціонування Електронної митниці з метою забезпечення гарантування конституційних прав громадян відповідно до засад розбудови демократичної правової держави та загальновизнаних міжнародних стандартів;

— забезпечення повноцінної участі України у міжнародному співробітництві, створення передумов до інтеграції України у світову спільноту;

— відстеження на базі сучасних інформаційних технологій динаміки міграційних, демографічних, соціальних та інших процесів у суспільстві;

— розвиток процесів інформатизації та електронного обігу інформації;

— підвищення прозорості та відкритості роботи органів державної влади;

— підвищення рівня інформаційної безпеки держави;

- зниження витрат, пов'язаних з використанням інформаційних ресурсів, що стосуються населення держави, за рахунок їх систематизації.

Критеріями оцінки ефективності реалізації Концепції є:

- створення інформаційно-технічних умов для оптимізації системи організації та здійснення митної справи, спрямованих на підвищення ефективності діяльності ДМСУ;
- рівень забезпечення ефективності автоматизації механізму справляння митних платежів;
- ступінь автоматизації виявлення та обліку митних правопорушень;
- рівень інтеграції інформаційних ресурсів митних органів з інформаційними системами інших міністерств і відомств України, а також з інформаційними системами митних служб інших країн;
- стан захищеності інформації;
- ступінь повноти, актуальності, достовірності інформації;
- рівень відмовостійкості системи;
- рівень забезпеченості митних органів сучасними апаратними засобами та програмним забезпеченням.

14.10. Шлях інформаційних технологій від e-Customs до i-Customs

Термін “інформаційні технології” вживають усі, але розуміє його кожен по-різному. Найчастіше під цим поняттям мають на увазі мережі, сервери, комп'ютери. Насправді ж інформаційні технології включають інші основи і тлумачення.

Розглянемо три джерела існування суспільства, які вже не можуть обійтися без застосування будь-якого обчислювального устаткування (рис. 14.1).

Перше джерело. Майбутнє для громадян. Громадяни здебільшого очікують від державних установ організації діяльності через приватні організації. Так, потрібен зручний, миттєвий доступ до державних послуг 24 години на добу, 7 днів на

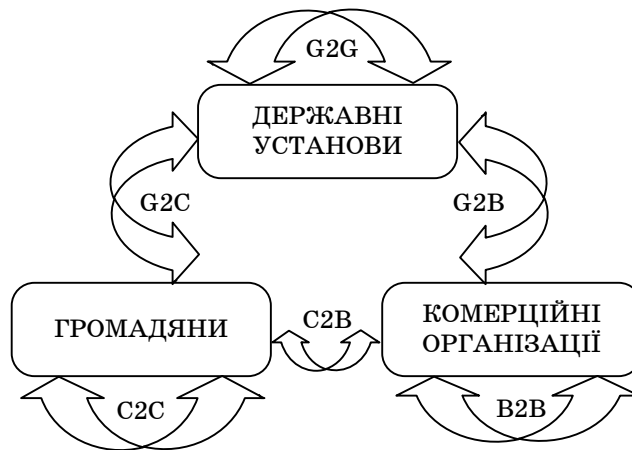


Рис. 14.1. Три джерела існування суспільства

тиждень, 365 діб на рік. Люди бажають одержувати послуги вдома, на роботі або в будь-якому іншому місці, не сприймаючи обмеження на типи пристроїв, які будуть використані для одержання доступу до державних послуг, — персональний комп'ютер, інтернет-телебачення, мобільний телефон чи інший портативний пристрій.

Громадян також не цікавить, яка конкретно група чиновників або яка офіційна особа відповідає за певну державну програму чи різновид послуг для населення. Проте завдяки технології єдиного доступу люди можуть більш активно брати участь у місцевому громадському житті та демократичних процесах, оскільки мають можливість взаємодіяти з державними органами та одержувати доступ до відкритої інформації та офіційних документів.

Друге джерело. Майбутнє для комерційних організацій. Взаємодія з державними установами за допомогою мережі Інтернету підвищує конкурентоспроможність комерційних організацій і дає їм можливість спростити різні офіційні процедури, зменшити кількість бюрократичних впливів. Компаніям стає легше дотримуватися законодавства, і вони можуть швид-

ше розпочати свою діяльність. Усе це досягається завдяки подачі документів в електронному вигляді, а також завдяки можливості сплатити податки чи надати звіти за допомогою мережі Інтернету.

Надання інтегрованих послуг через уніфіковану систему єдиного доступу дає можливість приватним установам і державним органам співпрацювати.

Третє джерело. Майбутнє для державних установ. Перебудова принципів взаємодії зі споживачами вимагає надавати послуги по-новому, без тривалих затримок і складних процедур. Організації, орієнтовані на споживачів, досягають більших успіхів у здійсненні своїх функцій, а також у спілкуванні з населенням. Такі організації здатні надати людям більш легкий доступ до послуг, збільшити обсяг послуг, що надаються, і знизити витрати часу службовців на діяльність, не пов'язану з роботою з клієнтами.

Організації, орієнтовані на потреби громадян, поєднують у єдине ціле систему керування взаємовідносинами зі споживачами, документообіг та інтернет-технології, перетворюючи державних службовців у працівників, “керуючих знаннями”. Співробітники повинні вміти використовувати програмні засоби керування справами, розбиратися у будь-якій ситуації, що виникла, і знати відповідні закони та норми. Їм необхідно впоратися з такою ситуацією і прийняти відповідне рішення. Таким працівникам варто вміти працювати в колективі та вільно переходити від одного документа (або бази даних) до іншого на будь-яких платформах.

Зважаючи на джерела існування суспільства, необхідно чітко розглянути базис та підґрунтя реалізації ефективного існування суспільства (рис. 14.2).

Розглянемо складники реалізації ефективного існування суспільства.

I. Модернізація інфраструктури.

1. Підтримка відкритих стандартів.
2. Інтегрування в комп'ютерні мережі й віртуалізація.
3. Міграція до служб орієнтованої архітектури.
4. Гарантія управління та управління доступом.

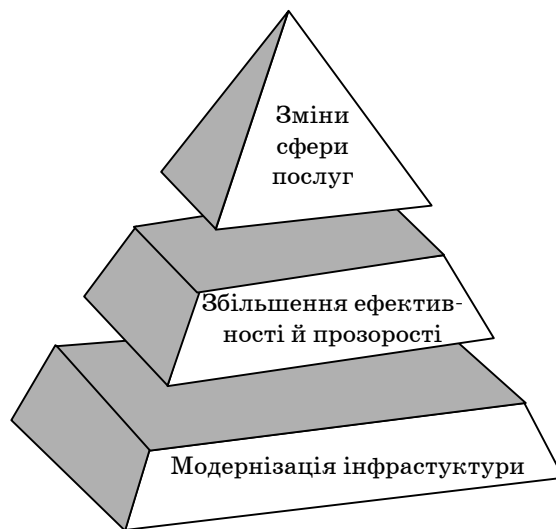


Рис. 14.2. Базис та підґрунтя реалізації ефективного існування суспільства

II. Збільшення ефективності й прозорості.

1. Надання послуг.

2. Управління діловими процесами:

- планування та складання бюджету;
- податки й доходи;
- фінансове та фіскальне управління;
- управління людськими ресурсами;
- придбання;
- проектування управління ресурсами.

3. Проектування й надання управління.

III. Зміни сфери послуг.

1. Забезпечення доступності системи обслуговування:

- CRM (централізоване управління);
- модульне управління;
- портали й зміст;
- автоматизація технологічного процесу та його призначення;

- GIS;
 - мобільна складова;
 - просування правил.
2. Управління даними.
 3. Доступність самообслуговування.
 4. Знання бізнесу й аналітики.

Враховуючи складові реалізації ефективного існування суспільства та необхідність реалізації технологічних досягнень, варто виокремити п'ять сукупних аспектів (рис. 14.3): інвестиції, інтелект, інфраструктура, інновації, інформація.

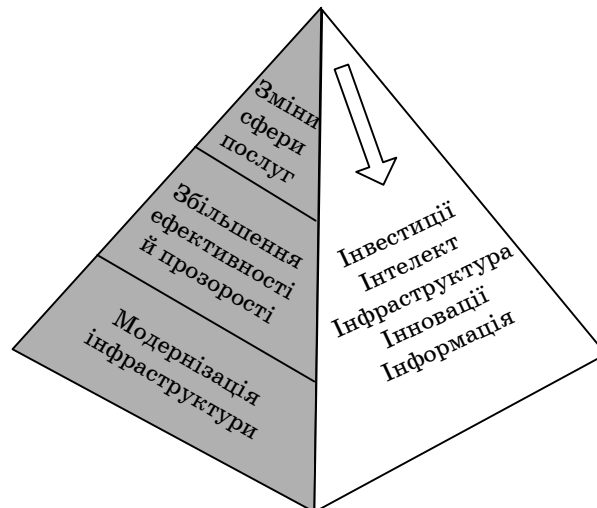


Рис. 14.3. П'ять сукупних аспектів

Інвестиції — довгострокові вкладення капіталу з метою отримання прибутку.

Інтелект — загальні здібності до пізнання, розуміння й вирішення проблем.

Інфраструктура — комплекс взаємопов'язаних обслуговуючих структур або об'єктів, складових, що забезпечують основу функціонування системи.

Інновація — нововведення в галузях техніки, технології, організації праці або управління, що ґрунтуються на викорис-

танні досягнень науки й передового досвіду, які забезпечують якісне підвищення ефективності виробничої системи або якості продукції.

Інформація — у широкому розумінні — абстрактне поняття, що має безліч значень залежно від контексту. У вузькому розумінні — відомості (повідомлення, дані) незалежно від форми їх представлення.

У недалекому минулому інформаційні технології визначали процес, який використовує сукупність засобів і методів збору, обробки та передачі даних для отримання інформації нової якості щодо стану об'єкта, процесу або явища.

Однак внаслідок розвитку науково-технічного прогресу, появи нових технічних засобів переробки інформації інформаційні технології зазнали еволюційних змін (рис. 14.4).

