Національна академія наук України
Інститут проблем реєстрації інформації

О.В. Нестеренко

БЕЗПЕКА ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЕРЖАВНОЇ ВЛАДИ

ТЕХНОЛОГІЧНІ ОСНОВИ

Київ Наукова думка 2009

УДК 681.324

Нестеренко О.В. Безпека інформаційного простору державної влади: технологічні основи: Монографія. — К., Наук. думка, 2009. — 352 с.

Книга є своєрідним підсумком участі автора у розробці державної політики інформатизації країни, формуванні інфраструктури інформаційного простору державної влади та в створенні автоматизованих інформаційно-аналітичних систем органів влади. Викладено оцінки технологічних проблем інформаційної безпеки державної влади як складової національної безпеки держави з урахуванням складної обстановки у міжнародному інформаційному просторі, сучасних тенденцій вдосконалення державного управління та можливостей інформаційно-комунікаційних технологій.

Аналіз актуальних проблем інформатизації органів влади України за роки її незалежності доповнюється викладенням перспектив їхнього вирішення в найближчому майбутньому, зокрема стосовно розв'язання завдань зі створення системи «електронного уряду» з урахуванням забезпечення інформаційної безпеки.

Для фахівців з питань національної безпеки та держслужбовців, а також для експертів, науковців, викладачів і студентів, яких цікавлять проблеми інформаційних технологій та інформаційної безпеки.

Рецензенти:

О.Г. Додонов	Заслужений діяч науки і техніки України, доктор технічних наук, професор
Л.В. Скрипник	Заслужений діяч науки і техніки України, доктор технічних наук, професор
А.І. Семенченко	доктор наук з державного управління

Рекомендовано до видання Вченою радою Інституту проблем реєстрації інформації НАН України (протокол № 13 від 24.11. 2009 р.)

Редактор *С.Ю. Ноткіна*

ISBN 978-966-00-0933-X

З М І С Т

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 5
ВСТУП 7
РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМ РОЗВИТКУ ІНФРАСТРУКТУРИ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЕРЖАВНОЇ ВЛАДИ . . 11
1.1. Особливості функціонування та вдосконалення державної влади в сучасних умовах 11
1.2. Формування інфраструктури інформаційного простору державної влади 35
1.3. Загрози інформаційній безпеці державної влади. 45
Підсумки до розділу 65
РОЗДІЛ 2. ОСОБЛИВОСТІ СТВОРЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ. 67
2.1. Основні класи задач, що розв'язуються в органах влади, та їхнє інформаційне забезпечення 67
2.2. Автоматизовані системи в органах влади 73
2.3. Необхідні передумови побудови АІАС 104
Підсумки до розділу 118
РОЗДІЛ 3. ФОМАЛІЗАЦІЯ ТА МОДЕЛЮВАННЯ АІАС 120
3.1. Підходи до формалізації та моделювання АІАС 120
3.2. Концептуальні засади формалізації та моделювання АІАС 140
3.3. Визначення та аналіз інформаційних потоків в АІАС . . . 152
3.4. Методи визначення інформаційного навантаження в АІАС 167
Підсумки до розділу 175
РОЗДІЛ 4. АРХІТЕКТУРА АІАС ЯК ОСНОВНИХ СКЛАДОВИХ ІНФРАСТРУКТУРИ ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЕРЖАВНОЇ ВЛАДИ 177
4.1. Архітектурні стратегії 177
4.2. Архітектура АІАС 189
4.3. Оцінка ефективності архітектурних рішень 202
Підсумки до розділу 209

РОЗДІЛ 5. МЕТОДОЛОГІЯ СТВОРЕННЯ ТЕХНОЛОГІЧНИХ ПІДСИСТЕМ АІАС 210
5.1. Сучасні інформаційні технології автоматизації інформаційно-аналітичної діяльності 210
5.2. Основні вимоги до інформаційного забезпечення та систем зберігання даних в АІАС 225
5.3. Забезпечення електронного документообігу в органі державної влади 247
5.4. Підтримка функціональної діяльності та аналітичної роботи в АІАС 260
5.5. Основні вимоги до телекомунікаційного середовища АІАС 287
5.6. Вибір апаратного та програмного забезпечення АІАС . . 297
5.7. Організація захисту інформації та забезпечення живучості АІАС 308
Підсумки до розділу 328
ПІСЛЯМОВА 330
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 334

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АІАС	— автоматизована інформаційно-аналітична система
АРМ	— автоматизоване робоче місце
АСЕК	— автоматизована система експортного контролю
ВО	— виконавча обов'язковість
ВПМ	— віртуальні приватні мережі
ГІС	— геоінформаційна система
ДБД	— документальна база даних
ДКЗІ	— Державний комітет зв'язку та інформатизації України
ДСЕК	— Державна служба експортного контролю України
ЕД	— електронний документ
ЕДО	— електронний документообіг
ЕЦП	— електронний цифровий підпис
ЄДАПС	— Єдина державна автоматизована паспортна система
ЗПМ	— зростаюча пірамідальна мережа
ІАС	— інформаційно-аналітична система
ІАЦ	— інформаційно-аналітичний центр
ІБ	— інформаційна безпека
ІБД	— інтегрований банк даних
ІзОД	— інформація з обмеженим доступом
ІІАС	— інтегрована інформаційно-аналітична система
ІК	— інтеграційна компонента
ІКТ	— інформаційно-комунікаційні технології
ІІП	— інфраструктура інформаційного простору
ІР	— інформаційні ресурси
ІСЕУ	— інформаційна система електронного уряду
КЗЗ	— комплекс засобів захисту
КМУ	— Кабінет Міністрів України
КСЗІ	— комплексна система захисту інформації
ЛІОМ	— локальна інформаційно-обчислювальна мережа
ЛЛМ	— логіко-лінгвістична модель
МВС	— Міністерство внутрішніх справ України
МНС	— Міністерство України з питань надзвичайних ситуацій та в справах захисту населення від наслідків Чорнобильської катастрофи
НКРЗ	— Національна комісія з питань регулювання зв'язку України
НРІР	— Національний реєстр інформаційних ресурсів
НСКЗ	— Національна система конфіденційного зв'язку
ОДА	— обласна державна адміністрація
ОДВ	— орган державної влади
ПЗ	— програмне забезпечення
ПКД	— пункт колективного доступу до Інтернету

ПОД — проблемно-орієнтований додаток
САО — система аналітичних обчислень
СБУ — Служба безпеки України
СЗІ — система захисту інформації
СЕДО — система електронного документообігу
СІТС — спеціальна інформаційно-телекомунікаційна система
СКБД — система керування базою даних
СКМУ — Секретаріат Кабінету Міністрів України
СІР — система інформаційних ресурсів
СІРВ — система інформаційних ресурсів органів влади
СНІР — система національних інформаційних ресурсів
СППР — система підтримки прийняття рішень
ТС — телекомунікаційне середовище
УІАС НС — Урядова інформаційно-аналітична система з питань надзвичайних ситуацій
ЦЗО — центральний засвідчувальний орган

ВСТУП

Сучасний етап розвитку цивілізації пов'язаний із стрімким зростанням потужності технологій, глобалізацією, відкритістю діяльності, що стає визначальними чинниками розвитку економіки, науки, освіти. Одним з визначень суспільства, яке йде на зміну існуючому (поряд з такими, як постіндустріальне, інфраструктурне, глобальне), є ***інформаційне суспільство***. У новому суспільстві завдяки розвитку Інтернету та засобів зв'язку, широкому використанню ***інформаційно-комунікаційних технологій*** (ІКТ) суттєво збільшується інтенсивність інформаційного обміну, а основним типом діяльності має стати обробка інформації та генерування нового знання.

В інформаційному суспільстві зазнають суттєвих змін соціальна структура суспільства та ринок робочих місць, економічні відношення та виробництво, форми прийняття політичних рішень, транснаціональних відносин і критерії розвитку. Вже зараз світ підійшов до тієї межі, коли кордони між державами перестали бути нездоланними бар'єрами для багатьох видів діяльності. На жаль, це стосується й таких небезпечних явищ як тероризм і злочинність, поширення зловживань у фінансовій сфері, порушення етичних і моральних норм життя. ІКТ стали вже невід'ємними елементами більшості застосувань, забезпечення функціонування яких значною мірою пов'язане із доступністю та ефективністю інформаційно-телекомунікаційних послуг. Обумовлена цими обставинами відкритість, взаємозалежність технологій та сфер діяльності веде до потенційної уразливості, техногенної небезпеки. Насамперед це стосується так званих, с точки зору національної безпеки, критичних інфраструктур суспільства — енергетичних систем, інженерної інфраструктури, систем транспортування ресурсів, особливо в надзвичайних ситуаціях.Усе це свідчить про наявність трансформацій безпекового інфор-маційного середовища в Україні й навколо неї, а, отже, і про відставання або навіть певну вичерпаність чинних донині підходів до забезпечення інформаційної безпеки держави.

Тому вищевказані проблеми набули особливої гостроти, і їхнє вирішення перейшло в розряд життєво-необхідних, а економічні, соціальні, науково-технічні, військові й політичні наслідки цих процесів обґрунтовано викликають занепокоєння. Про це свідчать і Укази Президента України «Про Стратегію національної безпеки України» від 12 лютого 2007 року № 105/2007, від 23 квітня 2008 року № 377/2008 «Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року «Про невідкладні заходи щодо забезпечення інформа-

ційної безпеки України» та від 8 липня 2009 року № 514/2009 «Про Доктрину інформаційної безпеки України».

Стратегія національної безпеки України окреслює пріоритети та напрями діяльності держави у сфері національної безпеки, серед головних з яких вказується ***підвищення ефективності системи державного управління та місцевого самоврядування.*** Фактично стратегія є системою координат для оцінки ефективності діяльності органів державної влади.

Одним із критеріїв оцінки цієї ефективності в сучасних умовах є такий новий виклик у демократизації відносин між владою і суспільством, утвердженні пріоритету прав і свобод громадянина, зростанні громадської довіри до влади, як ***відкритість уряду***, забезпечення вільного доступу громадськості до рішень та інформаційних ресурсів органів державної влади. Особливого значення у зв'язку із цим набуває формування в країні системи «***електронного урядування***».

Сучасний стан проникнення ІКТ у суспільні інституції дозволяє говорити про рівень ***інформатизації*** різних сфер людської діяльності як реалізації комплексу заходів, що спрямовані на забезпечення повного і своєчасного використання вірогідних інформації та знань. Аналіз світового досвіду засвідчує, що інформатизація в розвинених країнах стала важливою галуззю економіки та визначальною сферою суспільного життя, дозволяючи, у тому числі, забезпечувати ефективне державне, адміністративне й господарське управління.

У зв'язку із цим особливого значення набуває використання нових інформаційних технологій для підтримки ***інформаційно-аналітичної діяльності*** органів державної влади та створення в них відповідних ***автоматизованих інформаційно-аналітичних систем*** (АІАС) як головних складових інфраструктури інформаційного простору державної влади.

Про це свідчить досвід багатьох країн, зокрема, США, Канади, Німеччини, Естонії, Росії, ініціативи щодо формування інфраструктури інформаційного простору урядів країн Європейського Союзу та Співдружності Незалежних Держав.

Інформатизація органів державної влади дозволяє зробити реальністю й формування та розвиток ***інфраструктури інформаційного простору державної влади***, що в сучасних умовах стає безпосереднім чинником не лише економічного зростання, соціально-політичної стабільності та розвитку демократичних засад в управлінні державою, а й забезпечення національної безпеки. Стаття 17 Конституції України за-

значає: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави...».

Для України, яка знаходиться на шляху унезалежнення, постання самостійної, незалежної та автономної держави, питання інформатизації органів влади, формування інформаційної і аналітичної бази для прийняття управлінських рішень на державному рівні, забезпечення інформаційної безпеки є особливо актуальними. У Доктрині інформаційної безпеки України вказується, що «від обсягу, швидкості та якості обробки інформації значною мірою залежить ефективність управлінських рішень, зростає значення методів управління з використанням інформаційних технологій соціальними та економічними процесами, фінансовими і товарними потоками, аналізу та прогнозування розвитку внутрішнього і зовнішніх ринків. Але ефективність механізмів прийняття та виконання державних рішень все ще залишається недостатньою. Це зумовлено тривалою політичною нестабільністю, корумпованістю та непрофесіоналізмом державної служби, зрощенням бізнесу й політики, а також неефективністю створення та застосування автоматизованих інформаційних систем.

Значна увага до розвитку інфраструктури інформаційного простору держави, інформатизації органів влади, як з боку керівників країни, так і з боку науковців, фахівців з інформатики та користувачів — працівників органів державної влади, спричинила написання цієї книги. Вона присвячена розв'язанню важливої проблеми національної безпеки — розробки методологічних і технологічних основ синтезу й проектування автоматизованих інформаційно-аналітичних систем органів державної влади як основи розвитку інфраструктури інформаційного простору державної влади України з необхідним рівнем інформаційної безпеки.

У розділі 1 на основі огляду літератури за темою проведено аналіз сучасних напрямів розвитку інфраструктури інформаційного простору державної влади, пов'язаних із удосконаленням державного управління, методів і технологій автоматизації інформаційно-аналітичної діяльності в органах державної влади, забезпечення необхідного рівня інформаційної безпеки державної влади; доводиться, що головними складовими інфраструктури інформаційного простору державної влади є автоматизовані інформаційно-аналітичні системи органів державної влади.

У розділі 2 проаналізовано існуючі підходи до створення автоматизованих систем в органах влади та забезпечення їхньої інформаційної

безпеки, визначено пов'язані із цим проблеми та необхідні передумови побудови АІАС.

У розділі 3 проведено аналіз та оцінку підходів, визначено концептуальні засади формалізації та моделювання АІАС, а також дано визначення архітектури АІАС.

У розділі 4 здійснено інформаційне моделювання АІАС, запропоновано методи визначення інформаційних потоків та інформаційного навантаження в системі.

У розділі 5 запропоновано методологію створення технологічних підсистем АІАС, у тому числі щодо забезпечення захисту інформації та живучості АІАС.