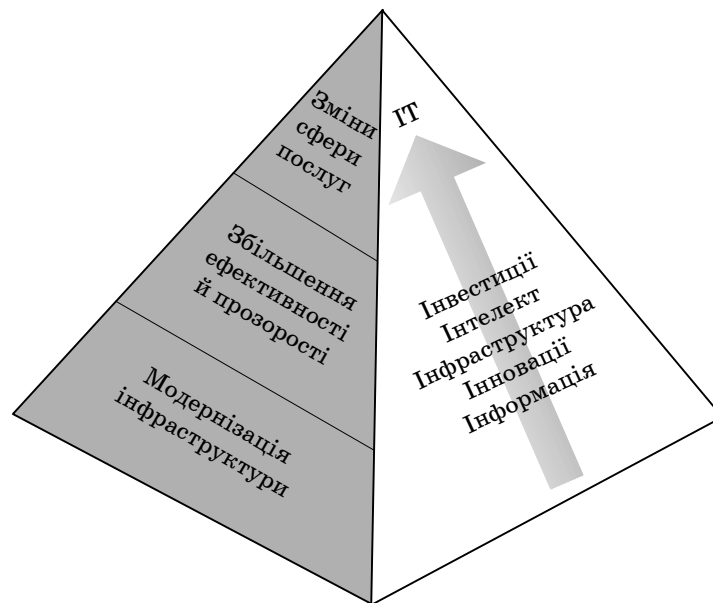
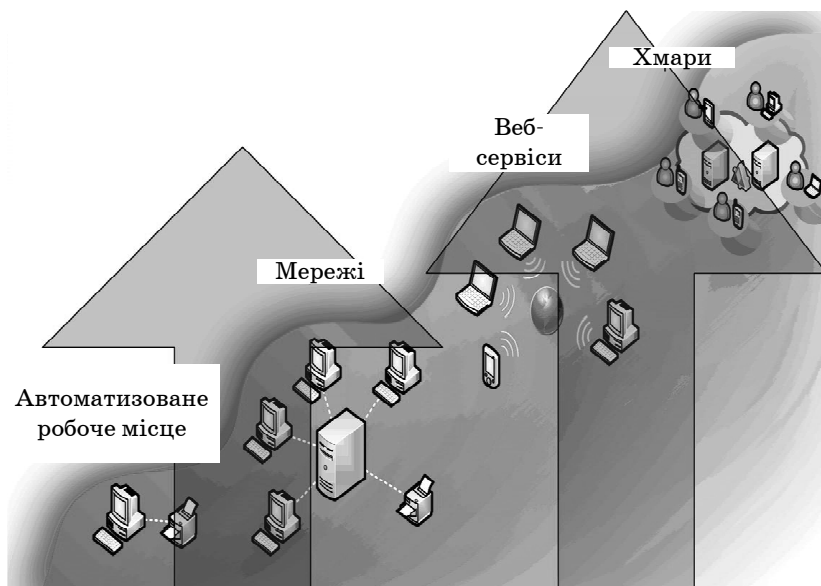


Рис. 14.4. Інформаційні технології в сучасному розумінні

Отже, *інформація* за допомогою нововведення в галузях техніки, технології тощо — *інновації*, що становлять комплекс взаємопов'язаних обслуговуючих структур або об'єктів, — *інфраструктура*, наділена загальними здібностями до пізнання, розуміння й вирішення проблем, — *інтелект* і довгострокові вкладення капіталу — *інвестиції* не тільки поєднують сучасне поняття інформаційних технологій, а й демонструють шлях їх активного та раціонального функціонування.

Практичну реалізацію п'яти сукупних аспектів реалізації ефективного існування суспільства наведено на рис. 14.5.



Електронна митниця (e-Customs) → Інформаційна митниця (i-Customs)

Рис. 14.5. Перехід від Електронної митниці до Інформаційної митниці

Поступова еволюція інформаційних технологій від функціонування окремих автоматизованих робочих місць до поєднання їх у мережі, подальшого надання доступу до інформації за

допомогою веб-сервісів і далі до поєднання засобів обчислювальної техніки в потужні централізовані центри обробки даних свідчить про перехід від застосування електронних засобів обробки інформації до сукупності методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, обробки, зберігання, розповсюдження, відображення й використання інформації в інтересах її користувачів.

Запитання і завдання для самоконтролю

1. Які принципи покладено в основу Міжнародної конвенції про спрощення та гармонізацію митних процедур?
2. Які положення Кіотської конвенції актуальні для України на сучасному етапі й чому?
3. За якою структурою передбачається модернізація митних органів України? У чому суть цієї модернізації?
4. Яку роль покладено на Регіональну інформаційну митницю?
5. Розкрийте сутність Концепції створення Електронної митниці.
6. Дайте визначення поняття “Електронний уряд”.
7. Яка мета створення Електронної митниці?
8. Які елементи мають стати складовими Електронної митниці?
9. Для чого необхідне впровадження системи електронного декларування у Державній митній службі України?
10. Які питання слід вирішити для реалізації концепції створення Електронної митниці?
11. Які основні завдання вирішує Електронна митниця?
12. Що таке “Інформаційна безпека Електронної митниці”?

ДОДАТКИ

Додаток 1

ПРОГРАМНО-ІНФОРМАЦІЙНІ КОМПЛЕКСИ ЄАІС ДМСУ

Розділ	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Митне оформлення	Приймання документів	Протокол приймання ВМД до ЦБД	Перегляд за номером ВМД або за період протоколу прийнятих або не прийнятих до ЦБД, за наявності помилки
		Протокол приймання листів узгодження до ЦБД	Перегляд за номером листа узгодження або за період протоколу прийнятих або не прийнятих до ЦБД, за наявності помилки
		Протокол приймання реєстрів залізничних вагонів до ЦБД	Перегляд інформації з реєстру залізничних вагонів за загальною ВМД
		Модифікація ВМД	Можливість внесення до ЄАІС заявок на коригування граф ВМД безпосередньо працівниками митниці, з подальшим повторним

Продовження дод. 1

Розділ	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Митне оформлення			наданням електронної копії ВМД для коригування в центральній базі даних
		Скасування інформації з контролю за доставкою вантажів	Надання митницям можливості відміни в ЄАІС раніше зроблених позначок про контроль за доставкою вантажів, в яких є помилкова інформація, із зазначенням причини відміни та введенням зміненої інформації
		Анулювання ВМД, що не підлягають контролю доставки вантажів	Анулювання електронних копій ВМД, які не підлягають контролю за доставкою вантажів, безпосередньо фахівцями митниці
	Митне оформлення	Оформлення ВМД	Приймання електронної копії ВМД безпосередньо від брокера, проходження етапів митного оформлення за web-технологією, реєстрації результатів митного оформлення на кожному етапі
		Листи узгодження	Використання електронних копій листів-узгодження під час контролю за доставкою вантажів (уведення та перегляд інформації)
		Реєстр ВМД типів ІМ 40 ПМД, ІМ 40 ТД та ІМ 40 НД	Перегляд інформації щодо ВМД типів ІМ 40 ПМД, ІМ 40 ТД та ІМ 40 НД
		Реєстр дозволів на право відкриття складів тимчасового зберігання	Перегляд інформації щодо дозволів на право відкриття складів тимчасового зберігання. Внесення та перегляд інформації стосовно дозволів на право відкриття складів тимчасового зберігання

Розділ	Підрозділ	Назва ПІК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Митне оформлення		Реквізити засвідчення сертифікатів про походження товару	Перегляд інформації щодо реквізитів засвідчення сертифікатів про походження товару. Внесення інформації щодо реквізитів засвідчення сертифікатів про походження товару
		Цінова інформація під час визначення митної вартості	Можливість перегляду цінової інформації про код товару з розрахунком ціни за одиницю товару на митниці, перегляд довідки-розрахунку, перегляд інформації про код товару та про ціни в регіоні з розрахунком середньої, мінімальної та максимальної цін
	Митне оформлення	Реєстр ВМД, в яких порушено вимоги НДМСУ № 520	Перегляд інформації за ВМД, в яких порушено вимоги НДМСУ № 520
		Аналіз ВМД	
		Реєстр класифікаційних рішень відділів ТМВ митниці	Перегляд інформації стосовно визначення митної вартості товарів, які приймалися на митницях
		Ведення реєстру класифікаційних рішень відділів ТМВ митниці	Внесення та перегляд інформації стосовно визначення митної вартості товарів, які приймалися на митницях
		Реєстрація товарів, що містять об'єкти інтелектуальної власності (ведення реєстру)	Внесення та перегляд інформації стосовно товарів, що містять об'єкти інтелектуальної власності, з можливим переглядом їх графічного зображення

Продовження дод. 1

Роз-діл	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Митне оформлення		Перегляд реєстру товарів, що містять об'єкти інтелектуальної власності (повний)	Перегляд (повний) інформації стосовно товарів, що містять об'єкти інтелектуальної власності, з можливим переглядом їх графічного зображення
		Здійснення контролю за переміщенням товарів, що містять об'єкти інтелектуальної власності	Контроль за переміщенням товарів, що містять об'єкти інтелектуальної власності, внесення відповідних позначок
		Перегляд реєстру товарів, що містять об'єкти інтелектуальної власності (обмежений)	Перегляд інформації стосовно товарів, що містять об'єкти інтелектуальної власності, з можливим переглядом їх графічного зображення
		Реєстр виробників дисків та СІД-кодів оптичних дисків для лазерних систем зчитування	Ведення реєстру виробників дисків та СІД-кодів оптичних дисків для лазерних систем зчитування. Перегляд реєстру виробників дисків та СІД-кодів оптичних дисків для лазерних систем зчитування
	Квитанція МД-1	Митний контроль і митне оформлення окремих транспортних засобів	Внесення інформації стосовно переміщення через митний кордон окремих видів транспортних засобів, їх митне оформлення та видача довідок для реєстрації в ДАІ. Перегляд реєстрів наявної інформації в ЄАІС

Розділ	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Митне оформлення		Перегляд квитанцій МД-1 та посвідчення на право реєстрації в ДАІ (ЦА Держмитслужби)	Перегляд наявної інформації в ЄАІС стосовно серії, номера та дати оформлення МД-1, МД-6, стосовно типу, марки, моделі, реєстраційного номера та номера кузова транспортного засобу
	Залізничні вагони	Реєстр залізничних вагонів, що є власністю суб'єктів ЗЕД	
	Експорт	Відділ контролю доставки вантажів	Контроль переміщення в режимі експорту через митний кордон України (уведення та перегляд інформації): — усіх товарів (для автомобільного виду транспорту); — давальницької сировини (для всіх видів транспорту); — експортний контроль (для всіх видів транспорту)
		Пункт пропуску	Уведення та перегляд інформації
		Відділ статистики	Перегляд інформації
		Відділення та служби боротьби з КБ та ПМП	Перегляд інформації
		Оператор УІЗМС	Перегляд повної інформації з контролю за доставкою вантажів
		Контроль переробки нафти на ВАТ “Нафтохімік Прикарпаття”	Уведення та перегляд інформації