Тематика книги тісно пов'язана із завданнями та проектами Національної програми інформатизації (розділи «Формування і розвиток національної інфраструктури інформатизації», «Інформатизація стратегічних напрямів розвитку державності, безпеки та оборони»), а також із результатами науково-дослідних робіт, що в різні роки проводилися за участю автора Інститутом кібернетики імені В.М. Глушкова НАН України, Інститутом проблем реєстрації інформації НАН України, Інститутом проблем математичних машин та систем НАН України, Інститутом телекомунікацій та глобального інформаційного простору НАН України, ВАТ «КП ОТІ», компанією «Єр-Джи-дата Україна», компанією «Софтлайн», іншими організаціями, що здійснюють розробки в сфері ІТ на замовлення органів влади.

РОЗДІЛ 1

АНАЛІЗ ПРОБЛЕМ РОЗВИТКУ ІНФРАСТРУКТУРИ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЕРЖАВНОЇ ВЛАДИ

1.1. Особливості функціонування та вдосконалення державної влади в сучасних умовах

Питання державного управління. Держава належить до політичної надбудови економічної структури суспільства, яка є реальним його базисом. При цьому термін «держава» в юридичній та іншій науковій літературі тлумачиться по-різному. Перш за все його розглядають в субстанціональному (організація в певні корпорації населення), атрибутивному (устрій певних суспільних відносин), міжнародному (як єдність території і населення) і інституціональному значенні [1–6]. Під останнім розуміється апарат публічної влади, державно-правові органи, що здійснюють державну владу.

Державна влада виконує роль арбітра у відносинах між різними соціальними верствами суспільства, пом'якшує їхнє протиборство, здійснює «спільні справи». Державна влада наділена владними повноваженнями, обсяг яких, як правило, визначається конституцією держави та законами. Органи державної влади — складова частина державного механізму, спеціальний апарат управління та примусу.

Орган державної влади (ОДВ) є державною установою, діяльність якого забезпечують посадові та службові особи, які працюють на професійних засадах, можуть здійснювати юридично чинні дії та мають спеціальний статус державного службовця й організаційної структури, що забезпечують реалізацію організаційних і технологічних процесів із підготовки та прийняття державних рішень (опрацювання документів, підготовка нормативних актів), взаємодії із зовнішнім середовищем (обслуговування запитів населення та підприємств, засобів масової інформації, міжнародне співробітництво) та ін.

Організація та діяльність органів державної влади в Україні здійснюється за принципом народного суверенітету, одним з елементів якого є поділ державної влади на законодавчу, виконавчу, судову. Окреме місце в системі органів державної влади належить Президенту України та органам прокуратури.

Створення сучасної, ефективної системи державної влади є важливим чинником становлення України як розвинутої, правової, цивілізованої, європейської держави з високим рівнем життя, соціальної стабільності, культури, демократії.

Політологи вважають, що державна влада — це державна організація політичного управління суспільством, яка як за обсягом, так і за засобами впливу перевищує всі інші різновиди влади в усіх соціальних утвореннях. Вона поширюється на всі сфери суспільного життя, здійснюється за допомогою спеціального апарату примусу або переконання та володіє монопольним правом видавати загальнообов'язкові нормативно-правові акти [7]. За своєю суттю, державна влада — це легітимне офіційне волевиявлення держави, її органів і посадових осіб, що представляє собою здійснення влади народу [8].

Державна влада, в кінцевому розумінні, — не панування осіб, які наділені нею, а служіння цих осіб на користь спільного блага: для організації та консолідації суспільства і нації, для створення необхідних умов для економічного й політичного розвитку.

Основними компонентами влади є її суб'єкт, об'єкт, засоби (ресурси) і процес, що приводить до руху всі її елементи (механізм і засоби взаємодії суб'єкта і об'єкта). Влада — це завжди двостороння взаємодія суб'єкта і об'єкта.

Держава постійно змушена виробляти та ухвалювати ті або інші ***рішення*** з метою впливу на керовані об'єкти. Механізм ухвалення рішень у будь-якій галузі державної діяльності є необхідним елементом і включає низку послідовних дій, організацій, органів і конкретних осіб, які є суб'єктами влади. До них належать офіційні посадови особи, котрі юридично відповідають за прийняті рішення, а також ті, хто забезпечує інформацією, необхідною для опрацювання рішень, та ті, хто забезпечує вибір альтернативних рішень.

За сферами діяльності держави її основні функції поділяються на внутрішні і зовнішні. Внутрішні здійснюються у межах держави, бо в них виявляється внутрішня політика. До цієї групи належать такі функції, як регулювання економічних відносин, охорона прав і свобод людини і громадянина, правопорядок, законність, соціальне обслуговування населення, охорона та раціональне використання природних ресурсів тощо. Зовнішні функції забезпечують здійснення зовнішньої політики держави. До них належать оборона країни, підтримання міжнародного миру, міжнародне економічне співробітництво тощо.

Таким чином, можна зробити висновок, що державна влада є *складною соціальною системою*, пов'язаною специфічними відносинами з багатьма об'єктами зовнішнього середовища. Якщо використати поняття та визначення складної системи, то можна сказати, що державна влада — це цілеспрямована система із взаємозалежними функціональними елементами (підсистемами управління, об'єктами управління і т.д.), розподіленими по рівнях, між якими в певному сенсі встановлені відношення співпідпорядкованості. У свою чергу, по суті справи, система державної влади є елементом соціальної метаструктури.

Вочевидь, система державної влади є ***динамічною системою, що розвивається,*** адже можна стверджувати, що значення її вихідних параметрів у будь-який момент часу не залежать виключно від поточного значення вхідних впливів і стану, з якого почалась еволюція системи. Один з суспільних законів неперервного прискорення соціального розвитку людини та суспільства як систем, що розвиваються, дає змогу представляти розвиток людської спільноти як природний історичний процес [9].

Нарешті, державна влада є *інформаційною системою* у широкому розумінні, основним типом діяльності якої є збирання та опрацювання інформації і генерування нової інформації, нового знання, що перш за все виявляється у підготовці державних рішень.

Сучасні тенденції вдосконалення державної влади. Складність, динамізм, цілеспрямованість державної влади як системи, залежність від значної кількості чинників зовнішнього середовища обумовлюють нестабільність її функціонування та розвитку, що веде до періодів розквіту, високої ефективності діяльності та спаду і навіть кризи. Так, у 80-х – 90-х роках XX ст. державне управління в країнах світу перебувало в кризовому стані під впливом таких факторів, як фінансовий тиск і бюджетний дефіцит (через урядові витрати і хиби оподаткування), глобалізація ринків і конкуренція за отримання інвестицій, надмірне державне регулювання, помилки в розробці та впровадженні державної політики, зменшення довіри та поваги населення до уряду з одночасним зростанням очікувань щодо якості державних послуг.

Водночас в останню третину XX століття людство вступило до нової фази свого розвитку — суспільство ризику[1]. Суспільство ризику — це постіндустріальна формація суспільства, головна з особливостей

[1] Соціологічна теорія сучасного суспільства, автором якої є німецький вчений Ульріх Бек.

якої полягає в тому, що коли для індустріального суспільства характерний розподіл благ, то для суспільства ризику — розподіл загроз різного походження й зумовлених ними ризиків. При цьому основу ризиків становлять загрози, спричинені передусім техносферою, а ядром цієї динаміки є соціальне протиріччя між існуванням високорозвинутих бюрократій, які займаються проблемами безпеки, і відкритої легалізації раніше небачених, вельми масштабних загроз, без можливості впоратися з їхніми наслідками. Квінтесенцією цих протиріч стали терористичні акти 11 вересня 2001 р., після яких світ суттєво змінився у ставленні до найважливіших умов забезпечення розвитку суспільства.

Ці процеси теж стали важливими чинниками переходу державного управління до кризового стану.

Що ж узагалі розділяє різни етапи розвитку влади, що є основним критерієм ефективності для державного управління? Як її визначити? Якими шляхами має вдосконалюватись влада? Ці питання є дуже непростими. Суттєвим критерієм може бути, наприклад, розквіт держави. Але в чому він полягає? Чи можна його об'єктивно виміряти? Існує концепція забезпечення сталого розвитку, якій останніми роками фахівцями багатьох країн світу приділяється значна увага, а наріжним каменем якої є оцінка розвитку держави, що базується на граничних значеннях. Одначе така оцінка є досить загальною і визначає лише основні напрями, за якими мають вживатись владою додаткові заходи.

Інший критерій, що також може бути взятий за основу, є так званий «індекс людського розвитку», який успішно використовується різними міжнародними організаціями для порівняння глобального розвитку країн нашої планети, зокрема, у щорічних звітах Програми розвитку Організації Об'єднаних Націй (ПРООН) у рамках стратегії сталого розвитку. Але цей критерій є дуже складним завдяки урахуванню сотень характеристик людського існування в державі, серед яких такі групи індикаторів, як забезпеченість людськими ресурсами, інтелектуальний розвиток суспільства, соціально-правова захищеність населення тощо [10–12]. Він також визначає напрями посилення діяльності, але більш деталізовано.

З критеріями пов'язані цілі державного управління як ідеальний образ (логічна модель) бачення стану сфер управління, сформульований на основі аналізу та врахування їхніх об'єктивних закономірностей і організаційних норм, потреб та інтересів. Виходячи з того, що головним для державного управління є принцип створення, підтримки й поліпшення умов для вільної, спокійної, творчої життєдіяльності людей, пріоритети потреб та інтересів розвитку суспільства вибудовують цілі

державного управління в певну ієрархію, що визначається соціологічним наповненням цілей і співвідношенням між дійсними можливостями та ідеальним образом.

Певні системоутворюючі моменти розробці цілей для державного управління, до яких відносяться суспільні джерела появи та фіксації цілей державного управління, суб'єктивний бік цілепокладання, відносність і прозорість сформульованих цілей, а також невідомість, ймовірність майбутнього обумовлюють реальні складнощі формування цілей [13]. Тому «живлющою силою» дерева цілей державного управління є ***інформація*** з усієї сукупності явищ, що впливають (рис. 1.1).

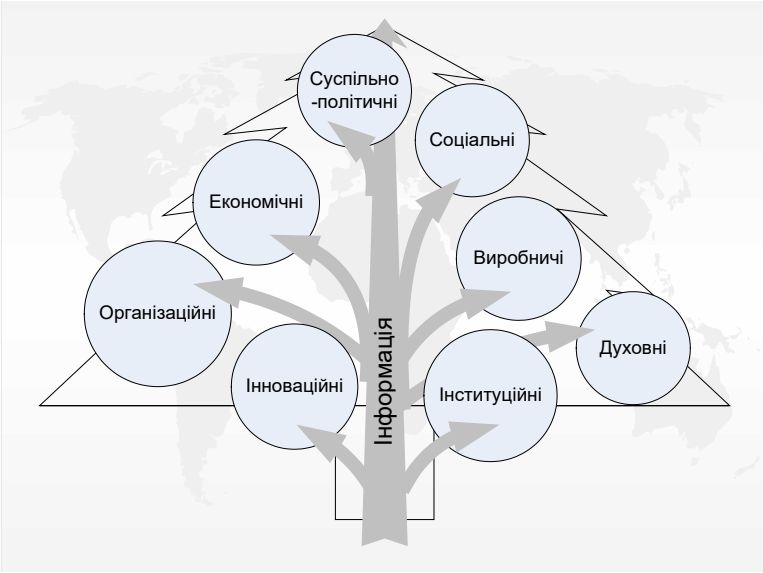

Рис. 1.1. Дерево цілей державного управління

У пошуках нових шляхів виходу з кризи кінця XX ст. уряди та суспільства розпочали взагалі перегляд встановлених канонів організації діяльності владних інституцій. Унаслідок цього низка країн почала використовувати підходи приватного сектору (менеджеризм Пітерса і Уотермена)[2], крупних бізнес-структур, розвивати партнерство з неурядовими організаціями, утворювати нові структури, такі як агенції і корпо-

[2] Т. Питерс, Р. Уотермен. В поисках эффективного управления, 1982 г.

рації, застосовувати пошук зовнішніх джерел, поширювати надання державних послуг та ін. Серед них важливе місце зайняв і поступ в ***інформаційних технологіях (ІТ)***.

У цьому зв'язку отримали розвитку, як піонерські, різні моделі реформ — у Новій Зеландії, Великобританії, США, Канаді. Спільною рисою цих моделей є те, що відомі ідеологи і практики цих реформ К. Гуд, Д. Осборн, Т. Геблер сформулювали як «новий державний менеджмент», який передбачає необхідність оцінювати урядові організації, згідно з їхньою суттєвістю, потреби в свободі управління, прагненні отримати кінцевий продукт (результат), здатності державного сектору конкурувати з приватним сектором у наданні послуг населенню [14].

Об'єднуючим і головним чинником указаних моделей стала ***інформаційна відкритість*** для чиновників. Утвердження пріоритету прав і свобод громадянина, неупередженість у ставленні до громадян, — у цьому, власне, найкраще проявляється сутність нової державної політики щодо демократизації відносин між владою і суспільством, зростання громадської довіри до влади [15–21].

Перший сучасний закон про відкритість уряду був прийнятий у США ще в 1966 р. Ним користувалися в основному адвокати, журналісти й співробітники посольств. Концепція інформаційної відкритості уряду має на увазі доступ громадян до всіх документів, що генеруються державою, аж до міжвідомчого листування, за винятком державної таємниці й паперів службового користування. За цей час інформаційна відкритість урядів отримала значного розвитку, впритул до таких підходів, що можуть здатися абсурдними. Наприклад, у Данії будь-який журналіст має право прийти в канцелярію прем'єр-міністра й переглянути все його ділове листування.

Насправді відкритість влади — не самоціль, а один з головних напрямів перебудови державного управління з метою його вдосконалення. І особливо гостро це питання постає у країнах, що відмовилися від тоталітарного минулого. Як зазначено у низці міжнародних документів[3] причинами бідності в цих країнах є неефективне урядування (*bad governance*), для якого характерним є непрозорість, корумпованість, залежність від тіньового капіталу. В цих обставинах особливо значущими стають якісний державний фінансовий менеджмент, прозорість державних закупівель, контроль і підзвітність при виконанні урядом своїх зо-

[3] Наприклад, у Eliminating World Poverty: Making Globalisation Work for the Poor. White Paper on International Development, London, 2000.

бов'язань. У розвитку цих компонентів якісного, ефективного державного управління неможливо переоцінити роль інформаційних технологій[4].

Адже дуже важливою особливістю нинішнього етапу розвитку суспільства є те, що у галузях виробництва, торгівлі, сферах надання послуг, банківської та фінансової, у нормативно-правової й законодавчої діяльності постійно наростають потоки інформації, що набувають характеру масовості [22]. Завдяки стрімкому розвитку ***інформаційно-комунікаційних технологій (ІКТ)***, зростанню кількості ринків послуг з їхнім використанням, ІКТ стали вже невід'ємними елементами більшості застосувань, забезпечення функціонування яких значною мірою пов'язане із доступністю та ефективністю цих послуг.

Враховуючи надзвичайно високий ступень інтеграції багатьох технологій, у першу чергу інформаційних, у всіх сферах людської діяльності, однією з найголовніших умов підвищення ефективності державного управління стає врахування викликів переходу до нової постіндустріальної форми суспільства — ***інформаційного суспільства***[5], що відбувається вже в наш час у багатьох країнах світу і, власне, й в Україні.

Концепція постіндустріального суспільства як загальносоціологічної теорії розвитку досить глибоко розроблена західними дослідниками. Один з апологетів цієї концепції французький економіст і соціолог, прихильник технологічного детермінізму Ж. Фураст'є (Fourastie) визначав постіндустріальне суспільство як «цивілізація послуг», тобто розвиток широкого спектра послуг на основі використання ІКТ (*e-Services*). При цьому одним з критеріїв переходу суспільства до інформаційної стадії розвитку може служити такий показник — якщо в суспільстві більше 50 % населення зайнято в сфері інформаційних послуг, суспільство стало інформаційним.

Підсумковими документами Всесвітнього самміту з питань інформаційного суспільства (Женева 2003 р. – Туніс 2005 р.), серед ключових принципів побудови інформаційного суспільства, орієнтованого на інтереси людей, визнається, що державні органи грають важливу роль і несуть відповідальність за розвиток інформаційного суспільства і, в належних випадках, за процеси прийняття рішень. Загальний, повсюд-

[4] За словами колишнього міністру інформаційних технологій і зв'язку РФ Леоніда Реймана, «інформаційні технології є єдиним способом скоротити відстань між людиною й урядом».

[5] http://www.itu.int/wsis

ний, рівноправний і прийнятний за ціною доступ до інфраструктури та послуг ІКТ складає одну з задач інформаційного суспільства.

Питання ефективності діяльності владних структур, їхньої взаємодії між собою та з населенням при вирішенні різних проблем життя країни — соціально-політичних, економічних, оборонних, інформаційних тощо, в інтересах держави, суспільства й особи, вочевидь, тісно пов'язані з поняттям безпеки, що у широкому, філософському розумінні трактується як надійність існування соціальної системи [23], а також з парадигмою ***національної безпеки***, згідно з якою в Україні, як і в інших демократичних державах, як основоположний компонент національної безпеки все більше сприймається безпека особи, і в цьому зв'язку як необхідність виникає вирішення проблем співвідношення безпеки особи та суспільної безпеки, безпеки особи та державної безпеки. Відповідно до ст. 4 Закону України «Про основи національної безпеки» суб'єктами забезпечення національної безпеки є практично всі владні структури — починаючи від Президента України і закінчуючи місцевими державними адміністраціями та органами місцевого самоврядування.

Останнім часом, враховуючи вищевказані тенденції, все більш істотне місце починають займати питання забезпечення ***інформаційної безпеки (ІБ)*** держави. Забезпечення ІБ інфраструктури, організацій і громадян (*e-Safety*) є одним з основних напрямів розбудови інформаційного суспільства. При цьому інформаційна безпека в сучасному постіндустріальному світі, в якому саме та чи інша інформація впливає на прийняття державою тактичних і стратегічних рішень, вважається основою національної безпеки.

Кофі Аннан у бутність Генеральним секретарем ООН у своїй заяві із приводу проголошення 17 травня Міжнародним днем інформаційного суспільства відзначив важливість підвищення довіри користувачів до ІКТ[6]. Він підкреслив, що в сучасному світі, обкутаному одною загальною мережею, у суспільства з'явилося багато загроз, серед яких і навмисні атаки на важливі інформаційні об'єкти, що веде до ослаблення економіки й суспільства в цілому. Для того, щоб підвищити довіру до електронної торгівлі, до електронних банківських систем, до телемедицини, до електронного уряду, необхідна загальна згуртованість у питаннях інформаційної безпеки на міжнародному рівні. І оскільки це залежить від політики безпеки кожної країни, бізнесу й кожного грома-

[6] Резолюція A/RES/60/252 Генеральної Асамблеї ООН від 27 березня 2006 р.

дянина, необхідно розвивати культуру інфобезпеки на міжнародному рівні.

Враховуючи актуальність і важливість питань безпеки інформаційної інфраструктури та запобігання комп'ютерних злочинів на шляху просування країн Європи до інформаційного суспільства Європейська комісія ще в рамках підготовки плану дій програми «*e*Europe–2002» сформувала спеціальне послання до комітетів комісії та широкої спільноти для обговорення та внесення відповідних заходів до вказаного плану[7].

Слід зазначити, що лише оснащене інформаційними технологіями суспільство є слабо захищеним і мало здатне до запобігання кризовим ситуаціям. У цьому зв'язку російський академік М. Моісєєв у своїй книзі «Универсум. Информация. Общество» відзначав, що планетарне суспільство можна буде називати інформаційним лише тоді, коли виникне Колективний Розум, здатний грати в цьому суспільстві таку ж роль, яку в організмі людини відіграє його власний розум. Ця концепція перекликається з необхідністю вибору нової парадигми ноосферізації, основи якої були закладені нашим вченим В.І. Вернадським, — розумної загальнопланетарної суспільної соціально-економічної облаштованості, що веде всі країни до монополярного світу, яка є інтернаціоналізацією, що не створює конфліктів, що є ключем до досягнення миру.

Дійсно, відповідно до механізму гомеостазу розум не запрограмований на завдання шкоди власному організмові. Одначе вбачається, що до епохи Колективного Розуму, навіть в окремо взятій державі, ще чимало води спливе, тому можна стверджувати, що питання безпеки в умовах поширення ІКТ ще довго буде залишатися актуальним.

Що ж стосується України, то аналіз ситуації свідчить про суттєву зміну безпекового середовища в країні й навколо неї, а, отже, і про певну вичерпаність чинних донині підходів до управління національною безпекою [24–27]. Попри існуючі позитивні зрушення, український сектор безпеки досі перебуває на ранній стадії трансформації культури безпеки[8], зокрема інформаційної.

---

[7] Creating a safer information society by improving the security of information infrastructures and combating computer-related crime / Communication from the Commission to the council, the European parliament, the Economic and Social committee and the Committee of the regions. — Brussels, 26.1.2001, Com(2000) 890 final.

[8] Документ «Аналіз української політики безпеки наприкінці 2006 року: критичний огляд», що підготували експерти Міжнародного центру перспективних досліджень (МЦПД) у рамках проекту «Кампанія з підвищення громадської обізнаності щодо державної політики у сфері безпеки та оборони».

Як приклад можна вказати, що дотепер існує переконання, що інформацію потрібно тримати в секреті, тоді як демократичний підхід полягає в тому, що інформацію треба піддавати розголосу, хіба що існують очевидні причини не робити цього з огляду на безпеку. На думку академіка Національної академії наук України М.В. Поповича, «інформаційний простір знаходиться, так би мовити, вище простору політичних інтересів, і забороняти в ньому можна тільки дезінформацію або приховування інформації». Водночас, «проблема узгодження свободи поширення інформації з національними інтересами, вираженими в певних нормах, залишається»[9].

Вочевидь, підвищення ефективності державної влади й в Україні перш за все залежить від рівня її взаємодії з громадянами і підприємствами, якості виконання власних функцій кожною державною установою, ефективності та оперативності взаємодії органів влади між собою. На це спрямована й низка державних нормативних документів.

У Стратегії національної безпеки України, затвердженої Указом Президента України від 12 лютого 2007 року № 105/2007, до головних пріоритетів та напрямів діяльності держави у сфері національної безпеки віднесено ***підвищення ефективності системи державного управління та місцевого самоврядування***.

Системою стандартів державної служби як оцінка ефективності роботи державних служб і державного сектора в цілому значною мірою визнається відкритість влади.

На реалізацію цих положень спрямовані й Закон України «Про ратифікацію Конвенції про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля» від 6 липня 1999 року й Укази Президента України «Про підготовку пропозицій щодо забезпечення гласності та відкритості діяльності органів державної влади» № 587/2002 від 27 червня 2002 року та «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади» № 683/2002 від 1 серпня 2002 року, а також інші нормативні акти.

Одначе влітку 2007 року в опитуванні Центру ім. О. Разумкова громадян України на питання «Назвіть, будь ласка, найбільш серйозні, на вашу думку, суспільно-політичні проблеми країни, що потребують першочергового вирішення» із запропонованих проблем на проблему

[9] «Національна культура з погляду національної безпеки» у щокв. наук. зб. «Національна безпека: український вимір», 2009. — Вип. 3 (22).

«Байдужість влади до думки громадян» зреагувало 58,2 % респондентів, а на проблему «Відсутність механізмів впливу простих громадян на прийняття рішень» вказало 29,4 %, тобто в цілому переважна кількість опитуваних. Ці дані свідчать про помітне відставання країни від реалізації парадигми відкритості влади та, відповідно, про значну актуальність цього питання для України.

Серед низки чинників, що впливають на таке становище, а саме: відсутність чіткого розуміння головних загроз, міжвідомчої співпраці, політичної волі верховних керівників, одне з головних місць — у контексті теми нашого розгляду — займає неадекватна оцінка розвитку та масштабів застосувань ІКТ і доступу до інформації, що знаходиться в державних комп'ютерних (автоматизованих) системах, та утворюють інфраструктуру інформаційного простору влади.

«Електронізація» уряду та суспільства. Отже, серед головних чинників, що в сучасних умовах впливають на державну владу та які визначились на початку нового тисячоліття, є вимога адаптації до нових викликів, які полягають у переході від прямого управління до виконання регулюючих функцій та здійсненні стратегічного планування, у здатності ефективно реагувати на запити та пропозиції населення та бізнесових структур, на розвиток технологій, на будь-які несподівані зміни, особливо в умовах складної міжнародної обстановки та загроз національній безпеці, а також передбачати ці зміни і, опанувавши, управляти ними (рис. 1.2).

Рис. 1.2. Чинники, що в сучасних умовах впливають на державну владу

У процесах наближення нашої країни до інформаційного суспільства важливе місце займає національна інформаційна стратегія, яка знайшла своє відображення у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», що направлена на формування «Електронної України» (*е*-Україна) [28]. У рамках цієї стратегії важливого значення для вдосконалення державної влади має відігравати інформаційна система ***«електронний уряд»*** (*е*-уряд) [29, 30].

Концепцію адаптації інституту державної служби в Україні до стандартів Європейського Союзу, *затвердженою* указом Президента України від 5 березня 2004 року № 278/2004, висувається вимога нормативного визначення поняття «державні послуги». У межах компетенції кожного органу державної влади необхідно на рівні стандартів визначити обсяг державних послуг, порядок надання та критерії оцінки їхньої якості, передбачивши запровадження відповідальності за порушення порядку надання таких послуг.

Процес оволодіння інформацією як ресурсом управління й розвитку за допомогою засобів ІКТ з метою створення інформаційного суспільства отримав назву «***інформатизація***». Процеси інформатизації суспільства як науки є предметом вивчення соціальної інформатики[10]. Соціальна інформатика відіграє методологічну роль для так званих галузевих інформатик: економічної, правової, соціологічної й інших. У цьому зв'язку вбачається, що до вказаного переліку доцільно включити й такий важливий напрямок, як ***інформатика державної влади***.

Отже, питання ефективності державного управління в сучасних умовах суттєво пов'язано з рівнем інформатизації органів влади. Ця стратегія для державної влади має дві головні складові. Перша — соціально-політична, що визначає вирішення проблем соціальної, правової, психологічної і моральної підготовки держслужбовців до виконання своїх обов'язків в умовах інформаційного суспільства. Друга — техніко-технологічна, яка пов'язана з запровадженням рішень щодо створення техніко-технологічної бази органів влади та суспільства за рахунок розвитку інформаційно-комунікаційної інфраструктури.

Відкритість влади може бути забезпечена реалізацією трьох складових: по-перше, веденням інформації про діяльність влади, по-друге, існуванням механізму, який би в автоматизованому режимі забезпечу-

[10] Під інформатикою розуміється система знань про виробництво, переробку, зберігання й поширення всіх видів інформації в суспільстві, природі й технічних пристроях.

вав громадськість інформацією, і, нарешті, налагодженою системою автоматизації відповідей влади на запитання й запити громадян. Згідно з викладеним, при реалізації цілей управління в сучасних умовах ОДВ мають вирішувати комплекс задач управління та забезпечення взаємодії з суспільством, використовуючи певні ***засоби автоматизації***.

Слід також при цьому звернути увагу й на те, що для забезпечення ефективного використання зазначених засобів держслужбовці мають суттєво підвищити власний рівень обізнаності з новими інформаційними технологіями. В умовах інформаційного суспільства, масової інформаційної просвіти на державну службу має приходити вже значною мірою підготовлена у цьому сенсі молодь [31, 32].

Використання нових інформаційних технологій дозволяє кардинально змінити взаємовідносини влади та громадян, якщо за основу береться нова концепція, що полягає у зміщенні акценту на обслуговування урядом населення (рис. 1.3). Таке бачення проблеми державного управління та пропозиції щодо її вирішення у вигляді «добропорядного управління» (good governance) уряд Європейського Союзу висловив у Білій книзі з європейського управління, що була представлена широкому загалу в 2001 р.