Продовження дод. 1

Розділ	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Митне оформлення		Відділ контролю доставки вантажів (давальницька сировина і товари з давальницької сировини)	Уведення та перегляд інформації
		Пункт пропуску (давальницька сировина і товари з давальницької сировини)	Уведення та перегляд інформації
		Відділ статистики (давальницька сировина і товари з давальницької сировини)	Перегляд інформації
		Оператор УІЗМС	Перегляд повної інформації з контролю за доставкою вантажів
		Оператор УІЗМС (давальницька сировина і товари з давальницької сировини)	Перегляд повної інформації з контролю за доставкою вантажів (давальницька сировина і товари з давальницької сировини)
		Перелік окремих видів готової продукції відповідно до наказу Держмитслужби від 27 січня 2004 р. № 53	Перегляд інформації щодо окремих видів готової продукції

Роз-діл	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Доставка вантажів	Імпорт	Відділ контролю доставки вантажів	Контроль переміщення в режимі імпорту (попереднє декларування) через митний кордон України всіма видами транспорту (введення та перегляд інформації)
		Пункт пропуску	Уведення та перегляд інформації
		Відділ статистики	Перегляд інформації
		Відділення і служби боротьби з КБ та ПМП	Перегляд інформації
		Оператор УІЗМС	Перегляд інформації
		ЦА ДМСУ	
		Реєстр ПП та ПД для Управління технологій митного контролю	Перегляд реєстру ПП та ПД для Управління технологій митного контролю
		Контроль переробки нафти на ВАТ “Нафтохімік Закарпаття”	Уведення та перегляд інформації
		Перегляд реєстру місць прибуття	Перегляд інформації з реєстру місць прибуття
		Ведення реєстру місць прибуття	Перегляд інформації

Продовження дод. 1

Роз-діл	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Доставка вантажів	Транзит	Відділ контролю доставки вантажів	Контроль переміщення в режимі транзиту через митний кордон України всіх товарів для автомобільного та залізничного транспорту; експортний контроль — усі види транспорту; контроль внутрішнього транзиту (уведення та перегляд інформації)
		Пункт пропуску	Уведення та перегляд інформації
		Відділ статистики	Перегляд інформації
		Відділення і служби боротьби з КБ та ПМП	Перегляд інформації
		Оператор УІЗМС	Перегляд інформації
		Реєстр ВМД підпорядкованих митниць (на основі інформації з гр. 7, 29 та 53)	Перегляд інформації
	Провізні відомості	Відділ контролю доставки вантажів	Перегляд інформації
		Пункт пропуску	Перегляд інформації
		Оператор УІЗМС	Перегляд інформації
	Декларація МД-7	Прикордонна митниця	Перегляд інформації

Роз-діл	Підрозділ	Назва ПІК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Доставка вантажів		Внутрішня митниця	Перегляд інформації
		Оператор УІЗМС	Перегляд інформації
	Книжки МДП	Ведення реєстру книжок МДП	Ведення реєстру книжок МДП: — уведення інформації про книжку МДП; — перегляд реєстру книжок МДП
		Перегляд реєстру книжок МДП	Перегляд реєстру книжок МДП
		Недійсні книжки МДП	Перегляд картотеки недійсних книжок МДП
		Уведення інформації про недійсні книжки МДП	Ведення реєстру недійсних книжок МДП: — уведення інформації про недійсні книжки МДП; — повернення недійсної книжки МДП у стан дійсної згідно з листом АсМап; — перегляд картотеки недійсних книжок МДП
	Експортний контроль	Реєстрація ВМД, що мають гриф обмеженого доступу	Ведення БД номерів ВМД, що мають гриф обмеженого доступу. Перегляд інформації
		Звіти про доставку вантажів, що підлягають експортному контролю	Формування звіту певної форми стосовно перетину кордону в режимах експорту, імпорту, транзиту товарів, які підлягають експортному контролю, і внесення відповідних позначок у ПІК про контроль за доставкою вантажів

Продовження дод. 1

Розділ	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Доставка вантажів	Повітряні судна	Контроль тимчасового ввезення / вивезення повітряних суден	
	ВМД Російської Федерації	Перегляд ВМД Російської Федерації	Перегляд інформації
Довідники	Печатки та штамп-пи	Перегляд БД особистого митного забезпечення	Перегляд інформації про особисте митне забезпечення
		Ведення БД особистого митного забезпечення	Уведення та перегляд інформації про особисте митне забезпечення
	Учасники ЗЕД	Перегляд картотеки учасників ЗЕД	Перегляд інформації про акредитацію учасників ЗЕД
		Ведення картотеки учасників ЗЕД	Ведення та перегляд картки реєстрації учасника ЗЕД на митницях
		Перегляд картотеки учасників ЗЕД у ЦА ДМСУ	Перегляд фахівцями Держмитслужби загальної інформації про акредитацію учасників ЗЕД
		Судові рішення	Ведення та перегляд інформації стосовно проходження судових справ, в яких задіяні митні органи
	Перевізники		Ведення та перегляд реєстру перевізників, порушників чинного законодавства

Роз-діл	Підрозділ	Назва ППК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Довідники		Перегляд БД зіпсованих, анульованих та невикористаних бланків форми МД-1, МД-2, МД-3, МД-6 і голографічних етикеток	Перегляд інформації про бланки суворої звітності
		Ведення БД зіпсованих, анульованих та невикористаних бланків форми МД-1, МД-2, МД-3, МД-6 і голографічних етикеток	Уведення та перегляд інформації про бланки суворої звітності
	Класифікаційна довідкова система	Перегляд УКТНЗЕД	Перегляд Українського класифікатора товарної номенклатури зовнішньоекономічної діяльності. Розробка додаткового програмного забезпечення стосовно його друку
		Пошук товарів в УКТНЗЕД	Ведення та перегляд Українського класифікатора товарної номенклатури зовнішньоекономічної діяльності (інформація про товари і митний тариф)
		Довідка про товар	Ведення та перегляд Українського класифікатора товарної номенклатури зовнішньоекономічної діяльності (інформація про товари)

Продовження дод. 1

Розділ	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Довідники		Пошук нормативних документів	Перегляд інформації стосовно тарифного та нетарифного регулювання
	Санкції	Перегляд реєстру спеціальних санкцій	Перегляд реєстру учасників ЗЕД, до яких застосовано спеціальні санкції
		Ведення реєстру спеціальних санкцій	Ведення та перегляд реєстру учасників ЗЕД, до яких застосовано спеціальні санкції
	Лікарські засоби	Лікарські засоби, зареєстровані в Україні (станом на ...)	Перегляд реєстру лікарських засобів, зареєстрованих в Україні. Інформація надається Мінздравом і використовується під час переміщення через митний кордон у режимі імпорту
	Міжнародна допомога	Державна реєстрація програм і проектів міжнародної технічної допомоги	Ведення та перегляд реєстру програм і проектів міжнародної технічної допомоги
	Гуманітарна допомога	Перегляд єдиного реєстру	Перегляд єдиного реєстру отримувачів гуманітарної допомоги та переліку вантажів, які визнано гуманітарною допомогою
		Ведення єдиного реєстру	Уведення і модифікація інформації єдиного реєстру отримувачів гуманітарної допомоги та переліку вантажів, які визнано гуманітарною допомогою

Розділ	Підрозділ	Назва ППК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Спеціальні санкції	ЦА Держмит-служби	Переміщення товарів та інших предметів за період часу	Перегляд інформації стосовно переміщення товарів та інших предметів за період часу
		Реєстр ВМД на зерно та зернопродукти за період часу	Перегляд реєстру ВМД на зерно та зернопродукти на заданий період часу
	Оперативна митниця	Контроль доставки вантажів	Перегляд інформації з контролю за доставкою вантажів
Контрабанда	Контрабанда	Боротьба з контрабандою та порушеннями митних правил	Уведення інформації про порушення митних правил та контрабанду (розробка НДПКІ “Іскра”). Перегляд інформації про порушення митних правил та контрабанду (розробка НДПКІ “Іскра”)
		Порушники митних правил	Ведення та перегляд картотеки порушників митних правил
		Аналітична і статистична обробка інформації про суб’єктів ЗЕД — порушників чинного законодавства	Перегляд звітів про порушення митних правил (формується за інформацією, яка накопичується ППК розробки НДПІ “Іскра”)

Продовження дод. 1

Роз-діл	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Контрабанда	Доставка вантажів	ЦА ДМСУ	Перегляд інформації
		Відділення і служби боротьби з КБ та ПМП: імпорт	Перегляд інформації
		Відділення і служби боротьби з КБ та ПМП: експорт	Перегляд інформації
		Відділення і служби боротьби з КБ та ПМП: транзит	Перегляд інформації
	Конфіскації	Облік конфіскацій	Облік затриманого, конфіскованого, прийнятого на зберігання майна та подальше його використання згідно з митним законодавством (уведення та перегляд інформації)
	Орієнтування	Орієнтування	Уведення та перегляд інформації щодо орієнтувань для затримання товарів, фізичних, юридичних осіб, транспортних засобів, якими не було доставлено в митницю призначення товари
	Пошук	ВМД усіх або обраних типів для певного транспортного засобу, суб'єкта ЗЕД	Отримання інформації щодо ВМД усіх типів для певного транспортного засобу, суб'єкта ЗЕД за заданими параметрами пошуку