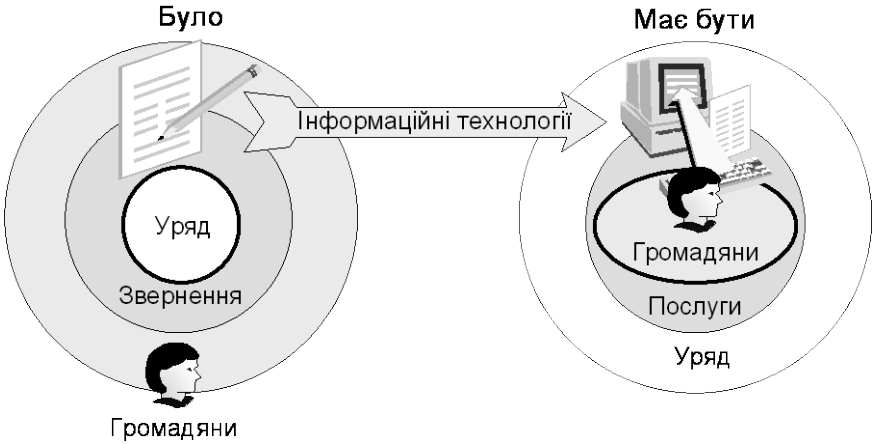

Рис. 1.3. Зміни у взаємовідносинах влади та громадян завдяки застосуванню інформаційних технологій

Указані у Білій книзі принципи відповідають концепції «електронного уряду» (*e*-Government), що була запропонована урядами США та

Канади [33] та впроваджується в країнах Європи [34, 35], в Росії [36–40], а також і в Україні [41]. Так, Кабінет Міністрів України прийняв розпорядження від 24.02.2003 р. № 208 «Про заходи щодо створення електронної інформаційної системи «Електронний уряд», а Указом Президента України «Про першочергові завдання щодо впровадження новітніх інформаційних технологій» № 1497/2005 було запропоновано Кабінету Міністрів України забезпечити протягом 2005–2006 років «організацію роботи з надання юридичним і фізичним особам адміністративних послуг на основі використання електронної інформаційної системи «Електронний уряд»».

Що таке «електронний уряд»? Комісія Європейського союзу *(Commission of the European Communities)* визначає, що «*е*-уряд — це безперервна оптимізація надання послуг і управління за допомогою перетворення внутрішніх і зовнішніх відносин із застосуванням нових технологій, Інтернету й нових засобів інформації». У свою чергу корпорація IBM як визнаний лідер у просуванні рішень для інформатизації державної влади визначає: «*е*-уряд — це злиття бізнесу й технологічних рішень в умовах, що вимагають від уряду реалізації стратегії орієнтування на громадян при одночасному поліпшенні ефективності влади й розширення інформаційної доступності для громадян»[11].

Як альтернатива *е*-уряду з'явився навіть термін «держава на вимогу» (*state on-demand*). За визначенням тієї ж корпорації IBM це «уряд, чиї ділові процеси інтегровані зверху до низу, а також й з іншими урядовими агентствами й установами, який може реагувати на вимогу, як тільки в цьому з'являється необхідність із боку громадян, бізнес-співтовариства, при виникненні змін економічних умов, із додержуванням змін законодавства й політичних пріоритетів».

Чому в демократичній країні питання «електронізації» уряду є таким важливим? Мабуть вичерпною відповіддю на це питання може бути висловлювання легенди канадської демократії сенатора Юджина Форсея (Eugene Forsey) про визначальну роль держави в сучасному світі для існування особи: «*We cannot work or eat or drink; we cannot buy or sell or own anything; we cannot go to a ball game or a hockey game or watch TV without feeling the effects of government. We cannot marry or educate our children, cannot be sick, born or buried without the hand of government somewhere intervening*».

[11] IBM Institute of Business Value.

Місце *е*-уряду в системі суспільних відносин, що складаються в умовах їхньої відкритості й «електронізації» та які визнано міжнародною спільнотою, показано на рис. 1.4 (верхня частина зображення). При цьому позначення C2G відповідає взаємовідношенням громадян та уряду, B2G — бізнесу та уряду, а G2G — між урядовими установами. Нижня частина ілюструє взаємодію в системі «електронного бізнесу».

Рис. 1.4. Місце *е*-уряду в системі «електронних» суспільних відносин

«Електронізація» взаємодії уряду з населенням є не лише технічною задачею, вона потребує нового рівня осмислення цієї проблеми. Як сказав Альберт Ейнштейн, «нові складні проблеми, з якими ми зіштовхуємося, не можуть бути вирішені на тому ж рівні мислення, на якому ми перебували в той момент, коли ми їх створили».

У цьому зв'язку перш за все потребує визнання парадигма, яка полягає у тому, що інформація, створювана державними органами, є суспільним надбанням. З іншого боку, набуває важливості питання проведення аналізу готовності країни до електронного розвитку (*e-Readiness Assessment*), а також створення політичного і нормативно-правового середовища для реалізації програм електронного розвитку, у тому числі на основі використання механізмів самоорганізації (*e-Legislation*).

У своєму виступі «*e*Europe: шлях уперед» на історичній (для інформатизації європейських країн) урядовій зустрічі в Лісабоні 10 квітня 2000 року член Європейської Комісії Еркки Лііканен, відповідальний за промисловість і інформаційне суспільство, сказав: «Уряд і державні адміністрації на всіх рівнях повинні використовувати нові технології. Не тільки, щоб зробити інформацію доступною, наскільки це можливо. Навіть більш важливо представити уряд громадянам ближче, зробити уряд більш прозорим і сприяти більшій участі громадян у ньому». Тобто перехід до проектів «***електронної демократії***» (*e-Governance*), що дозволяє підвищити залучення суспільства до прийняття державних рішень демократичним шляхом, є взагалі головною метою інформатизації влади.

Слід звернути увагу й на таку особливість «електронного уряду», що для громадян уся система державної влади має уявлятися як одна інституція, доступ до послуг якої відбувається через єдину «точку входу» (концепція «єдиного вікна») (рис. 1.5).

Сьогодні за оцінками експертів 90 % всіх транспортних переміщень людей пов'язане з інформаційними цілями (наради, підписи, довідки тощо). Серед цих цілей відвідування державних установ є, мабуть, чи не найвідчутнішою складовою. Тому будь який запит громадянина чи то з питань працевлаштування, чи пенсійного забезпечення, чи отримання дозволу на проведення підприємницької діяльності має подаватись в електронному вигляді на одну адресу Інтернету, а опрацювання цього запиту в автоматизованому режимі має розподілятися між причетними органами влади.

Інший виклик сучасності полягає в тому, що об'єктивно чотири основні учасники, а саме органи державної влади, опозиція, ЗМІ, а також незалежні експерти (громадянське суспільство) регулярно вступають в ***інформаційні відносини***, у конфлікт узгодження суперечливих інтересів [15, 19], тим самим формуючи для системи державної влади змінне, динамічне ***зовнішнє середовище***, що безупинно еволюціонує.

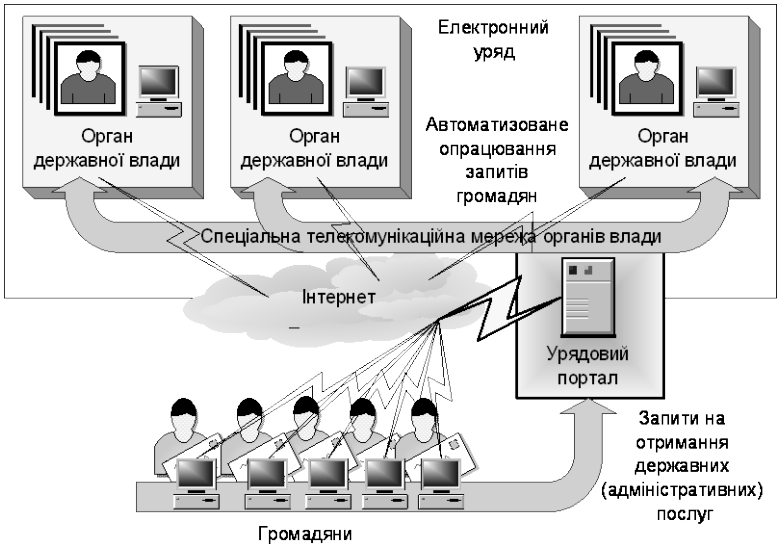

Рис. 1.5. Концепція єдиної «точки входу» до «електронного уряду»

Вплив цього середовища, зокрема це дії зовнішніх директив, політика державного розвитку, зміна законодавства, нормативні акти вищих органів влади, загрози інформаційній безпеці й т.ін., перш за все відчувають на собі органи державної влади (рис. 1.6).

У цих процесах також суттєве значення має вплив вектора взаємодії засобів масової інформації і влади [15], який є реалізацією зворотного зв'язку від суспільства до влади. Фоновими, але не менш суттєвими зовнішніми впливами є й зміни у міжнародних стосунках держави.

Указані чинники проявляють себе у вигляді ***інформаційних потоків*** (*information flows*), що набувають усе більшої інтенсивності, а зовнішнє середовище має розглядатися як ***інформаційний простір*** (*information space*), що постійно еволюціонує.

Основні принципи інформаційних відносин і вимоги до їхньої організації в Україні визначені низкою нормативних актів. Статтею 5 Закону України «Про інформацію» принципами інформаційних відносин визначено 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. Кодексом про адміністративні правопорушення передбачені санкції за порушення законодавства

про державну таємницю (ст. 212-2), за порушення права на інформацію (ст. 212-3) та за порушення порядку поводження з конфіденційною інформацією, що є власністю держави (ст. 212-5).

Рис. 1.6. Динамічне середовище, що оточує систему державної влади

Законом України «Про боротьбу з корупцією» встановлені спеціальні антикорупційні обмеження, одним з яких є заборона незаконної відмови в інформації, умисна її затримка або надання недостовірної чи неповної інформації (п. «г» ч. 1 ст. 5), за порушення яких передбачена відповідальність у вигляді штрафу (ст. 8).

Законом України «Про внесення змін до Цивільного кодексу України щодо права на інформацію» зокрема змінено положення ч. 3 ст. 277 Цивільного кодексу України щодо права на інформацію стосовно негативної інформації та ст. 302 щодо поширення офіційної інформації. Цими змінами захищені як свобода висловлення поглядів і думок, так і право особи на спростування недостовірної інформації щодо себе або членів своєї родини, а також права юридичних осіб на захист конфіденційної інформації.

Водночас перебіг суспільно-політичних процесів останніми роками виявив низку негативних тенденцій у сфері забезпечення свободи слова. Мають місце факти відновлення в різних формах цензури ЗМІ,

перешкоджання виконанню журналістами професійних обов'язків з боку посадових осіб, що заважає їм інформувати громадськість про події у суспільстві і державі, публічного незадоволення чиновників самим фактом критики на свою адресу.

Моніторинг інформаційної відповідальності влади, метою якого є вивчення стану справ із застосування передбачених законодавством санкцій за порушення держслужбовцями інформаційного законодавства, що постійно провадиться різними ЗМІ та агенціями, свідчить, що це питання є особливо актуальним як для пересічних громадян, так і для журналістів, інформаційні права яких часто порушуються. Адже органи влади, які виконують функції нагляду та контролю питань порушень чиновниками інформаційного законодавства, самі часто грубо порушують інформаційні права громадян і журналістів, а кількість справ у судових органах про порушення інформаційної відкритості влади є мізерною.

Питання інформаційної відкритості влади є особливо важливим з огляду й на те, що непрозорість діяльності влади та протизаконне обмеження доступу до інформації створює підґрунтя для корупції, яка є істотною перешкодою у розвитку держави. В той же час згідно з ч. 11 ст. 30 Закону України «Про інформацію» право громадськості знати цю інформацію переважає право її власника на її захист.

Отже, множина зовнішніх впливів на систему державної влади та на окремі ОДВ має інформаційну природу і тому приводить до постійного пристосування до них ***інформаційно-аналітичної діяльності*** органу влади. Тобто діалектика державної політики та відкритості влади перед суспільством вимагає від органу влади знаходитись у стані превентивної ***адаптації*** (рис. 1.7).

Урядовці мусять всякчас балансувати між протилежними, взаємовиключними тисками. З одного боку, в них має бути жорстка односпрямована затверджена стратегія, бо інакше державна діяльність неефективна, якщо не веде до заявленої мети. А з іншого — вони повинні зважати на вимоги з різних суспільних сторін, де кожний тягне у свій бік.

Тому в сучасних умовах постійно зростає прагнення органів управління мати у своєму розпорядженні всеосяжну, цілком вірогідну, без суб'єктивного нальоту інформацію щодо конкретних питань. На рівні управління державою ця інформація повинна відображати не тільки реальне становище справ, але й тенденції, масштаби та очікувані наслідки розвитку процесів життєдіяльності держави і світу на ближню та далеку перспективи. Це є необхідною умовою забезпечення системного

управління країною, узгоджених і цілеспрямованих дій усіх ланок державної влади [42, 43].

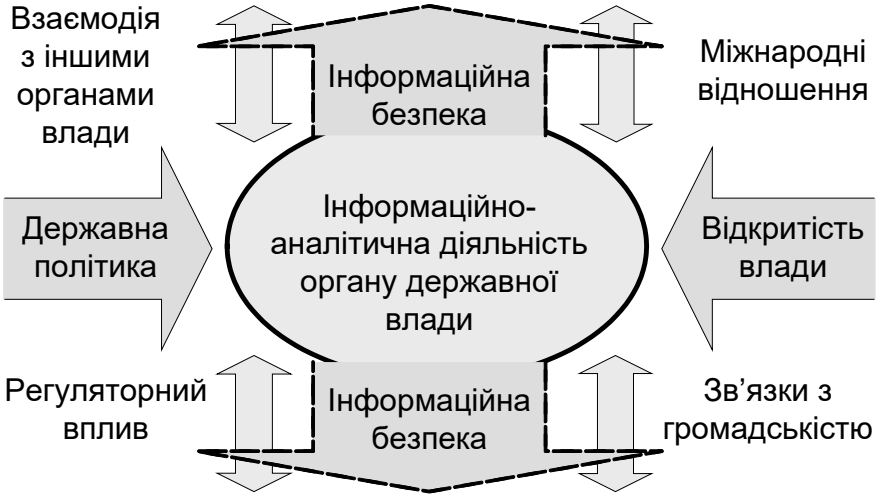

Рис. 1.7. Чинники, що впливають на інформаційно-аналітичну діяльність органу влади

Інформаційний аспект державного управління. Слід констатувати, що у вказаних умовах як складовий елемент системи державного управління, а також як основний засіб усунення кризових і передкризових явищ шляхом використання в підготовці рішень релевантної та пертинентної інформації слід розглядати ***інформаційний простір державної влади*** та динаміку інформаційної взаємодії органів влади із суспільством [20, 44].

У [44] поняття «єдиного інформаційного простору» держави розглядається як сума «проблемно-орієнтованих інформаційних просторів» (ПОІП) і центрів інформаційно-аналітичної підтримки, де одними з ПОІП власне й є галузеві інформаційні простори — культури, медицини, науки тощо.