Розділ	Підрозділ	Назва ППК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Контрабанда		ВМД, які підлягають контролю за доставкою вантажів для обраного транспортного засобу в "Історії документа" і суб'єкта	Отримання інформації щодо ВМД, які підлягають контролю за доставкою вантажів для обраного транспортного засобу в історії документа та суб'єкта
		Транспортні засоби за номерами державної реєстрації, кузова, шасі, двигуна (МД-7)	Перегляд інформації щодо транспортних засобів за номерами державної реєстрації, кузова, шасі, двигуна (МД-7)
		Транспортні засоби за номерами державної реєстрації, кузова, шасі, двигуна (МД-1 та МД-6)	Перегляд інформації щодо транспортних засобів за номерами державної реєстрації, кузова, шасі, двигуна (МД-1 та МД-6)
Звіти	Форми звітності	Заповнення встановлених форм звітності	Формування статистичної звітності регіональними митницями та митницями за основними напрямками їх діяльності (уведення та перегляд)
	Платежі	Довідка про платежі за попередніми деклараціями	Перегляд інформації
		Довідка про платежі, сплачені за квитанціями МД-1	Перегляд інформації

Продовження дод. 1

Роз-діл	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Звіти	Статисти-ка	Оформлені ВМД та допущені при цьому помилки	Перегляд протоколів приймання ВМД до ЄАІС Держмитслужби
		Контроль переміщення цукру та виробів з цукру (імпорт і транзит)	Перегляд інформації про переміщення через митний кордон України окремих видів товарів (індивідуальний доступ для користувачів за номером службового посвідчення)
		Експортно-імпортні операції з нафтою і нафтопродуктами	Отримання звіту (за номером посвідчення) щодо експортно-імпортних операцій з нафтою і нафтопродуктами для Управління митної статистики
		Експортно-імпортні операції із зерном	Отримання звіту (за номером посвідчення) щодо експортно-імпортних операцій із зерном
		Експортно-імпортні операції із взуттям	Отримання звіту (за номером посвідчення) щодо експортно-імпортних операцій зі взуттям
		Експортні операції з чорними металами	Отримання звіту (за номером посвідчення) щодо експортних операцій з чорними металами
		Моніторинг увезення цукру-сирцю	Моніторинг (за номером посвідчення) ввезення цукру-сирцю

Роз-діл	Підрозділ	Назва ПК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Звіти		Звіт про експортні операції, загальна фактурна вартість яких перевищує один мільйон гривень	Отримання (за номером посвідчення) звіту щодо експортних операцій, загальна фактурна вартість яких перевищує один мільйон гривень
		Форми звітності для державних органів України (Кабмін України, СБУ)	
	Митниця	Системний аналіз завантаженості митниці	Уведення та перегляд інформації про завантаженість митниці
	Транспортні засоби	Оформлення автотранспортних засобів фізичними особами	Перегляд узагальненої інформації про оформлення автотранспортних засобів фізичними особами
	Ліцензійні склади	Довідка про рух товарів через митні ліцензійні склади	
	Боротьба з КБ та ПМП	Довідка про роботу відділів боротьби з КБ та ПМП	
		Реєстр ВМД, за якими здійснювалося оформлення товарів за кодами УКТЗЕД, що входять до 6 групи	

Закінчення дод. 1

Розділ	Підрозділ	Назва ПІК в ЄАІС ДМСУ	Опис процесів, що автоматизуються підсистемою
Навчання та тестування	Тестування	Проведення Тестування	
		Створення та модифікація тестових запитань і складання екзаменаційних білетів	
		Ведення та перегляд екзаменаційних відомостей	
	Навчальний УК-ТНЗЕД	Ведення УКТНЗЕД і Митного тарифу України	
		Ведення Українського класифікатора товарної номенклатури зовнішньоекономічної діяльності	
		Ведення Митного тарифу України	
Регламентований доступ	Паролі доступу	Зміна пароля доступу до ЄАІС Держмитслужби	Зміна пароля користувача, що здійснюється безпосередньо користувачем
		Перелік ПІК ЄАІС Держмитслужби	
	Адміністратор	Адміністратор регламентованого доступу до ЄАІС Держмитслужби	Адміністрування доступу користувачів ЄАІС (проводиться безпосередньо адміністратором митного органу)
		Перелік ПІК ЄАІС Держмитслужби	Доступ для всіх користувачів, які зареєстровані в ЄАІС

Таблиця 1. Види гарантій

Код	Назва
00	Гарантія не потрібна
01	Гарантія банку
02	У вигляді внесення грошової застави
03	Гарантія митного перевізника
04	Охорона і супроводження товарів митною вартою
05	Гарантія відповідно до конвенції МДП
06	Гарантія незалежного фінансового посередника

Таблиця 2. Митні режими

Код	Назва
010	Експорт
011	Реекспорт
031	Тимчасове ввезення (вивезення)
040	Імпорт
041	Реімпорт
051	Переробка на митній території України
061	Переробка за межами митної території України
071	Спеціальна митна зона
072	Магазин безмитної торгівлі
074	Митний склад
075	Відмова на користь держави
076	Знищення або руйнування
080	Транзит

Таблиця 3. Види транспорту

Код	Назва
10	Морський транспорт (у контейнері)
12	Залізничний вагон на морському судні
16	Самохідний дорожній засіб на морському судні
17	Несупроводжуваний причіп на морському судні
18	Річкове судно на морському судні
20	Залізничний транспорт, крім ДТЗ
23	Дорожній транспортний засіб у залізничному вагоні
30	Автодорожний транспорт
40	Повітряний транспорт
50	Пошта
60	Змішані перевезення
70	Стаціонарний транспортний засіб (трубопровід, ЛЕП)
80	Внутрішній водний транспорт
90	Вид транспорту невідомий (поклажа)

Таблиця 4. Митні платежі

Код	Назва
001	Митний збір за перебування товарів та інших предметів під митним контролем
003	Митний збір за митне оформлення товарів та інших предметів у зонах митного контролю на територіях і в приміщеннях підприємств, що зберігають такі товари та інші предмети, чи поза робочим часом, установленим для митниці
004	Митний збір за відмову від замовлених послуг, передбачених кодом 003 цього Класифікатора, без завчасного попередження в письмовій формі
005	Митний збір за митне оформлення транспортного засобу індивідуального користування, якщо цей засіб використовується для перевезення товарів та інших предметів в обсягах, що підлягають обкладенню митом

Продовження табл. 4

Код	Назва
006	Митний збір за видачу посвідчень на право реєстрації (перереєстрації) увезених в Україну транспортних засобів (у тому числі ввезених тимчасово), а також номерних агрегатів, що підлягають реєстрації в органах Державної автомобільної інспекції
008	Митний збір за зберігання товарів та інших предметів на складах митниць (крім товарів та інших предметів, зазначених у ст. 86 Митного кодексу України від 12 грудня 1991 р. № 1970-ХІІ)
009	Митний збір за зберігання товарів та інших предметів, що підлягають обов'язковому переданню митниці для зберігання й зазначені в ст. 86 Митного кодексу України від 12 грудня 1991 р. № 1970-ХІІ
010	Митний збір за митне оформлення товарів та інших предметів
012	Митний збір за митне оформлення товарів відповідно до режиму тимчасового ввезення (вивезення)
015	Митний збір за митне оформлення товарів відповідно до режиму митного складу
018	Митний збір за продовження строку дії (перереєстрацію) свідоцтва про визнання підприємства декларантом
019	Митний збір за видачу підприємству свідоцтва про визнання його декларантом
020	Мито на товари, що ввозяться на територію України суб'єктами підприємницької діяльності
021	Мито на нафтопродукти, які підлягають обкладенню акцизним збором, транспортні засоби, які підлягають обкладенню акцизним збором, та шини до них, які раніше, згідно із Законом України "Про ставки акцизного збору і ввізного мита на деякі транспортні засоби", обкладалися акцизним збором, що ввозяться суб'єктом підприємницької діяльності
023	Антидемпінгове мито на товари, що ввозяться на територію України суб'єктами підприємницької діяльності
024	Спеціальне мито на товари, що ввозяться на територію України суб'єктами підприємницької діяльності

Продовження табл. 4

Код	Назва
026	Плата за супроводження та охорону товарів
027	Інші підакцизні товари (акцизний збір з товарів, увезених на територію України суб'єктами підприємницької діяльності)
028	Податок на додану вартість з товарів, увезених на територію України суб'єктами підприємницької діяльності
029	Збір за видачу ліцензії на право відкриття та експлуатації митного ліцензійного складу на території України. Збір за щорічну перереєстрацію митних ліцензійних складів
032	Надходження коштів від надання в установленому законодавством порядку консультацій з питань митної справи
039	Надходження коштів від надання митними органами в установленому законодавством порядку інших видів послуг у галузі митної справи
040	Мито на товари, що вивозяться (пересилаються) з території України суб'єктами підприємницької діяльності
043	Антидемпінгове мито на товари, що вивозяться з території України суб'єктами підприємницької діяльності
050	Штрафи за порушення митних правил
051	Надходження коштів від реалізації конфіскованого митними органами майна
052	Валюта конфіскована
053	Надходження валюти, щодо якої минув строк позовної давності
055	Валютні цінності та грошові кошти, власники яких невідомі
059	Надходження коштів від реалізації безхазяйного майна та майна, за яким не звернувся власник, строк зберігання якого закінчився. Компенсація вартості конфіскованих товарів
065	Додатковий митний збір за митне оформлення нафтопродуктів, що імпортуються на митну територію України й підлягають обкладенню акцизним збором
067	Митний збір за видачу сертифіката підтвердження доставки товару, прийнятого під режим експортного контролю України

Продовження табл. 4

Код	Назва
070	Єдиний збір, який справляється в пунктах пропуску через державний кордон України (код застосовується виключно під час заповнення граф В, С вантажної митної декларації відповідно до митного режиму транзиту)
072	Митний збір за реєстрацію товарів, що містять об'єкти інтелектуальної власності, на строк 6 місяців
073	Митний збір за реєстрацію товарів, що містять об'єкти інтелектуальної власності, на строк 12 місяців
074	Митний збір за продовження строку реєстрації кожного товару
075	Митний збір за внесення до реєстру товарів, що містять об'єкти інтелектуальної власності
079	Надходження сум кредиторської та депонентської заборгованості підприємств, організацій та установ, щодо яких минув строк позовної давності
080	Спирт (акцизний збір з товарів, увезених на територію України суб'єктами підприємницької діяльності)
081	Лікєро-горілочна продукція (акцизний збір з товарів, увезених на територію України суб'єктами підприємницької діяльності)
082	Виноробна продукція (акцизний збір з товарів, увезених на територію України суб'єктами підприємницької діяльності)
083	Пиво (акцизний збір з товарів, увезених на територію України суб'єктами підприємницької діяльності)
084	Тютюн і тютюнові вироби (акцизний збір з товарів, увезених на територію України суб'єктами підприємницької діяльності)
085	Транспортні засоби (крім мотоциклів і велосипедів) (акцизний збір з товарів, увезених на територію України суб'єктами підприємницької діяльності)
086	Мотоцикли й велосипеди (акцизний збір з товарів, увезених на територію України суб'єктами підприємницької діяльності)
088	Бензин моторний (акцизний збір з товарів, увезених на територію України суб'єктами підприємницької діяльності)
089	Інші нафтопродукти (акцизний збір з товарів, увезених на територію України суб'єктами підприємницької діяльності)

Продовження табл. 4

Код	Назва
120	Мито на товари, що ввозяться (пересилаються) на територію України громадянами
121	Мито на нафтопродукти, які підлягають обкладанню акцизним збором, транспортні засоби та шини до них, які раніше, згідно із Законом України “Про ставки акцизного збору і ввізного мита на деякі транспортні засоби та шини до них”, обкладалися акцизним збором, що ввозяться на територію України громадянами
123	Антидемпінгове мито на товари, що ввозяться на територію України громадянами
124	Спеціальне мито на товари, що ввозяться на територію України громадянами
127	Інші підакцизні товари (акцизний збір з товарів, увезених на територію України громадянами)
128	Податок на додану вартість з товарів, увезених на територію України громадянами
143	Антидемпінгове мито на товари, що вивозяться з території України громадянами
180	Спирт (акцизний збір з товарів, увезених на територію України громадянами)
181	Лікєро-горілочна продукція (акцизний збір з товарів, увезених на територію України громадянами)
182	Виноробна продукція (акцизний збір з товарів, увезених на територію України громадянами)
183	Пиво (акцизний збір з товарів, увезених на територію України громадянами)
184	Тютюн і тютюнові вироби (акцизний збір з товарів, увезених на територію України громадянами)
185	Транспортні засоби (крім мотоциклів і велосипедів), акцизний збір з товарів, увезених на територію України громадянами)
186	Мотоцикли й велосипеди (акцизний збір з товарів, увезених на територію України громадянами)
188	Бензин моторний (акцизний збір з товарів, увезених на територію України громадянами)

Додатки

Закінчення табл. 4

Код	Назва
189	Інші нафтопродукти (акцизний збір з товарів, увезених на територію України громадянами)
228	Податок на додану вартість з товарів, увезених на територію України з дотриманням вимог ст. 129 Митного кодексу України

Таблиця 5. Умови поставки

Код	Назва	English
1	EXW франко-завод	EXW
2	FCA франко-перевізник	FCA
3	FAS франко вздовж борту судна	FAS
4	FOB франко-борт	FOB
5	CFR вартість і фрахт	CFR
6	CIF вартість, страхування і фрахт	CIF
7	CPT перевезення оплачено до ...	CPT
8	CIP перевезення й страхування оплачено до ...	CIP
9	DAF поставка до кордону	DAF
10	DES доставлено франко-строп судно	DES
11	DEQ доставлено франко-набережна (мити сплачено)	DEQ
12	DDU доставлено, мито не сплачено	DDU
13	DDP доставлено, мито сплачено	DDP

Таблиця 6. Одиниці виміру

Код	Коротка назва	Назва
0013	см ³	Сантиметр кубічний
0056	7,5 м ²	Сім з половиною метрів квадратних
0101	м	Метр
0123	м ²	Квадратний метр
0124	7,5 м ²	Сім з половиною квадратних метрів

Продовження табл. 6

Код	Коротка назва	Назва
0134	м ³	Кубічний метр
0138	л	Літр
0160	100 г	Сто грамів
0161	140 г	Сто сорок грамів
0164	200 г	Двісті грамів
0165	250 г	Двісті п'ятдесят грамів
0167	100 кг	Сто кілограмів
0168	Б/КГ	Брутто-кілограм
0180	1000 кг	Тисяча кілограмів
0182	т	Тонна
0211	туб	Туб
0212	см	Сантиметр
0213	см ³	Сантиметр кубічний
0301	кг	Кілограм
0302	1 кг живої ваги	Один кілограм живої ваги
0303	г	Грам
0304	б/кг	Брутто-кілограм
0310	100 кг	Сто кілограм
1215	Ki	Кюрі
1501	кг U	Кілограм урану
1507	кг K ₂ O	Кілограм оксиду калію
1521	кг H ₂ O ₂	Кілограм пероксиду водню
1527	кг N	Кілограм азоту
1528	кг KOH	Кілограм гідроокису калію
1529	кг NaOH	Кілограм гідроокису натрію
1531	кг P ₂ O ₅	Кілограм п'ятиокису фосфору
1532	кг C ₅ H ₁₄ ClNO	Кілограм хлориду холіну
1617	пар	Пара (2 шт.)
1773	кар	Карат метричний (=200 мг)

Закінчення табл. 6

Код	Коротка назва	Назва
1806	тис. кВт·год	Тисяча кіловат-годин
2009	шт.	Штука
2012	100 шт.	Сто штук
2013	тис. шт.	Тисяча штук
2087	л 100 % спирту	Літр 100 % спирту
2088	1 об. % спирту	Один об'ємний відсоток спирту в одному літрі
2155	г поділ. ізотоп	Грам подільних ізотопів
2349	1000 кг	Тисяча кілограмів
2350	брутто реєстр. т	Брутто-реєстрова тонна
2351	вантажопідйом.	Вантажопідйомність у метричних тоннах
2352	т	Тонна
2779	тис. м ³	Тисяча кубічних метрів
2826	кг сух. 90 % реч	Кілограм сухої на 90 % речовини
2839	тис. л	Тисяча літрів

Таблиця 7. Форма оплати

Код	Назва
10	Акредитив
20	Інкасо
30	Переказ
40	Акредитив/інкасо
50	Акредитив/переказ
60	Інкасо/переказ
70	Акредитив/інкасо/переказ

Таблиця 8. Країни

Код	Код літерний	Назва	English
004	AFG	Афганістан	Afghanistan
008	ALB	Албанія	Albania
012	DZA	Алжир	Algeria
031	AZE	Азербайджан	Azerbaijan
032	ARG	Аргентина	Argentina
036	AUS	Австралія	Australia
040	AUT	Австрія	Austria
044	BHS	Багами	Bahamas
051	ARM	Вірменія	Armenia
056	BEL	Бельгія	Belgium
076	BRA	Бразилія	Brazil
100	BGR	Болгарія	Bulgaria
112	BLR	Білорусь	Belarus
124	CAN	Канада	Canada
144	LKA	Шрі-Ланка	Sri Lanka
156	CHN	Китай	China
158	TWN	Тайвань	Taiwan, province of China
191	HRV	Хорватія	Croatia
192	CUB	Куба	Cuba
196	CYP	Кіпр	Cyprus
203	CZE	Чеська Республіка	Czech Republic
208	DNK	Данія	Denmark
233	EST	Естонія	Estonia
246	FIN	Фінляндія	Finland
250	FRA	Франція	France
268	GEO	Грузія	Georgia
276	DEU	Німеччина	Germany
300	GRC	Греція	Greece
304	GRL	Гренландія	Greenland

Код	Код літерний	Назва	English
344	HKG	Гонконг	Hong Kong
348	HUN	Угорщина	Hungary
352	ISL	Ісландія	Iceland
356	IND	Індія	India
360	IDN	Індонезія	Indonesia
364	IRN	Іран	Iran, Islamic Republic of
368	IRQ	Ірак	Iraq
372	IRL	Ірландія	Ireland
376	ISR	Ізраїль	Israel
380	ITA	Італія	Italy
392	JPN	Японія	Japan
398	KAZ	Казахстан	Kazakhstan
408	PRK	Корея (КНДР)	Korea, Democratic People's Republic
410	KOR	Корея, Республіка	Korea, Republic of
417	KGZ	Киргизстан	Kyrgyzstan
428	LVA	Латвія	Latvia
440	LTU	Литва	Lithuania
		...	
442	LUX	Люксембург	Luxembourg
496	MNG	Монголія	Mongolia
498	MDA	Молдова	Republic of Moldova
504	MAR	Марокко	Marocco
528	NLD	Нідерланди	Netherlands
578	NOR	Норвегія	Norway
616	POL	Польща	Poland
620	PRT	Португалія	Portugal
642	ROM	Румунія	Romania
643	RUS	Російська Федерація	Russian Federation

Закінчення табл. 8

Код	Код літерний	Назва	English
702	SGP	Сінгапур	Singapore
703	SVK	Словаччина	Slovakia
704	VNM	В'єтнам	Viet Nam
705	SVN	Словенія	Slovenia
724	ESP	Іспанія	Spain
752	SWE	Швеція	Sweden
756	CHE	Швейцарія	Switzerland
762	TJK	Таджикистан	Tajikistan
764	THA	Таїланд	Thailand
792	TUR	Туреччина	Turkey
795	TKM	Туркменистан	Turkmenistan
		. . .	
804	UKR	Україна	Ukraine
840	USA	Сполучені Штати Америки	United States
860	UZB	Узбекистан	Uzbekistan
862	VEN	Венесуела	Venezuela
891	SIG	Сербія і Чорногорія	Serbia and Montenegro
894	ZMB	Замбія	Zambia

ЛІТЕРАТУРА

1. Про інформацію : Закон України від 2 жовтня 1992 р. // Відомості Верховної Ради України. — 1992. — № 48. — Ст. 650.
2. Про Національну програму інформатизації : Закон України від 4 лютого 1998 р. // Відомості Верховної Ради України. — 1998. — № 27—28. — Ст. 181.
3. Про науково-технічну інформацію : Закон України від 25 червня 1993 р. // Відомості Верховної Ради України. — 1993. — № 33. — Ст. 345.
4. Про державну таємницю : Закон України від 21 січня 1994 р. // Відомості Верховної Ради України. — 1994. — № 16. — Ст. 93.
5. Про захист інформації в автоматизованих системах : Закон України.
6. Про електронний цифровий підпис : Закон України від 22 травня 2003 р. // Відомості Верховної Ради України. — 2003. — № 36. — Ст. 276.
7. Про Єдиний митний тариф : Закон України від 5 лютого 1992 р. // Відомості Верховної Ради України. — 1992. — № 19. — Ст. 259.
8. Про застосування міжнародних правил інтерпретації комерційних термінів : Указ Президента України від 4 жовтня 1994 р.
9. Про Державний класифікатор управлінської документації ДК 010-98 : наказ Держстандарту України від 31 грудня 1998 р. № 1024.
10. Про затвердження Концепції створення, запровадження і розвитку системи електронного декларування товарів : наказ Державної митної служби України від 18 жовтня 2006 р. № 907.