Таким чином, розглядаючи з інформаційної точки зору середовище державної влади, його можна структурувати на безпосередньо інформаційний простір державної влади, що складається з інформаційних середовищ (*information environment*) окремих органів влади, національний інформаційний простір і навіть глобальний інформаційний простір (рис. 1.8). При цьому на діяльність влади більш суттєвий вплив здійс-

нюють саме останні складові. Вони ж і є одночасно головними джерелами загроз інформаційній безпеці державної влади.

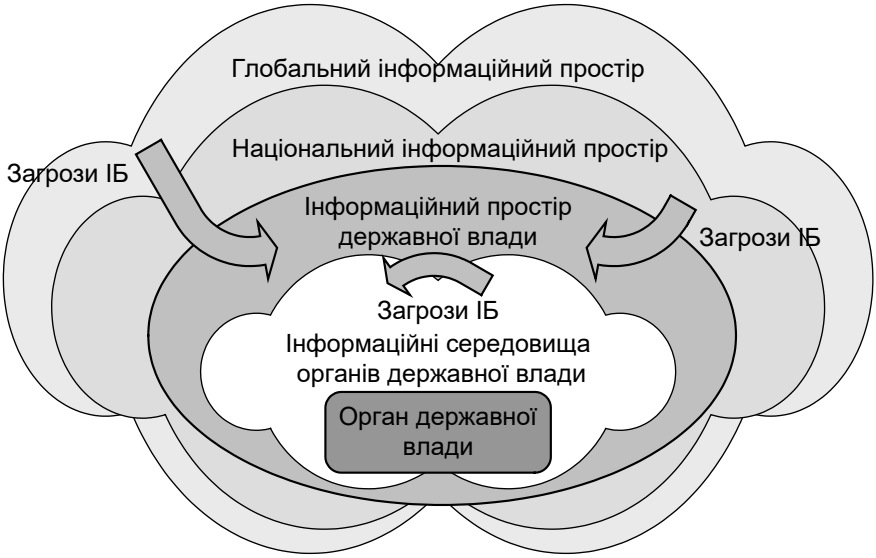

Рис. 1.8. Місце системи державної влади в інформаційному просторі

Узагальнюючи різні підходи до дефініцій вказаних понять, що зараз мають місце, визначимо, що ***інформаційний простір*** — це середовище, де здійснюється формування, збір, зберігання та розповсюдження інформації, інформаційна взаємодія організацій і громадян та задоволення їхніх інформаційних потреб. У свою чергу ***національний інформаційний простір*** — це інформаційний простір, на який розповсюджується юрисдикція країни.

Інфраструктура інформаційного простору (інформаційна інфраструктура) — це система організаційних структур, що забезпечують функціонування та розвиток інформаційного простору й засобів інформаційної взаємодії. Тобто інформаційна інфраструктура являє собою сукупність даних (структурованих чи неструктурованих); засобів збору, накопичення, обробки, збереження та розповсюдження інформації; системи виробництва інформаційних ресурсів; інструктивних матеріалів і документації; людини як активного фактора впливу на інформаційний простір.

Інформаційний ресурс — це складова інформаційного простору, що поєднує в собі дані, їхнє місцезнаходження, взаємозв'язок між інформаційними елементами, відомості про процеси надходження, зберігання, обробки тощо.

Сучасний стан проникнення ІКТ у суспільні інституції дозволяє казати про формування в країні ***національної інформаційної інфраструктури (НІІ)*** та ***інформаційної інфраструктури державної влади***.

Загальновизнаним є перелік складових інформаційної інфраструктури, до якого входять лінії та засоби зв'язку, мережі телекомунікацій, електронні інформаційні ресурси (ЕІР), а також відповідні інституційні складові (обчислювальні центри, інформаційні агенції, оператори та провайдери тощо). Вочевидь, мова йде про відповідні ***автоматизовані інформаційні системи (АІС)*** і системи телекомунікацій. Але останні фактично є елементами сучасних АІС. Отже, можна зробити висновок, що до інформаційної інфраструктури належить сукупність АІС і систем зв'язку, на базі яких будуються системи телекомунікацій.

Сучасна ідеологія інформаційного впливу на діяльність підприємств, установ і організацій відкриває широкі можливості для впровадження в них ІКТ і, відповідно, створення в них АІС. У відповідності до існуючої концепції інтеграції пов'язаних між собою АІС, направленої перш за все на підвищення рівня ефективності їхнього функціонування, широко впроваджуються так звані корпоративні інформаційні системи (КІС). Такі системи активно використовують ЕІР, як власні, так і загальнодержавні, а їхніми невід'ємними складовими є розвинуті засоби зв'язку та телекомунікацій. Ґрунтуючись на цих фактах, можна стверджувати, що АІС є основними елементами НІІ [45, 46] (рис. 1.9).

Таким чином, інформаційну інфраструктуру можна уявити як деяку метасистему множин, що складається з підмножин $S \in I$, які самі утворюють системи:

$$I = \{S_1, S_2, ..., S_n, ...\}, \ \ n = \overline{1, \infty}, \tag{1.1}$$

де $S_i, i \in n$ — i-та система.

Інформаційний простір, в якому відбувається державне управління, головним чином може бути визначеним у трьох основних «координатах», що відображають три основні аспекти державного управління та зв'язність складових систем: функціональний, галузевий та територіальний [19, 44, 47].

Рис. 1.9. Складові НІІ

Функціональний аспект I_f визначає функції, які можуть бути розподілені на головні функції (економічні, соціальні, освітні та культурні), допоміжні (внутрішні потреби адміністративних структур) і командні (необхідність застосування влади) функції.

Галузевий аспект I_g передбачає урахування особливостей людської діяльності в різних галузях. Територіальний аспект I_t є невід'ємною складовою аналізу державного управління, оскільки будь-яка держава має ієрархічну адміністративно-територіальну структуру, яка віддзеркалюється в структурах і методах управління (централізація та децентралізація, самоврядування, підпорядкованість тощо).

Опис зв'язності може бути здійснений із застосуванням різноманітних підходів, але найбільш вдалі з них будуються на основі теорії графів та алгебраїчної топології. Для оцінки зв'язності кожна система уявляється у вигляді деякого багатовимірного об'єкта, вимірність якого визначається числом вихідних (вхідних) зв'язків. У топології такому уявленню відповідає геометричний об'єкт, що має назву симплекс. Відомо, що *n*-вимірним симплексом з верхівками $\{x_1, x_2, ..., x_{n+1}\} \subset R^n$ називається множина точок *n*-вимірного евклідового простору R^n, що задається співвідношенням

$$y = \left\{ \; x \mid x = \sum_{i=1}^{n+1} \alpha_i x_i, \sum_{i=1}^{n} \alpha_i = 1 \; \right\} \subset R^n . \qquad (1.2)$$

Отже, класифікаційно-структурні системи (проекції) взаємовідношень кожної з трьох координатних осей та площин такого простору породжують дуже складну картину, динамічною складовою якої виступає ***інформація*** у різних своїх проявах (рис. 1.10) [15, 48, 49].

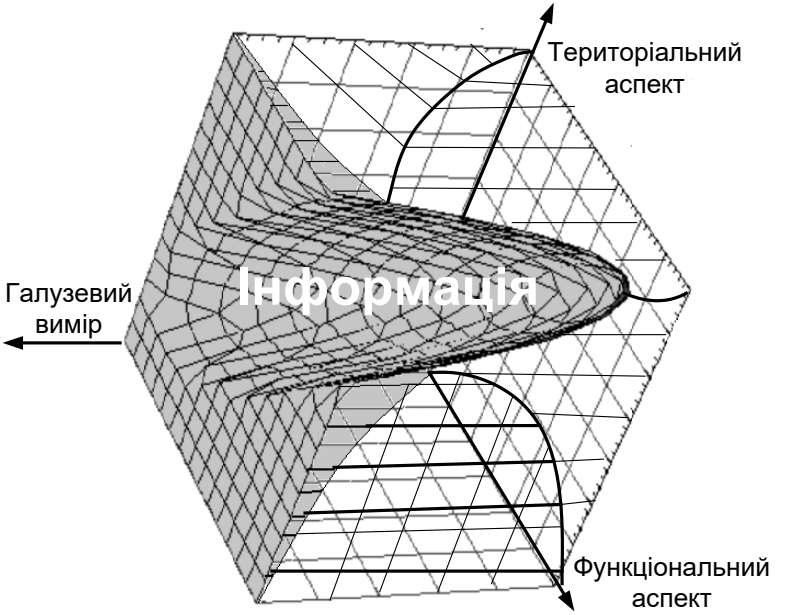

Рис. 1.10. Простір основних аспектів державного управління

Уведеному в [48, с. 8] поняттю «інформаційного закону взаємодії» як суми «інформаційних законів», які являють собою «сутність природи, що має властивості визначати інші сутності» належить визначальний прояв і у сфері державного управління.

Однак, розглядаючи інформаційний аспект, дослідження з питань державного управління та його «інформатизації», як вже вказувалося, переважно не враховують той факт, що в сучасному світі держава та її органи управління все більш значною мірою підпадають під вплив світового та національного інформаційного простору, що пов'язано з такими характерними рисами сучасності, як явищем масовості інформаційних потоків і їхнім транскордонним характером, а також стрімким розвитком супутніх проблем «інформаційного вибуху» [22].

Фактично інформаційні потоки і ресурси вже стали найважливі-

шими складовими процесів державного управління. Водночас при розгляді питань критеріїв державного управління та регламенту його роботи аспект ефективності та повноти опрацювання інформації, як правило, залишається не врахованим.

Розглядаючи реальні механізми формування, збереження і поширення інформації в системі державної влади слід зазначити, що цільова функція збору, обробки, збереження даних в органах влади в більшості випадків або вкрай неефективна, або цілком ігнорується. Тобто, інформаційні процеси здійснюються спонтанно, без використання наукових розробок, теорії побудови сучасних інформаційних систем. На підставі приведених міркувань не буде перебільшенням висловити припущення про те, що в реально діючій системі державного управління відсутній дуже важливий регулюючий і стимулюючий елемент, роль якого має виконувати інформація.

Ще раз слід зазначити, що проблеми, які вирішуються органами влади, тісно пов'язані саме з інформацією і, отже, основою технологією має стати нагромадження даних і їхній детальний аналітичний аналіз. Це набуває актуальності, враховуючи й той факт, що при переході проблеми в стадію конфлікту різко збільшується інформаційний потік, а також зворотний зв'язок з даного питання.

Враховуючи викладене, за роки незалежності «електронізація» органів влади беззаперечно визнана як актуальне завдання і набула широкого розмаху. Але загалом багатьма авторами, що розглядають різні аспекти зазначеного питання, проблема створення в органах державного управління комплексних автоматизованих систем із аналітичною складовою, забезпечення їхньої взаємодії між собою, з бізнесом і населенням залишається переважно не розкритою.

1.2. Формування інфраструктури інформаційного простору державної влади

Інформаційно-аналітичне забезпечення органів влади. Фундаментальна відмінність систем суспільного управління взагалі і систем державного управління у тому числі від суто технічних систем полягає у тому, що ці системи є *людино-машинними,* де атрибутами управління є *людський* та *суспільний* фактори, а об'єктами управління можуть виступати колективи людей, регіони, господарські галузі і навіть цілі суспільні підсистеми.

Ці обставини вимагають забезпечення найефективнішого інформаційного обміну між системою управління й об'єктами. Це, у свою чергу, тягне за собою проблему інтеграції інформаційно-аналітичних систем органів державної влади в єдину загальнодержавну систему, що має вирішити таке масштабне завдання, як ведення загального інформаційного середовища державної влади та забезпечення необхідного рівня його захисту [50, 51].

В умовах змін у сфері взаємодії між урядом, приватним сектором і суспільством важливого значення набуває ***інформаційно-аналітичне забезпечення*** управлінської діяльності [1]. Якісне вдосконалення управлінської праці може бути досягнуто шляхом подальшої її інтенсифікації, здійснюваної на базі використання сучасних економіко-математичних методів, електронно-обчислювальної техніки, засобів телекомунікацій, що об'єднані в автоматизовані системи управління [1, 10]. Власне, саме таким чином виникло поняття інформаційно-аналітичної діяльності як сукупності дій та заходів на основі концепцій, методів і засобів, нормативно-методичних матеріалів для збору, накопичення, обробки та аналізу даних на основі інформаційних технологій з метою обґрунтування прийняття рішень.

Питанням розвитку інформаційно-аналітичної діяльності на основі застосування ІКТ в органах влади як в Україні, так, наприклад, і в Росії присвячується усе більше публікацій [52–62]. Але вони ще мають розрізнений характер, не складають цільного уявлення про напрямки вирішення існуючих проблем, зокрема, що стосується питань інформаційної безпеки влади.

Важливим чинником переходу українського суспільства до більш ефективної системи державного управління є проведення адміністративної реформи, сформульованої в Указі Президента України № 810/98 від 22.07.98 «Про заходи щодо впровадження Концепції адміністративної реформи в Україні». Але, на жаль, нею не передбачаються інституційні зміни, пов'язані з автоматизацію управлінської праці та впровадженням концепції «електронного уряду», не кажучи вже про забезпечення необхідного рівня інформаційної безпеки. Та й сама реформа відбувається дуже повільно.

Інформаційно-аналітичні системи органів влади. Одним із головних аспектів адміністративної реформи є інформатизація державного управління. Очевидно, що державні служби повинні користуватися найкращими і найсучаснішими технологіями в сфері комуні-

кацій, електронної пошти і електронного документообігу, які не поступаються технологіям корпоративного і приватного сектора.

Отже, розгорнення державотворчих процесів в країні тісно пов'язане з використанням новітніх досягнень комп'ютерної науки та інформаційних технологій у всіх сферах розвитку держави й суспільства. Ще наприкінці 80-х рр. минулого століття під час обговорення концепції інформатизації країни вченими й фахівцями виділялося головне твердження — справа не стільки в концепції інформатизації, скільки в концепції розвитку суспільства, всіх його структур; інформатизація — супутник демократизації й неможлива без неї. Тому законами України, указами президента України, іншими нормативними актами та документами передбачено широке впровадження засобів автоматизації інформаційно-аналітичної діяльності в органах державної влади з метою підвищення ефективності та досягнення якісно нового рівня в управлінні державою.