11. Положення про електронну інформацію в митній системі України : наказ Державної митної служби України від 8 лютого 1996 р. № 48.

12. Про затвердження Порядку організації захисту інформації під час здійснення митного контролю та митного оформлення товарів і транспортних засобів із застосуванням вантажної митної декларації, яка містить інформацію з обмеженим доступом, що є власністю держави : наказ Державної митної служби України від 5 січня 2005 р. № 5.

13. Про затвердження Положення про Центральний засвідчувальний орган : Пост. Кабінету Міністрів України від 28 жовтня 2004 р. № 1451.

14. *Буров Є.* Комп'ютерні мережі / Є. Буров. — 2-ге вид., оновл. і доповн. — Л. : Бак, 2003. — 584 с.

15. *Вертузаєв М.С.* Захист інформації в комп'ютерних системах від несанкціонованого доступу : навч. посіб. / М.С. Вертузаєв, О.М. Юрченко. — К. : Вид-во Європ. ун-ту, 2001. — 321 с.

16. *Волик О.Ф.* Основні принципи побудови Єдиної автоматизованої інформаційної системи ДМСУ : навч.-метод. посіб. / О.Ф. Волик, І.В. Дорда. — Д. : АМСУ, 2004.

17. *Гребельник О.П.* Основи митної справи : навч. посіб. / О.П. Гребельник. — К. : Центр навч. л-ри, 2003. — 600 с.

18. *Гужва В.М.* Інформаційні системи і технології на підприємствах : навч. посіб. / В.М. Гужва. — К. : КНЕУ, 2001. — 400 с.

19. *Гужва В.М.* Інформаційні системи в міжнародному бізнесі : навч. посіб. / В.М. Гужва, А.Г. Постевой. — 2-ге вид., доповн. і переробл. — К. : КНЕУ, 2002. — 458 с.

20. *Домарев В.В.* Защита информации и безопасность компьютерных систем / В.В. Домарев. — К. : ДияСофт, 1999. — 480 с.

21. *Дубиніна А.А.* Основи митної справи в Україні : навч. посіб. / А.А. Дубиніна, С.В. Сорокіна. — К. : Професіонал, 2004. — 360 с.

22. *Жорін Ф.Л.* Правові засади митної справи України : навч. посіб. / Ф.Л. Жорін, І.Н. Звягіна. — К. : Магістр — ХХІ сторіччя, 2005. — 384 с.

23. Інформаційні системи та технології в економіці : посібник / за ред. В.С. Пономаренко. — К. : Академія, 2002. — 542 с.

24. Митний контроль та митне оформлення : навч. посіб. / за ред. М.М. Каленського, П.В. Пашка. — К. : Т-во "Знання", КОО, 2002. — 284 с.

25. *Згуровський М.З.* Вступ до комп'ютерних інформаційних технологій : навч. посіб. / М.З. Згуровський, І.І. Коваленко, В.М. Михайленко. — К. : Вид-во Європ. ун-ту, 2002. — 265 с.
26. Информатика для юристов и экономистов / С.В. Симонович и др. — СПб. : Питер, 2001. — 688 с.
27. Інформаційні системи і технології : навч. посіб. / С.Г. Карпенко, В.В. Попов, Ю.А. Тарнавський та ін. — К. : МАУП, 2004. — 192 с.
28. *Макогон Ю.В.* Митна справа : навч. посіб. / Ю.В. Макогон, А.Б. Яценко. — К. : Центр навч. л-ри, 2005. — 224 с.
29. *Матієга В.* Створення ефективної системи аналізу та управління ризиками / В. Матієга // Митниця. — 2006. — № 5 (18).
30. *Науменко В.* Митна вартість товарів: Теорія та практика : довід. посіб. / В. Науменко, М. Яворський. — К. : Інтерес, 2004. — 142 с.
31. Основи митної справи : навч. посіб. / В.А. Аргунов, В.П. Батіг, Є.М. Березний та ін. ; за заг. ред. Ю.П. Соловкова, П.В. Пашка. — Х. : РА-Каравела, 2000. — 320 с.
32. *Пашко П.В.* Митна безпека (теорія, методологія та практичні рекомендації) : монографія / П.В. Пашко. — О. : АТ “Пласке”, 2009. — 628 с., іл.
33. Руководство пользователя MD Office.
34. Руководство пользователя QD Professional.
35. *Ситник В.Ф.* Основи інформаційних систем : навч. посіб. / В.Ф. Ситник та ін. — 2-ге вид., переробл. і доповн. — К. : КНЕУ, 2001. — 420 с.
36. *Соколов А.В.* Защита от компьютерного терроризма : справ. пособие / А.В. Соколов, О.М. Степанюк. — СПб. : Арлит, 2002.
37. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум. — 4-е изд. — СПб. : Питер, 2003. — 992 с.
38. *Терещенко С.* Використання в митній справі системи аналізу та управління ризиком / С. Терещенко // Митниця. — 2006. — № 2 (15).
39. *Хомоненко А.Д.* Базы данных : учеб. для высш. учеб. завед. / А.Д. Хомоненко, В.М. Цыганков, М.Г. Мальцев ; под ред. А.Д. Хомоненко. — СПб. : КОРОНА-принт, 2000. — 416 с.
40. *Шуляк В.* Огляд комп'ютерної криптографії / В. Шуляк, В. Петров, Н. Савінова та ін. // Вісник АМСУ. — 2002. — № 4.

ОСНОВНІ ПОНЯТТЯ І ТЕРМІНИ

Автентифікація — процедура перевірки відповідності пред’явленого ідентифікатора об’єкта обчислювальної системи на предмет належності цьому об’єкту; встановлення або підтвердження автентичності.

Автоматизована інформаційна система управління організацією — взаємопов’язана сукупність даних, обладнання, програмних засобів, персоналу, стандартів процедур, призначених для збирання, опрацювання, розподілу, зберігання, видачі (надання) інформації відповідно до вимог, що впливають з діяльності організації.

Автоматизована інформаційна технологія — системно організована для виконання завдань управління сукупність методів і засобів збирання, реєстрації, передачі, накопичення, пошуку, опрацювання та захисту інформації на базі застосування розвинутого програмного забезпечення, засобів обчислювальної техніки і зв’язку, а також способів, за допомогою яких інформація пропонується клієнтам.

Автоматизована інформаційна технологія — комплекс методів і процедур, за допомогою яких реалізуються функції збирання, передавання, обробки, зберігання та доведення до

користувача інформації в організаційно-управлінських системах з використанням вибраного комплексу технічних засобів.

Автоматизована підсистема митного оформлення — складова ЄАІС ДМСУ, що вирішує завдання автоматизації діяльності митних органів у напрямках торгового й неторгового обігу.

Відкритий ключ — параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису.

Головний інформаційно-телекомунікаційний комплекс — це сукупність DNS-серверів, серверів Lotus Domino, пов'язаних між собою локальною обчислювальною мережею Департаменту інформаційних технологій і митної статистики (ДІТМС).

Дайджест повідомлення — унікальна послідовність символів, що однозначно відповідає змісту повідомлення. Зазвичай дайджест має фіксований розмір, наприклад, 128 або 168 біт, що не залежить від довжини самого повідомлення. Дайджест вводиться до складу електронного цифрового підпису разом з відомостями про автора і шифрується разом з ними.

Дані — інформація, подана у формалізованому вигляді, прийнятому для опрацювання автоматичними засобами за можливої участі людини (вхідні дані, вихідні дані, база даних тощо).

Документообіг — процес проходження документів усередині інформаційної системи: від джерела формування до використання в управлінні.

Документоорієнтована база даних — база даних слабо-структурованих об'єктів, в якій основною одиницею збереження інформації є окремий документ, що містить стільки полів і під поле виділяється стільки пам'яті, скільки необхідно для збереження конкретних даних.

Доступність — властивість ресурсу системи (комп'ютерної системи, послуги, об'єкта комп'ютерної системи, інформації), яка полягає в тому, що користувач і/або процес, який має відповідні повноваження, може використовувати ресурс згідно з правилами безпеки, не очікуючи довше заданого (малого) проміжку часу.

Електронна бібліотека — розподілена система, що дає змогу надійно зберігати й ефективно використовувати різноманітні колекції електронних документів за допомогою глобальних мереж передачі даних у зручному для кінцевого користувача вигляді.

Електронна митниця — багатофункціональна комплексна система, яка є в митних органах країни і поєднує інформаційно-комунікативні технології та сукупність механізмів їх застосування і дає можливість підвищити якість митного регулювання й удосконалити митне адміністрування для забезпечення митної безпеки держави.

Електронна передача грошових коштів (EFT — Electronic Funds Transfer) — система передачі фінансових (кредитних, платіжних) документів між клієнтами і банками, між банками, між банками та іншими фінансовими і комерційними організаціями.

Електронна пошта — система обміну й обробки повідомлень (сукупність електронних поштових скриньок, програмних засобів обробки, збереження і передачі повідомлень, термінальних станцій для підготовки та виведення повідомлень).

Електронне декларування — автоматизована система, орієнтована на реалізацію єдиного алгоритму автоматизованої обробки відомостей, що заявляються у ВМД, на рівні митних органів зі здійсненням автоматизованого форматно-логічного контролю, аналізу ризиків і виданням різноманітних застережень для посадових осіб митних органів, які здійснюють митний контроль і митне оформлення товарів, та запровадженням електронного документообігу між митними органами і суб'єктами ЗЕД з використанням механізму електронного цифрового підпису.

Електронний обмін даними — це міжкомп'ютерний обмін діловими, комерційними та фінансовими електронними документами.

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.

Єдина автоматизована інформаційна система (ЄАІС) ДМСУ — автоматизована інформаційна система, призначена для виконання функціональних завдань митних органів з використанням передових технологій обробки інформації за допомогою засобів обчислювальної техніки та телекомунікацій.

Загроза — будь-які обставини або події, що можуть бути причиною порушення безпеки інформації і/або нанесення збитків інформаційній системі.

Засвідчувальний центр центрального органу виконавчої влади — центр, визначений Кабінетом Міністрів України для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи центрів сертифікації ключів, які надають послуги електронного цифрового підпису цьому органу і підпорядкованим йому підприємствам, установам та організаціям.

Засіб електронного цифрового підпису — програмне і/чи апаратне забезпечення, призначене для генерації пари ключів (закритого і відкритого) та їх автоматизованого застосування під час шифрування або дешифрування електронного підпису.

Захист від несанкціонованого доступу — запобігання або істотне ускладнення несанкціонованого доступу до інформації.

Захист даних — апаратні та програмні засоби для запобігання втратам або порушенню цілісності даних.

Захист інформації в інформаційних системах — діяльність, спрямована на забезпечення безпеки в інформаційних системах інформації та інформаційної системи в цілому, що дає змогу запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки внаслідок реалізації загроз.

Зовнішньоекономічна діяльність (ЗЕД) — діяльність суб'єктів господарської діяльності України та іноземних суб'єктів господарської діяльності, яка побудована на взаємовідносинах між ними на території України та за її межами.

Ідентифікація — процедура присвоєння ідентифікатора об'єкту чи користувачу комп'ютерної системи або встановлення відповідності між об'єктом і його ідентифікатором; упізнання.

Інкотермс — офіційні правила Міжнародної торговельної палати для тлумачення торговельних термінів — полегшують ведення міжнародної торгівлі. Метою І. є забезпечення єдиного набору міжнародних правил для тлумачення найбільш уживаних торговельних термінів у зовнішній торгівлі. Таким чином можна уникнути або, щонайменше, значно скоротити невизначеності, пов'язані з неоднаковою інтерпретацією таких термінів у різних країнах.

Інформатизація — процес насичення виробництва й усіх сфер життя і діяльності людини інформацією.

Інформатика — наука, що вивчає властивості інформації, питання її збирання, зберігання, пошуку, опрацювання, перетворення, поширення і використання у різних сферах діяльності людини.

Інформаційна технологія — система методів і способів збирання, передачі, накопичення, опрацювання, зберігання, подання і використання інформації.

Інформаційне забезпечення — сукупність методів і засобів розміщення й організації інформації, що включають системи класифікації і кодування, уніфіковані системи документації, раціоналізації документообігу та форми документів, методів створення внутрішньомашинної інформаційної бази інформаційної системи.

Інформаційний ресурс — особливий вид ресурсу, що ґрунтується на ідеях і знаннях, нагромаджених у результаті науково-технічної діяльності людей, і поданий у формі, придатній для збирання, реалізації та відтворення.

Інформаційні ресурси спільного користування — сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання.

Інформаційно-аналітичне митне управління (ІАМУ) ДМСУ — спеціалізована митна установа щодо розробки, впровадження, супроводження та експлуатації ЄАІС ДМСУ.

Інформаційно-телекомунікаційний комплекс Державної митної служби України “Електронна пошта” — система,

що забезпечує інформаційний обмін у межах митної системи та ефективне функціонування автоматизованої системи митного оформлення.

Інформація — відомості про навколишній світ (об'єкти, явища, події, процеси тощо), які зменшують міру наявної невизначеності, неповноти знань, відчужені від їх творця і які стали повідомленнями (вираженими певною мовою у вигляді знаків, у тому числі записаними на матеріальному носії). Їх можна відтворювати шляхом передачі людьми усним, письмовим або іншими способами (за допомогою умовних сигналів, технічних та обчислювальних засобів тощо).

Керівна мережна служба (Managed Network Services) — мережна служба, яка виконує різні виробничі, адміністративні та службові функції управління об'єктами, технологічними лініями, транспортними системами і службовцями підприємств.

Ключ шифрування — набір параметрів (даних), необхідних для застосування методу шифрування.

Компрометація — порушення правил безпеки та несанкціоноване ознайомлення.

Конфіденційність інформації — властивість інформації, яка полягає в тому, що інформація не може бути отримана користувачем, який не має певних повноважень.

Крипостійкість — оцінка якості захисту та можливості відтворення зашифрованої інформації.

Легітимність — визначення правомірності.

Лінгвістичне забезпечення — сукупність мовних засобів, що використовуються на різних стадіях створення й експлуатації СОД для підвищення ефективності розробки і забезпечення спілкування людини та ЕОМ.

Метод шифрування — формальний алгоритм, що описує порядок перетворення вихідного повідомлення в результуюче.

Митна адміністративно-правова підсистема — складова ЄАІС ДМСУ, що забезпечує автоматизоване управління митними органами на всіх рівнях, контроль і дотримання законності під час автоматизованого митного оформлення.

Митна вартість товарів, які переміщуються через митний кордон України, — ціна, що була фактично сплачена

або підлягає сплаті за ці товари на момент перетину митного кордону, обчислена відповідно до положень Митного кодексу. Для визначення митної вартості встановлено єдині критерії: момент перетину митного кордону та ціна угоди (вартість, зазначена у рахунку-фактурі). Вона визначається декларантом відповідно до положень Кодексу. Методи визначення митної вартості товарів, які переміщуються через митний кордон України, та умови їх застосування встановлюються Кодексом.

Митна електронна інформація — сукупність даних і програм, яка підлягає або може підлягати обробці, передачі та збереженню засобами електронної обчислювальної техніки, незалежно від її фізичного й логічного подання, на кожному рівні структурного підрозділу митної системи України та яка містить відомості про роботу митних органів або стосується зовнішньоекономічної діяльності.

Митна зовнішня інформаційна підсистема — складова ЄАІС ДМСУ, що забезпечує електронний обмін інформацією ДМСУ з іншими організаціями України, іноземними державами і міждержавними організаціями, встановлює необхідний рівень повноважень доступу до ЄАІС і підтримує його.

Митна підсистема інформаційної безпеки — складова ЄАІС ДМСУ, що забезпечує контроль, оперативне управління функціонуванням і захист системи в цілому.

Митна телекомунікаційна підсистема — складова ЄАІС ДМСУ, яка є базовою транспортною системою і контролює маршрутизацію й роботу запитів (отримання повідомлень у глобальній мережі в он-лайн режимі й передачу повідомлень в оф-лайн режимі електронної пошти).

Несанкціонований доступ до інформації — доступ до інформації, що порушує правила доступу користувачів і процесів до об'єктів інформаційної системи.

Несиметричне шифрування — шифрування, за якого перетворення відкритого тексту на шифротекст виконується із застосуванням одного ключа, а перетворення шифротексту на відкритий текст — із застосуванням другого ключа.

Нова інформаційна технологія (комп'ютерна інформаційна технологія) — інформаційна технологія з "дружнім" інтерфейсом роботи користувача, що використовує персональ-

ні комп'ютери і телекомунікаційні засоби. Інструментарієм нової інформаційної технології є один або декілька взаємопов'язаних програмних продуктів для певного типу комп'ютера, технологія роботи в якому дає змогу досягти поставленої користувачем мети.

Онлайнні бази даних — бази даних, які цілодобово доступні в оперативному режимі з терміналів користувачів для діалогового пошуку інформації та видачі довідок і різних статистичних звітів.

Організаційні компоненти ІС — сукупність методів і засобів, що дають можливість удосконалити організаційну структуру об'єктів та управлінські функції, які виконуються структурними підрозділами; визначити штатний розклад і кількісний склад кожного структурного підрозділу; розробити посадові інструкції персоналу управління в умовах функціонування СОД.

Особистий ключ — параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Підписувач — особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа.

Посилений сертифікат відкритого ключа — сертифікат ключа, який видано акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом.

Правове забезпечення — сукупність правових норм, що регламентують створення і функціонування інформаційної системи. Правове забезпечення розробки інформаційної системи містить нормативні акти договірних взаємовідносин між замовником і розробником ІС, правове регулювання відхилень. Правове забезпечення функціонування СОД включає: умови надання юридичної чинності документам, отриманим із застосуванням обчислювальної техніки; права, обов'язки і відповідальність персоналу, в тому числі за своєчасність і точність опрацювання інформації; правила користування інформацією та порядок пов'язання суперечок щодо її достовірності.

Програмне забезпечення — сукупність програмних засобів для створення та експлуатації СОД засобами обчислювальної техніки. До складу програмного забезпечення входять базові (загальносистемні) та прикладні (спеціальні) програмні продукти. Базові програмні засоби необхідні для автоматизації взаємодії людини і комп'ютера, організації типових процедур опрацювання даних, контролю та діагностики функціонування технічних засобів СОД. Прикладне програмне забезпечення становить сукупність програмних продуктів, призначених для автоматизованого розв'язування функціональних завдань інформаційної системи.

Проникнення — успішне подолання механізмів захисту системи.

Регіональний інформаційно-телекомунікаційний комплекс — сукупність DNS-сервера та сервера Lotus Domino митного органу, пов'язаних між собою локальною обчислювальною мережею відповідного митного органу, спеціалізованої митної установи та організації.

Реплікація — створення спеціальних копій (реплік) бази даних, з якими користувачі можуть працювати одночасно на різних робочих станціях.

Санкціонований доступ до інформації — доступ до інформації, що не порушує правил доступу користувачів і процесів до об'єктів інформаційної системи.

Сертифікат відкритого ключа — документ, який засвідчує чинність і належність відкритого ключа підписувачу, виданий центром сертифікації ключів.

Симетричне шифрування — шифрування, за якого перетворення відкритого тексту на шифротекст і перетворення шифротексту на відкритий текст виконується із застосуванням одного ключа.

Система аналізу ризиків — автоматизована система, призначена для отримання митним органом необхідних даних про можливі ризики для спрямування контрольних ресурсів переважно до ділянок, на яких імовірність порушення законодавства України з питань митної справи є найвищою.

Система документації — сукупність взаємопов'язаних документів, що застосовуються у певній сфері діяльності.

Система опрацювання даних (СОД) — система, призначена для інформаційного обслуговування фахівців різних органів управління підприємства, що приймають управлінські рішення.

Система форматно-логічного контролю — автоматизована система, що забезпечує здійснення контролю за правильністю заповнення граф ВМД згідно з вимогами єдиного Порядку заповнення граф вантажної митної декларації відповідно до митних режимів, класифікаторів, що використовуються під час заповнення ВМД, та інших нормативно-правових актів шляхом аналізу відомостей, зазначених у ВМД і поданих документах, а також відповідність поданої до оформлення ВМД вимогам, установленим Специфікацією форматів електронних повідомлень.