У зв'язку з цим інформатизація державного управління має передбачати побудову на єдиній методологічній і програмній основі ***автоматизованих інформаційно-аналітичних систем органів влади (АІАС)*** як основних елементів інфраструктури інформаційного простору державної влади, головним завданням яких має стати створення та підтримка банків даних, забезпечення доступу до міжнародних інформаційних мереж, насамперед Інтернету, аналітичний моніторинг результативності та ефективності управлінської діяльності органів влади тощо [63, 64]. При цьому слід вважати, що ці АІАС є основним засобом забезпечення інформаційної безпеки влади [65].

Сьогодні у більшості органів влади — починаючи від районного рівня й до міністерств і вищих органів управління — створюються або вже функціонують системи різних масштабів і функціональної спрямованості, зокрема, спрямовані на автоматизацію інформаційно-аналітичної діяльності [65]. Враховуючи значну кількість в країні органів державного управління, їхній визначальний вплив на діяльність суспільства не буде перебільшенням зазначити, що ці автоматизовані інформаційно-аналітичні системи й ті складові, що спеціально створюються або використовуються задля забезпечення функціонування АІАС можна вважати не лише основою інфраструктури інформаційного простору державної влади, а й водночас головною частиною НІІ (рис. 1.11). Отже, інформаційно-комп'ютерні системи в галузі державного управління є невід'ємними елементами НІІ.

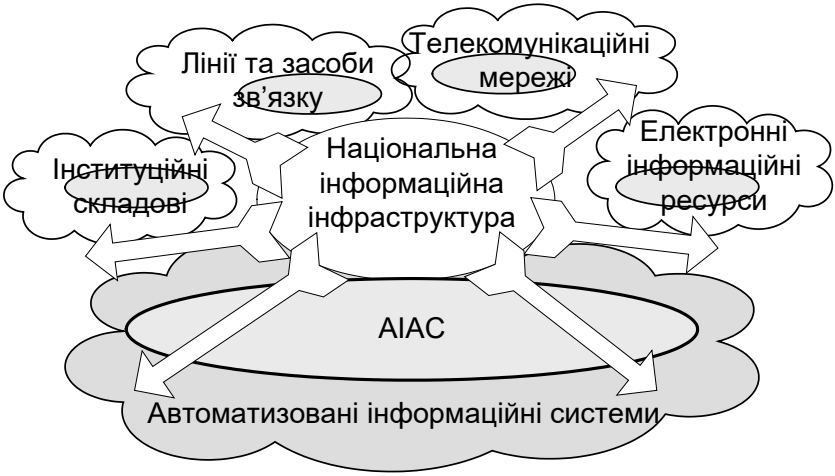

Рис. 1.11. АІАС як головна частина НІІ

У [44] наведене таке визначення інформаційно-аналітичної системи: «це автоматизована система, що містить крім корпоративної інформації довідкового характеру алгоритми аналізу ситуацій, що виникають при розв'язанні конкретних задач, які характерні для даного проблемно-орієнтованого інформаційного простору, а також алгоритми прогнозу розвитку ситуацій з видачею рекомендацій з прийняття рішень».

При цьому в [65] інформаційно-аналітичні системи в органах державної влади визначаються як суспільні структури, до яких належать інформаційні технології, інформаційні системи й інформаційні ресурси для забезпечення здійснення інформаційно-аналітичної діяльності.

При їхньому створенні потрібен новий підхід до вирішення проблем управління на інформаційній основі, який би враховував сучасне уявлення про інформацію як про інтелектуальний продукт — знання, як ресурс суспільства, і який спирався б на досягнення інформаційних технологій і програмно-технічної бази інформатики [66]. На озброєння повинен бути взятий інформаційний підхід створення нового знання і обміну знаннями (*e-Knowledge*), який базується на антиентропійному розумінні переборення проблем управління. При цьому інформаційні системи мають розглядатися не як «людино-машинні», а як соціотехнічні, як системи, що перероблюють знання [67].

Але при цьому застосування засобів комп'ютерної техніки для аналітичної обробки інформації в суспільній сфері зараз тільки починається. Вирішення проблем інформаційного управління на рівні структур влади в країні відбувається вже тривалий час [68], але у напрямку забезпечення при цьому питань інформаційної безпеки робляться лише перші кроки.

Чимало авторів погоджуються з тим, що об'єднуючим фактором виступає єдина природа всіх функцій управління, а саме інформація [69–78]. Водночас вказується на постійну недостатність нормативно-правової бази в інформаційній сфері, породжуваній об'єктивним відставанням засобів правового регулювання від потреб життя, для забезпечення однакового тлумачення норм і правил управління [79–81]. Також майже немає публікацій, у яких розкривалися б питання інтегруючого значення інформації, технологічні аспекти її обробки та забезпечення належного захисту саме в ІАС органів влади.

Вітчизняний досвід автоматизації організаційного управління налічує вже декілька десятиліть та пов'язаний перш за все з ім'ям академіка В.М. Глушкова. Ним були запропоновані ідеї та розроблені наукові засади загальнодержавної системи автоматизації управління. За його ініціативою були проведені розробки та виконані впровадження автоматизованих систем управління (АСУ) на багатьох підприємствах, в організаціях невиробничої сфери, міністерствах і відомствах, а визначені академіком принципи проектування АСУ не втратили своєї актуальності й досі [82–84].

Проблема автоматизації державної управлінської сфери в Україні, що потребує нових підходів і принципів, усе більше заслуговує на увагу. Визначено, що основні напрямки цієї роботи повинні охоплювати увесь досвід інформатизації і управління, накопичений на різних рівнях — державному, галузевому, регіональному, корпоративному, а також спиратися на новітні досягнення у сфері наукових розробок і технологій [85].

Упродовж останніх років проведені певні дослідження з питань створення інформаційних систем, інформатизації органів влади, зокрема, в Україні [85–101]. Серед них, наприклад, заслуговують на увагу праці члена-кореспондента НАН України А.О. Морозова та його колег [102–111], зокрема, що стосуються застосування в державних установах методів ситуаційного управління.

Вагомі наукові й прикладні результати по програмуванню, отримані вченими Кібцентру НАНУ, впроваджено при створенні інформа-

ційних технологій і державних систем різноманітного призначення. Серед них слід відмітити технологи підтримки інформаційно-аналітичної діяльності органів державного управління, моніторингу та прогнозування екологічних ситуацій. Як приклад заслуговує на увагу автоматизована система ГАРТ, створена Інститутом програмних систем НАНУ під керівництвом академіка П.І. Андона в інтересах Держкомкордону України й спрямована на підтримку повсякденної діяльності всієї інфраструктури прикордонних військ, яка отримала високу оцінку міжнародних експертів.

Але, по-перше, таких робіт вкрай недостатньо, а, по-друге, вони присвячені лише окремим аспектам інформатизації державних органів і майже не торкаються питань комплексного вирішення проблем інформаційно-аналітичного забезпечення в органах влади з урахуванням питань інформаційної безпеки.

Державна політика щодо формування інформаційного простору органів влади. У зв'язку з тим, що інформатизація фактично проникає у всі сфери життя, стає фактором забезпечення добробуту держави, національної безпеки та суверенітету, регулювання цього процесу та формування системи «електронного уряду» вже виходить на рівень важливішої функції держави. Особливої актуальності набувають питання державного регулювання сфери інформатизації органів влади. Саме на цьому напрямку роль держави стає вирішальною, а політика інформатизації визначається як важлива складова частина загальної внутрішньої і зовнішньої політики країни.

Закон України «Про Концепцію Національної програми інформатизації» визначає, що державна політика інформатизації — це системно узгоджені концептуальні засади та принципи, які обумовлюють і регламентують функції, форми і зміст правових, організаційних, економічних та інших взаємовідносин як між державою та суб'єктами, так і між самими суб'єктами у сфері інформатизації.

Відповідно до статті 6 Закону України «Про інформацію» ***державна інформаційна політика*** — це сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації.

Демократичні засади розвитку суспільства передбачають право усіх суб'єктів на отримання повної, вірогідної та своєчасної інформації [112]. Роз'яснення можливостей і переваг використання ІКТ для життя й роботи (*Awareness & Preparedness campaigns*), участь у міжнародних і регіональних ініціативах, програмах і мережах, особливо в рамках про-

цесів економічної інтеграції (*e-Initiatives & e-Networks*) — саме на цих напрямках роль держави стає вирішальною, а політика інформатизації визначається як важлива складова частина загальної внутрішньої і зовнішньої політики країни. Особливе значення мають такі її аспекти, як правовий, організаційний, економічний, науково-технічний, промисловий, соціальний, міжнародний та інформаційної безпеки.

Серйозну увагу державному регулюванню процесів інформатизації органів влади приділяють зокрема такі країни, як США, Японія, Німеччина, Росія. У США, поряд із підтриманим шляхом різних законодавчих пропозицій розвитком інформаційної супермагістралі та пов'язаної з нею Національної інформаційної інфраструктури (НІІ), широко розглядається як аспект лідерства в інформаційному віці політика електронного розповсюдження урядової інформації, встановлена ще з 1993 р. «Актами щодо зменшення паперової роботи» [75].

Важливе значення має досвід країн Європейського Союзу, які спрямовують політику і діяльність у сфері інформатизації перш за все на підвищення ефективності державного управління.

Країнами СНД у рамках Координаційної ради з питань інформатизації Регіональної співдружності адміністрацій зв'язку всебічно розглядаються аспекти формування в цих країнах систем електронного уряду.

Яскравим прикладом державної уваги до питань інформатизації є виступ Президента Росії Дмитра Медведєва на першому засіданні Ради з питань розвитку інформаційного суспільства при Президентові Росії (в 2009 р.). Відкриваючи засідання, він підкреслив, що ніякий прогрес і модернізація неможливі без ІТ: «це стосується й науково-технічної сфери, і власне питань управління й навіть питань зміцнення демократії в країні»[12].

В Україні увага до питань інформатизації органів влади приділялась майже з перших років її незалежності. Шляхи становлення сфери інформатизації органів державної влади в Україні, існуючі проблеми та досягнуті результати розглянуті в [85, 86], а також у [113].

Без перебільшення історичне значення у сфері інформатизації має прийняття Законів України «Про інформацію» від 02.10.92 р. № 2658-ХП, «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.94 р. № 81/94-вр, «Про Концепцію Національної програми інформатизації» від 4.02.98 № 75/98-вр, «Про Національну програму інформатизації» від 4.02.98 № 76/98-вр, «Про електронний циф-

[12] Джерело — CNews.

ровий підпис» та «Про електронні документи та електронний документообіг» (2004 р.).

Активні заходи щодо вдосконалення системи управління інформаційною сферою вживаються Президентом України. Свого часу важливого політико-правового значення мали Укази Президента України «Про вдосконалення державного управління інформаційною сферою» (16.09.1998 р.); «Про положення про технічний захист інформації в Україні» (27.09.1999 р.); «Про вдосконалення інформаційно-аналітич-ного забезпечення Президента України та органів державної влади» (14.07.2000 р.); «Про заходи щодо розвитку Національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі» (31.07.2000 р.); «Про додаткові заходи щодо безперешкодної діяльності засобів масової інформації, дальшого утвердження свободи слова в Україні» (09.12.2000 р.); «Про рішення Ради національної безпеки і оборони України від 19 липня 2001 року «Про заходи щодо захисту національних інтересів у галузі зв'язку та телекомунікацій» (23.08.2001 р.) та ін.

Базовими документами при створенні систем захисту інформації стали накази Держспецзв'язку «Про положення про державну експертизу в сфері технічного захисту інформацій» (від 16.05.2007 р. № 93) та «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» (від 04.07.2008 р. № 112).

Основні принципи діяльності держави в сфері інформатизації на найближчі роки визначено «Основними засадами розвитку інформаційного суспільства в Україні на 2007–2015 роки» (далі — Основні засади), розробленими на виконання рішень Всесвітнього самміту з питань інформаційного суспільства (WSIS) та затверджені Законом України від 9 січня 2007 року № 537-V.

План заходів із виконання завдань, передбачених указаним законом, затверджено розпорядженням Кабінету Міністрів України від 15 серпня 2007 року № 653. Важливо, що цим планом передбачається суттєвий розвиток нормативно-правового поля інформатизації. Так, пунктом 13 цього розпорядження передбачено розробити проекти Інформаційного кодексу України та Закону України «Про електронну комерцію», а також проекти законів про внесення змін до деяких законів України, а саме до Законів «Про друковані засоби масової інформації (пресу) в Україні» (щодо удосконалення системи реєстрації друкованих засобів масової інформації з використанням інформаційно-телекомунікаційних

технологій); «Про видавничу справу» (щодо удосконалення порядку внесення суб'єктів видавничої справи до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції з використанням інформаційно-телекомунікаційних технологій); «Про інформаційні агентства» (щодо удосконалення системи державної реєстрації інформаційних агентств і визначення правового статусу засобів масової інформації, що створюють виключно електронні інформаційні ресурси); «Про звернення громадян», «Про Національний архівний фонд і архівні установи» (щодо звернень громадян, які подаються з використанням Інтернету і цифрового підпису, запровадження в органах виконавчої влади систем електронного документообігу та електронного цифрового підпису).

Крім того, зазначеним розпорядженням Кабінету Міністрів України передбачено підготовку проектів нормативно-правових актів з питань впровадження механізмів і регламентів надання органами виконавчої влади та органами місцевого самоврядування інформаційних послуг юридичним і фізичним особам через Інтернет; забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, порядку виявлення, попередження, оцінювання та прогнозування загроз безпеці державних інформаційних ресурсів, визначення рівня захисту інформації від несанкціонованих дій в інформаційно-телекомунікаційних системах; визначення загальних вимог до програмних продуктів, які закуповуються та створюються на замовлення державних органів, у тому числі щодо захисту прав інтелектуальної власності; визначення основних засад запровадження та функціонування систем забезпечення електронних бірж, аукціонів і депозитаріїв.

Визнається й необхідність забезпечення ефективності системи державного управління національними інформаційними ресурсами та їхнього захисту, що значною мірою пов'язане із загальним рівнем національної безпеки. Проблема формування організаційно-правових засад системи управління і захисту інформаційних ресурсів держави, створення збалансованої інформаційної інфраструктури, спроможної забезпечити формування, поширення й ефективне використання і захист державних інформаційних ресурсів, визначається як найактуальніша і невідкладна.

Розв'язання вище перелічених ключових проблем повинно здійснюватися на основі відповідної державної політики в галузі інформаційної безпеки. Багато вчених і фахівців визнають, що, на жаль, галузь інформаційної безпеки в Україні знаходиться ще в зародковому стані й

істотно відстає від розвинутих країн. Тому положення державної політики забезпечення інформаційної безпеки мають базуватись на таких основних принципах, як обов'язкове забезпечення прав громадян і організацій на вільний пошук і отримання інформації державних органів будь-яким законним способом, визнання пріоритетним розвиток сучасних вітчизняних конкурентноздатних інформаційних і телекомунікаційних технологій, створення національних телекомунікаційних мереж, забезпечення узгодженості рішень, що приймаються органами влади і місцевого самоврядування для забезпечення автоматизації діяльності та інформаційної безпеки в рамках єдиного національного інформаційного простору України, не допускаючи монополізму окремих органів влади і організацій в цій сфері та прагнучи відмовитися від закордонних інформаційних технологій для інформатизації органів державної влади й управління.

Суттєвого значення набувають питання забезпечення інформаційної безпеки в умовах функціонування «електронного уряду». Тут основні положення державної політики мають допускати обмеження доступу до державної інформації виключно на основі законодавства, визначених законом прав власності на цю інформацію, персоніфікувати відповідальність за збереження, засекречення і розсекречення державної інформації, визначати відповідальність перед законом органів влади і установ, що збирають, накопичують і обробляють персональні дані та конфіденційну інформацію, за їхнє збереження й використання; забезпечувати захист суспільства від помилкової, спотвореної та недостовірної інформації, що надходить від органів влади; забезпечення державного контролю за створенням і використанням засобів захисту інформації шляхом їхньої обов'язкової сертифікації і ліцензування діяльності в сфері захисту інформації.

Також має проводитися протекціоністська політика підтримки діяльності вітчизняних виробників засобів інформатизації і захисту інформації з одночасним здійсненням заходів із захисту державних органів від проникнення в них неякісних засобів інформатизації і інформаційних продуктів, з протидії інформаційної експансії різних країн.

Згідно з викладеним, стратегія автоматизації інформаційно-аналітичної діяльності органу державної влади має полягати у розробці цілісної системи збору, первинної та аналітичної обробки, зберігання, передачі і захисту інформації на базі застосування відповідних програмно-технічних засобів з урахуванням принципів державної політики інформаційної безпеки. Єдиний підхід до вирішення таких завдань поля-

гає у створенні у кожному державному органі такої АІАС, яка б змогла сформувати відповідне інформаційне середовище, надати уяву про достовірне середовище діяльності галузі, життя країни та світу, забезпечити прийняття керівництвом обґрунтованих ефективних рішень та необхідний рівень інформаційної безпеки як органу влади, так і всієї системи державної влади в цілому. Для забезпечення вказаних завдань ці системи мають інтегруватися між собою для налагодження ефективної та захищеної інформаційної взаємодії.

Підходи до вирішення деяких із вказаних завдань висвітлюються далі у цій книзі.

1.3. Загрози інформаційній безпеці державної влади

Питання інформаційної безпеки. Чому питання інформаційної безпеки так гостро стоїть на порядку денному? Воно взагалі кажучи не нове. Ще Леонардо да Вінчі у середні віки казав, що «очі та вуха, охочі до чужих секретів, завжди знайдуться». Уся історія людства пов'язана з ***інформаційними злочинами*** (*information crime*) — навмисними діями, спрямованими на розкрадання або руйнування інформації в інформаційних системах[13], які виходять з корисливих або хуліганських спонукань, тобто фактами порушення інформаційної безпеки, які зводяться, грубо кажучи, до викрадання або знищення інформації, та які часто мають суттєві наслідки для розвитку цивілізації.

З іншого боку, великою звитягою розвитку цивілізації стало й здобуття людиною права на інформацію. У резолюції Генеральної Асамблеї ООН від 10.12.1948 р. написано: «Свобода інформації є основним правом людини і являє собою критерій усіх видів свободи». Сьогодні чимало експертів ратують за вільне поширення будь-яких відомостей і прозорість державних інформаційних процесів. Але постіндустріальне суспільство, в якому ми з вами живемо, вважає найвищою цінністю саме інформацію, яку потрібно зберігати не менш ретельно, ніж золотий запас. Ця діалектика власне й є причиною тієї великої уваги, що приділяється проблематиці інформаційної безпеки.

Водночас слід звернути увагу й на психологічні аспекти сприйняття стану безпеки, що суттєво ускладнюють забезпечення інформаційної

[13] Під інформаційною системою тут розуміється будь-яка сукупність інформаційних відношень, не обов'язково автоматизованих (паперовий документообіг, бібліотеки, поштове листування тощо).

безпеки. Як пише Брюс Шнайер, один з відомих теоретиків питань безпеки: «Ви можете бути в безпеці, навіть коли ви цього не відчуваєте. І ви можете відчувати себе в безпеці, коли в дійсності це не так. Відчуття й реальність безпеки, безсумнівно, співвідносяться один з одним, але вони безперечно не є тим самим»[14].

Свідомість і рефлексія як функціональні механізми психічної регуляції діяльності людини дуже важливі в процесах прийняття державних рішень. Так, люди з високою самооцінкою (ці якості, вочевидь, притаманні багатьом високопосадовцям) схильні ігнорувати наявні інформаційні факти і недооцінювати ймовірність негативних наслідків ухвалених ними рішень, перебільшувати власні можливості щодо досягнення поставленої ними мети.

У загальному плані інформаційна безпека — це стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави. Відповідно ***загрозами*** (*threats*) інформаційній безпеці є чинники або їхня сукупність, що створюють небезпеку функціонуванню та розвитку інформаційного простору, перешкоджання інформаційним інтересам особистості, суспільства, держави.

Сфера ІКТ сьогодні стала об'єктом зосередженої уваги значного інтелектуального потенціалу цивілізації і водночас концентрації складних негативних явищ. Тому на відміну від класичних силових загроз, значення яких зменшується, загрози в інформаційній сфері відносяться до асиметричних (нетипових) [114].

Ці нові, нетрадиційні загрози, як вказувалось, є серйозною проблемою національної безпеки. Вони можуть торкатися безпеки як об'єктів і служб, істотних для злагодженого функціонування системи забезпечення життєдіяльності, так і безпеки громадян, спільноти й держави. З іншого боку, їхні джерела є також нетрадиційними, іноді важкими для ідентифікації (від маловивчених «сигналів з космосу» та більш реальних впливів всіляких військових космічних ешелонів до несанкціонованих або помилкових дій людей, що працюють в організації, в органі влади).

Тому оцінка стану інформаційної безпеки державної влади і визначення ключових проблем в цій сфері мають базуватися на аналізі ***джерел загроз***. Джерела загроз традиційно можна поділити на зовнішні і внутрішні.

[14] Джерело — Security Lab.

До зовнішніх джерел належать недружня політика іноземних держав у сфері поширення інформації і нових інформаційних технологій, діяльність іноземних розвідувальних і спеціальних служб, політичних і економічних структур, направлена проти інтересів України, злочинні дії міжнародних груп, формувань і окремих осіб, глобальні економічні кризи, стихійні лиха і катастрофи.

До внутрішніх джерел інформаційної безпеки державної влади слід віднести протизаконну діяльність політичних і економічних структур у сфері формування, поширення й використання інформації, неправомірні навмисні дії та ненавмисні помилки держслужбовців і персоналу інформаційних систем, відмови технічних засобів і збої програмного забезпечення.

Поділ джерел на внутрішні та зовнішні є певним чином умовним, адже скоєння злочинів із застосуванням комп'ютерів і Інтернету зазвичай має транснаціональний характер. І кожне з названих джерел може привести до нанесення серйозного збитку життєво важливим інтересам країни в політичній, економічної, оборонній і інших сферах діяльності або заподіяння істотного соціально-економічного збитку суспільству і окремим громадянам. До речі, за даними щорічного дослідження відомого аналітичного центру InfoWatch у галузі корпоративного захисту від внутрішніх загроз інформаційної безпеки, проведеного в 2007 році, поділ загроз на зовнішні та внутрішні є приблизно однаковим (відповідно 43,5 % і 56,5 %).

Які ж явища сьогодні можна віднести до загроз інформаційній безпеці державної влади?

Перш за все, слід зазначити, що завдяки потужності сучасних технологій визначальним чинником розвитку економіки, науки, освіти в наш час стає ***глобалізація,*** від якої, вочевидь, залежить й існування та виживання цивілізації. З розвитком Інтернету, засобів зв'язку світ вже підійшов до тієї межі, коли кордони між державами перестали бути нездоланними бар'єрами для багатьох видів діяльності. Але це стосується, на жаль, і таких небезпечних явищ, як тероризм і злочинність.

Так, за даними Міністерства внутрішніх справ України кількість злочинів у багатьох сферах діяльності постійно суттєво зростає, особливо у сфері Інтернет-технологій (рис. 1.12). Компанія Symantec опублікувала рейтинг «Найбрудніших сайтів літа 2009 року»[15]. Згідно з ним, у середньому на кожному з таких сайтів міститься близько 18 000 обра-

[15] Джерело — Cybersecurity.

зів шкідливого програмного коду, небезпечних посилань, схованих фреймів та інших небезпек, а лідер серед них — сайт, присвячений громадському харчуванню, — містить усього на один домен 23 414 комп'ютерні загрози! У Symantec свідчать, що ці дані говорять про дві речі: по-перше, про гігантський розмах діяльності творців шкідливих кодів, а по-друге (і головне), про вихід Інтернету на перше місце в категорії засобів доставки шкідливих кодів.

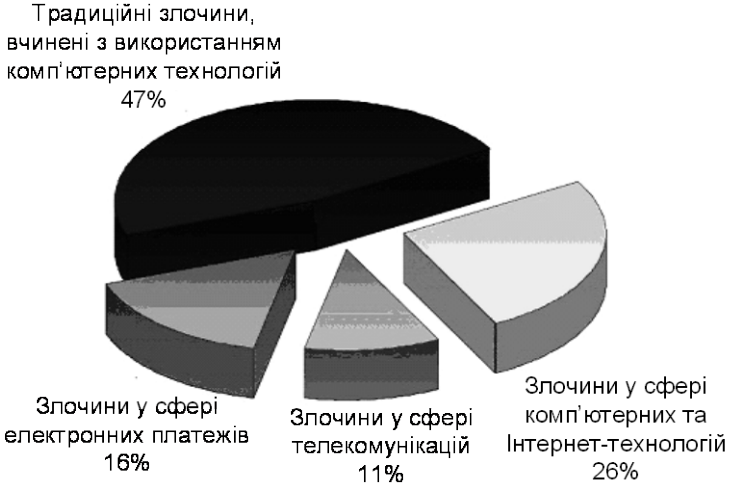

Рис. 1.12. Структура комп'ютерних злочинів

Не буде перебільшенням сказати, що в світі вже йдуть численні ***інформаційні війни*** різних масштабів (*інформаційна боротьба, інформаційне протиборство, інформаційні операції* — це вже досить поширені поняття), які завдяки віртуальній сфері їхнього проходження ми не помічаємо, поки ми самі, або підприємства, установи, де працюємо, раптом не опиняться у самому пеклі цих протистоянь [115].

Колишній глава ЦРУ Джордж Тенет ще в 2004 р. назвав Інтернет «ахіллесовою п'ятою США» і «чорним ходом» для терористів і ворогів. Водночас американська асоціація компаній, що спеціалізуються на комп'ютерній безпеці (CSIA), звернулася до державного керівництва США, у якому також призвала адміністрацію найсерйознішим образом зайнятися питаннями національної безпеки в Інтернеті. Інакше, на думку фахівців, вороги Америки можуть одного разу організувати потужну й несподівану кібератаку на мережі державного значення.

З тих пір ситуація на краще не змінилася. Так, уже в перші дні приходу до влади Президента США Б. Обами (2009 р.) незалежна експертна комісія Центру зі стратегічних і міжнародних досліджень підготувала для нього спеціальну доповідь[16], в якій зазначено, що «у кіберпросторі війна вже почалась», а населенню Сполучених Штатів доводиться вести «невидиму битву з військовими й спецслужбами іноземних держав». Водночас стверджується, що Америка, як найбільш комп'ютеризована країна світу, є більш уразливою у віртуальному просторі, ніж інші держави. «Це битва, що ми програємо», — додає група експертів, які підготували даний документ.

Експерти Центру підтвердили, що в 2007 році Міністерство оборони, департаменти державної й внутрішньої безпеки, Національне управління США з аеронавтики й дослідженню космічного простору (НАСА) серйозно постраждали через численні атаки «невідомих іноземних хакерів». «Міноборони щодня зазнає сотні тисяч спроб атакувати його комп'ютерні системи. В результаті терабайти інформації загублено», — констатують експерти. При цьому робиться висновок, що фронт невидимої боротьби проліг у битві за доступ до інформації і головними суперниками Вашингтона стали вже не хакери-одинаки, а спеціально створені служби на державному рівні.

Справа дійшла навіть до того, що врешті-решт американські сенатори[17] підготували проект білля, що надає президентові США другу «червону кнопку», за допомогою якої у випадку надзвичайних ситуацій в ім'я національної безпеки президент зможе відключати доступ до Інтернету[18]!

Відмінною рисою наших часів став також перехід кіберзлочинників від хуліганських міркувань до заробітку грошей. Епоха комп'ютерних вірусних епідемій, самореклами або питань помсти вже з 2002–2003 рр. почала відходити в минуле[19]. Зараз кіберзлочинність приносить доходи, порівнянні з наркоторгівлею. За даними казначейства США, у 2006 році прибуток кібершахраїв склав десь 100 млрд доларів.

Це підтверджує й традиційний щорічний звіт (за 2008 р.) компанії Symantec про стан безпеки в Інтернеті. На чорному ринку атаки на сервери й сайти продаються й купуються. Люди торгують не тільки шкід-

[16] Джерело — SecurityLab.
[17] Демократ Джон Рокфеллер і республіканка Олімпія Сноу.
[18] Як відомо, кореневі сервери всесвітньої Мережі знаходяться в США.
[19] За даними глобального центру досліджень і аналізу загроз «Лаборатории Касперского».

ливими програмами, але й цілими арміями заражених комп'ютерів, об'єднаних у так звані ботнети, які здатні розсилати океани спаму та армади шкідливих програм [20].