Спостережливість — властивість комп'ютерної системи, що дає можливість фіксувати діяльність користувачів і процесів, використання об'єктів системи, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів для запобігання порушенню правил безпеки і/або забезпечення відповідальності за певні дії.

Телеметрична служба — система оперативного спостереження, дистанційного виміру і контролю за нерухомими та рухомими об'єктами.

Технічне забезпечення — комплекс технічних засобів, що застосовуються для функціонування системи опрацювання даних, містить пристрої, за допомогою яких виконуються типові операції опрацювання даних як поза ЕОМ (периферійні технічні засоби збирання, реєстрації, первинного опрацювання інформації, оргтехніка різного призначення, засоби телекомунікації та зв'язку), так і на ЕОМ різних класів.

Транспортна мережа супутникового зв'язку (ТМСЗ) Держмитслужби України — транспортна комунікаційна служба, призначена для організації високоякісного (швидкісного, надійного, достовірного) повнодоступного обміну будь-якою електронною інформацією між Держмитслужбою України, Департаментом інформаційних технологій та митної статистики і підрозділами митної служби (митницями, митними постами, відділами митних постів і спеціалізованими митницями) на всій території України.

Уніфікована система документації (УСД) — система документації, створена за єдиними правилами та вимогами, яка містить інформацію, необхідну для управління у певній сфері діяльності.

Уніфікована система зовнішньоторговельної документації — система документації, яка використовується для виконання завдань зовнішньоторговельної діяльності.

Уніфікована форма документа (УФД) — сукупність реквізитів, установлених відповідно до завдань у певній сфері діяльності та розташованих у певному порядку на носії інформації.

Фактурна (контрактна) вартість — ціна товару, зумовлена в контракті та відповідно в рахунку-фактурі.

Функціональні компоненти — система функцій управління або повний набір (комплекс) взаємопов'язаних у часі й просторі робіт з управління, необхідних для досягнення поставлених перед підприємством цілей.

Цифровий підпис — дані, одержані в результаті криптографічного перетворення блоку даних і/або його параметрів (хеш-функції, довжини, дати утворення, ідентифікатора відправника та ін.), що дають змогу приймальнику даних упевнитися в цілісності блока, справжності джерела даних і забезпечити захист від підробки та фальсифікації.

Цілісність інформації — властивість інформації, яка полягає в тому, що інформація не може бути модифікована користувачем, який не має певних повноважень.

Шифротекст — дані, отримані в результаті шифрування відкритого тексту.

Шифрування даних — процес перетворення відкритого тексту на шифротекст або процес перетворення шифротексту на відкритий текст.

Шлюз — устаткування, необхідне для з'єднання двох мереж різної архітектури, призначене для перетворення даних на відповідний формат під час переходу з однієї мережі в іншу, для перевірки повноважень користувачів та обліку використання ресурсів.

Lotus Domino та Notes — інтегрована система для колективної роботи, призначена для збирання, організації й розподілення інформації та знань.

Предметний покажчик

Lotus Domino та Notes, 94
Аутентифікація, 106
Автоматизована інформаційна система управління, 27
Автоматизована інформаційна технологія, 19
Автоматизована підсистема митного оформлення, 48
Віддалений користувач, 237
Відкритий ключ, 126
Головний інформаційно-телекомунікаційний комплекс, 236
Дайджест повідомлення, 158
Дані, 16
Документообіг, 52
Документоорієнтована база даних, 95
Доступність, 122
Електронна митниця, 312
Електронна передача грошових коштів (EFT — Electronic Funds Transfer), 64
Електронна пошта, 63
Електронне декларування, 314
Електронний обмін даними, 60
Електронний цифровий підпис, 126
Єдина автоматизована інформаційна система (ЄАІС) ДМСУ, 38
Загроза, 118
Засвідчувальний центр центрального органу виконавчої влади, 127, 134
Засіб електронного цифрового підпису, 139
Захист від несанкціонованого доступу, 123
Захист інформації в інформаційних системах, 118
Захист інформації, 105
Зовнішньоекономічна діяльність, 53
Ідентифікація, 148
Інформатизація, 15
Інформатика, 15
Інформаційна технологія, 19
Інформаційне забезпечення, 34
Інформаційний ресурс, 17
Інформаційні ресурси спільного користування, 246
Інформаційно-аналітичне митне управління (ІАМУ) ДМСУ, 46
Інформаційно-телекомунікаційний комплекс ДМСУ “Електронна пошта”, 235
Інформація, 14
Керівна мережна служба (Managed Network Services), 64
Ключ шифрування, 148
Компрометація, 130, 151
Конфіденційність інформації, 122
Користувач сторонньої організації, 237
Криптостійкість, 152

Лінгвістичне забезпечення, 35
Локальний користувач, 237
Метод шифрування, 151
Митна адміністративно-правова підсистема, 49
Митна електронна інформація, 244
Митна зовнішня інформаційна підсистема, 49
Митна підсистема інформаційної безпеки, 49
Митна телекомунікаційна підсистема, 49
Міжнародний стандарт електронного обміну даними, 60
EANCOM, 65
EDIFACT, 62
OBI, 64
Міжнародний стандарт електронної пошти X.400, 70
Несанкціонований доступ до інформації, 120
Несиметричне шифрування, 149
Нова інформаційна технологія, 21
Онлайнові бази даних, 63
Організаційні компоненти IC, 35
Особистий ключ, 126
Підписувач, 126
Посилений сертифікат відкритого ключа, 127
Правове забезпечення, 35
Програмне забезпечення, 35
Регіональний інформаційно-телекомунікаційний комплекс, 237
Реплікація, 97
Санкціонований доступ до інформації, 120
Сертифікат відкритого ключа, 126
Симетричне шифрування, 149
Система аналізу ризиків, 202, 328
Система документації, 53
Система опрацювання даних, 34
Система форматно-логічного контролю, 167
Спостережливість, 122
Телеметрична служба, 64
Технічне забезпечення, 35
Транспортна мережа супутникового зв'язку (ТМСЗ), 239
Українські стандарти електронного цифрового підпису, 144
Уніфікована система документації, 53
Уніфікована система зовнішньоторговельної документації, 53
Уніфікована форма документа, 53
Функціональні компоненти, 30
Цифровий підпис, 106
Цілісність інформації, 122
Шифрування даних, 106
Шлюз, 68
Шлюз адресний, 69
Шлюз протокольний, 69
Шлюз форматів, 69

Від авторів

Посібник призначено для курсантів, студентів і слухачів навчальних закладів митної служби України, а також для працівників митної служби, декларантів, керівників підприємств та організацій, державних службовців, підприємців. Може бути корисним для студентів і викладачів, які досліджують проблеми застосування сучасних інформаційних технологій у митній службі України.

Автори висловлюють щиру подяку за надані матеріали співробітникам митних органів України та Академії митної служби України, які значною мірою вплинули на формування концепції цієї книги.

Окрему подяку висловлюємо співробітникам Академії митної служби України В.В. Ченцову, О.П. Борисенку; Державного науково-дослідного інституту митної справи І.Г. Бережнюку; Регіональної інформаційної митниці М.В. Данильченко, К.В. Зарубіну, В.В. Страшку, М.В. Кузьменку, О.З. Флінті, І.В. Ємельяновій; Департаменту аналізу ризиків В.В. Буланій, С.С. Демченку, А.С. Жучкову; співробітникам Вадул-Сіретської та Луганської митниць В.Д. Семотюк та С.В. Пересипкіну за організаційну і технічну допомогу під час роботи над рукописом.

Навчальне видання

Серія “Митна справа в Україні”

*ВОЛИК Ольга Федорівна, ДОРДА Ірина Володимирівна,
КАЩЕЄВА Олена Віталіївна, КОПОСОВ Сергій Анатолійович,
НІКОЛАЙЧУК Олег Олександрович, ПАШКО Павло Володи-
рович, ПІСНОЙ Павло Якович, ШУЛЯК Валентин Петрович*

МИТНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Навчальний посібник

*В оформленні палітурки використані фото С. Орлова;
заставка “Інспектор-2006” (автор — С. Копосов).*

В Україні книгу можна придбати за адресами:

- м. Київ, вул. Стрілецька, 28 (вхід з двору), маг. “Абзац”, тел. (044)581-15-68, 238-82-66
- м. Луцьк, просп. Волі, 41, маг. “Знання”, тел. (0332)77-00-46
- м. Львів, пл. Галицька, 12, маг. “Глобус”, тел. (032)235-51-77
- м. Тернопіль, вул. Чорновола, 14, маг. “Книжкова хата”, тел. (0352)52-24-33
- м. Ужгород, пл. Корятовича, 1, маг. “Кобзар”, тел. (03122)3-35-16
- м. Харків, вул. Сумська, 51, маг. “Books”, тел. (057)714-04-70, 714-04-71
- м. Херсон, вул. Леніна, 14/16, маг. “Книжковий ряд”, тел. (0552)22-14-56
- м. Хмельницький, вул. Подільська, 25, маг. “Книжковий світ”, тел. (0382)79-25-59
- м. Черкаси, вул. Б. Вишневецького, 38, маг. “Світоч”, тел. (0472)36-03-37
- м. Чернівці, пл. Соборна, 1, маг. “Будинок книги та медіа”, тел. (0372)52-00-19
- м. Чернігів, просп. Миру, 45, маг. “Будинок книги”, тел. (04626)9-92-62

**Книготорговельним організаціям та оптовим покупцям
звертатися за тел.: (044) 537-63-61, 537-63-62; факс: 235-00-44.
E-mail: sales@znannia.com.ua**

Підп. до друку 05.10.2010. Формат 60×90 1/16. Папір офс. Друк офс.
Гарнітура SchoolBook. Ум. друк. арк. 24,5. Обл.-вид. арк. 23,5.
Тираж 500 прим. Зам. №

Видавництво “Знання”

01034, м. Київ, вул. Стрілецька, 28

Свідоцтво про внесення до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції ДК № 3596 від 05.10.2009.

Тел.: (044) 234-80-43, 234-23-36

E-mail: sales@znannia.com.ua <http://www.znannia.com.ua>