Злочинці «заробляють» також значною мірою й на викраданні персональних даних. При цьому украдені особові дані заносяться до прайс-аркуша й навіть забезпечуються гарантією. За даними Symantec 80 % шкідливого програмного забезпечення спрямовано саме на крадіжки конфіденційної інформації.

Загальновизнаними є декілька типів інформаційних війн[21] — це й боротьба з пунктами управління та зв'язку супротивника (*Command& Control Warfare*, *C2W*) і за отримання інформації про стан його сил і ресурсів у режимі онлайн, і радіоелектронна боротьба, психологічна війна (операції проти національної свідомості, операції проти керівництва країною, операції проти військ і культурні експансії — *Psychological Operations, PSYOP*), «хакер–війна» (боротьба проти комп'ютерних систем супротивника — *Computer Network Attack, CNA*), блокування або контроль економічної інформації для отримання економічного домінування.

Вже прийшов і той час, коли описані фантастами так звані «кібервійни» стають реальністю. На тлі зникнення відкритих глобальних вірусних епідемій та падіння популярності хробаків і вірусів зростання сигнатур у базі «Лаборатории Касперского» склало приблизно 200 %. Це викликано тим, що зараз 92 % реальних загроз пов'язані з троянськими програмами, при цьому спостерігається еволюція шкідливих технологій, коли багато програм стають здатними до самореплікації, адже чим далі, тим ширше будуть поширюватися автоматизовані системи, що самоепліцируються. На думку експертів з безпеки «Лаборатории Касперского», «війна людей проти людей вже практично закінчена, зараз б'ються роботи проти роботів».

Прикладом ефективної кіберзброї для нелегальної діяльності — розсилання спаму, перебору паролів на віддаленій системі, для атак типу DDoS («відмова в обслуговуванні») є комп'ютерні мережі, що складаються з безлічі хостів із запущеними «ботами» (автономним програмним забезпеченням, установленим за допомогою комп'ютерних вірусів). Хазяїн зараженої машини, як правило, навіть не підозрює про те, що вона використовується зловмисниками. Саме тому такі комп'ютери називають ще зомбі-машинами.

[20] Джерело — Компьюлента.

[21] За класиком і ідеологом інформаційних війн Мартином Лібіки (Libicki).

У цій ситуації об'єктами підвищеної інформаційної небезпеки стають органи влади, до якої кіберзлочинці мають підвищений інтерес. Так, згідно із статистикою різного роду мотивів при здійсненні комп'ютерних злочинів поряд із корисливими політичні мотиви займають досить відчутне місце[22] (рис. 1.13).

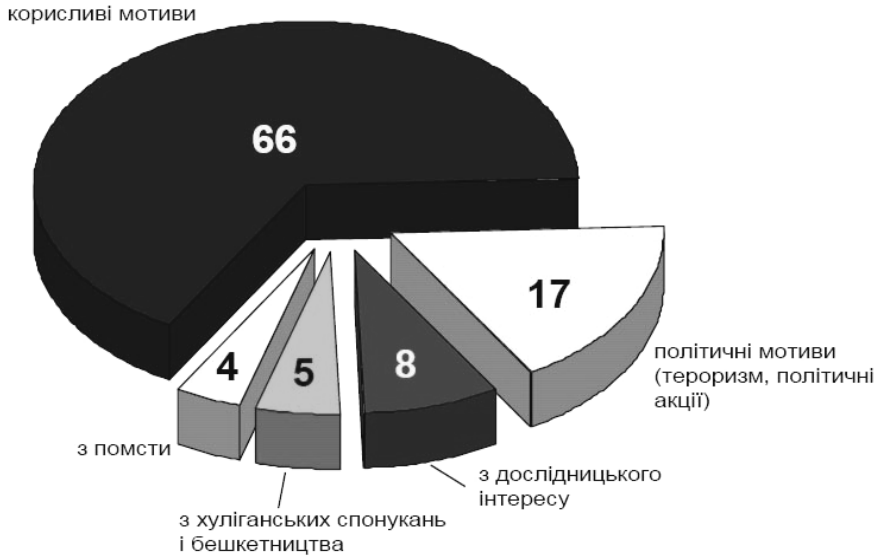

Рис. 1.13. Співвідношення різного роду мотивів при здійсненні комп'ютерних злочинів (у %)

Наразі зростає потенційна загроза того, що закордонні спецслужби, а також терористичні, екстремістські угруповання чи організовані злочинні групи можуть вдаватися до спроб здобуття недозволеного доступу до інформації, яка не підлягає розголошенню та циркулює в системі органів влади.

Через інформаційні порушення в діяльності органів влади можуть бути створені перешкоди в сфері таких державних інтересів, як прийняття найважливіших політичних, економічних й інших рішень, співпраця України з іншими державами, підтримка міжнародного авторитету й іміджу України, підтримка на належному рівні функціонування

[22] За даними МВС України.

систем управління енергосистемами, інженерних служб, телекомунікаціями, військами, озброєнням, військовою технікою, нарешті, економічна та соціальна стабільність у різних сферах суспільного життя. Внаслідок порушень вимог інформаційної безпеки органу влади може бути також створена атмосфера напруженості і нестабільності в роботі штатних працівників, спровоковані службові конфлікти, дискредитовані самі органи влади і установи державного управління тощо.

В умовах функціонування «електронного уряду» соціально-економічний збиток суспільству від порушень ІБ може мати вираз у нанесенні істотних матеріальних і моральних збитків громадянам, втрати або некоректного використання персональної інформації, що може вплинути негативним чином на їхнє відношення до уряду і державної влади в цілому.

За даними вже згаданого звіту Infowatch-2007 серед найбільш суттєвих утрат від витоку інформації на другому місці знаходиться зниження репутації організації (вказали 42,3 % респондентів), а на третьому — втрата клієнтів (36,9 %).

Обумовлена сучасними обставинами взаємозалежність технологій і сфер діяльності, процеси інтеграції АІС у різних сферах ведуть до потенційної уразливості, техногенної небезпеки. Насамперед це стосується так званих, с точки зору національної безпеки, критичних інфраструктур суспільства — енергетичних систем, інженерної інфраструктури, систем транспортування ресурсів, особливо в надзвичайних ситуаціях [116] (рис. 1.14).

Діяльність у сфері захисту критичної інфраструктури бере свій початок з формування американської Президентської комісії із захисту критичної інфраструктури (Presidents Commission for Critical Infrastructure Protection) ще у 1996 році. Звітна доповідь цієї комісії виявила уразливість національної безпеки США в інформаційній сфері. Підсумки роботи комісії були покладені в основу урядової політики в сфері забезпечення інформаційної безпеки критичної інфраструктури, сформульованої у відповідній Директиві Президента (PDD-63)[23].

На жаль, певні загрози ІБ існують й у інформаційному просторі державної влади, і в середовищі окремого органу влади. Можна стверджувати, що одна з основних загроз інформаційній безпеці знаходиться саме в сфері діяльності органів державної влади, зокрема у невиконанні або неналежному виконанні органами державної влади своїх повнова-

[23] http://www.agentura.ru/equipment/psih/info/war/

жень. Мабуть тому аналітики вважають, що сучасний розвиток України характеризується тим, що основними загрозами її національній безпеці є саме внутрішні [23].

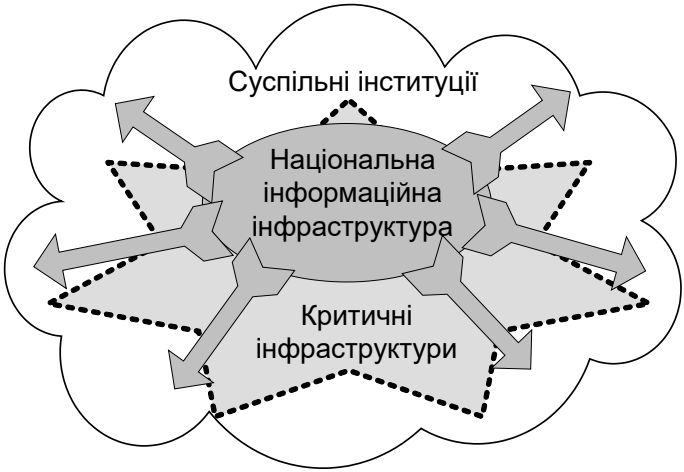

Рис. 1.14. Взаємозалежність критичних інфраструктур суспільства та НІІ

За даними обзору Global Information Security Survey 2004, Ernst& Young, серед десяти головних загроз інформаційній безпеці на другому місті знаходяться неправомірні дії працівників з інформаційними системами, а на четвертому — витоки конфіденційної інформації. Проблема інсайду — загроз безпеки інформаційних систем від власних працівників — стала головним трендом останніх років у багатьох організаціях і продовжує тільки загострятися.

У цьому зв'язку вбачається, що атаки хакерів, хоча й є дуже небезпечними, але не становлять головної загрози для безпеки влади. Існують й інші суттєві чинники, що пов'язані з інформацією, яка на сьогодні стає важливим ресурсом прийняття владних рішень.

Ще в 1982 році футуролог Джон Нейсбіт у праці «Мегатренди» вказував, що будь-яка нова технологія супроводжується компенсаторною гуманітарною реакцією. Стосовно інформаційних технологій це має означати, що культура поводження з інформацією повинна домінувати над рівнем опанування цих технологій. Тут доцільним може бути приведення висловлення відомого авторитета ІТ-бізнесу та передбачень у сфері використання інформаційних технологій Б. Гейтса: «Саме те, як

ви збираєте, організуєте та використовуєте інформацію, визначає, переможете ви або програєте».

Останніми роками сформувалася тенденція неухильного зростання кількості інцидентів з витоком інформації й загального масштабу цієї проблеми. Компанією InfoWatch було проведено глобальні дослідження інцидентів внутрішньої інформаційної безпеки за 2008 р. Було проаналізовано всі витоки конфіденційної інформації, що згадувалися в ЗМІ у всіх країнах світу й у всіх галузях[24]. За цими даними серед усіх інцидентів витоки персональних даних займають аж 97,5 %, а доля державних установ серед різних типів організацій сягнула вже майже 20 %. В умовах «електронного уряду» ці дані свідчать про існування реальних загроз для інформаційної безпеки влади.

Адже таке нове поняття як «персональні дані» (ПДн) є досить складним і потенційно уразливим. Розповсюджено поділ ПДн на 4 категорії[25]. До найпростіших відносяться знеособлені й (або) загальнодоступні персональні дані, а також інформація, що дозволяє ідентифікувати суб'єкта ПДн. Дві ж інші категорії дозволяють не тільки ідентифікувати суб'єкта, але й одержати про нього додаткову інформацію, зокрема таку, в якій відбиті расова, національна приналежність, політичні погляди, релігійні й філософські переконання, стан здоров'я, інтимне життя. Зрозуміло, що такі дані потребують найбільш серйозного захисту.

За даними американського центру дослідження злочинів, пов'язаних із розкраданнями персональних даних (Identity Theft Resource Center, ITRC)[26], у 2008 році на території США відбулося як мінімум 656 публічних витоків інформації (рис. 1.15).

Це значення на 47 % перевершує показники 2007 року й більш ніж у чотири рази — дані за 2005 рік. Традиційно найбільший збиток принесли витоки з комерційного (36,6 %) та з фінансового сектора (52,5 %) — на них прийшлося більше третини всіх потерпілих. Але вже стає досить помітним й державний сектор — на нього у 2008 році припало 16,8 % інцидентів.

Ще одна небезпечна тенденція, що спостерігається у світі — це істотне зростання кількості навмисних витоків у порівнянні з 2007 роком — з 29 до 45 % (за даними InfoWatch). І це також пов'язується із зростанням вартості та ліквідності персональних даних. Крадіжка особистості (*identity theft*) поставлена на потік, й у цей кримінальний бізнес у

[24] http://www.infowatch.ru/

[25] Зокрема, в Законі РФ «О персональных данных» (№ 152-ФЗ).

[26] www.CNews.ru

зв'язку з його технічним спрощенням утягується усе більше виконавців. А коло потенційних потерпілих увесь час розширюється за рахунок впровадження нових форм надання послуг і на нових територіях, у тому числі державними інформаційними системами, зокрема на муніципальному рівні.

Рис. 1.15. Тенденція витоків персональних даних на території США

Так, російський кадровий холдинг «Анкор» навів результати дослідження відношення співробітників IT-компаній до конфіденційних даних[27]. 45 % опитаних визнали, що один раз використовували комерційну інформацію в особистих цілях, а 3 % — що робили це неодноразово. Приблизно 13 % респондентів отримували пропозиції про продаж комерційних відомостей. Водночас респонденти впевнені, що подібного роду дії характерні для третини співробітників у сфері IT.

Серед найзначніших (тобто надвеликих або таких, що зачіпляють найважливішу інформацію) витоків персональних даних, що стали відомими в 2008 році, є й інциденти, пов'язані з державними органами. Хакер зміг викрасти дані із серверів Міністерства освіти про 6 мільйонів громадян Чилі й опублікував їх в Інтернеті. Дані містили ідентифікаційні номери, номери телефонів, домашні й електронні адреси й ві-

[27] Джерело — CNews.

домості про освіту громадян. Італійський уряд у «пориві поліпшення прозорості» опублікував на одному з державних сайтів імена, адреси, відомості про доходи й податковий статус усіх громадян Італії. Але дані все-таки були вилучені із сайту через 24 години після опублікування через скарги італійської організації з питань захисту таємниці приватного життя.

Ще одна загроза — це неефективне витрачання робочого часу в умовах застосування ІТ. Американська компанія Basex, що багато років займається дослідженнями проблем інформаційної перевантаженості, опублікувала сумний звіт за 2008 р. і не менш сумний прогноз, що й у 2009 році ситуація на краще не зміниться[28]. 28 % робочого часу в офісах витрачається на читання непотрібної електронної пошти, спілкування за допомогою месенджерів і ознайомлення з непрофільними електронними публікаціями. До цього треба додати час, необхідний для концентрації на робочих проблемах після серфінгу й вивчення «лівої» інформації. Ще 15 % робочого часу йде на пошук інформації в Інтернеті. Частка невдалих пошукових запитів становить від 30 до 50 % їх загальної кількості, а запити, оцінені користувачами як удалі, не завжди є такими, оскільки містять застарілі або неточні дані. З урахуванням інших факторів (зустрічі, наради, обговорення зі співробітниками), на вирішення головного завдання — створення «продуктивного контенту» залишається лише 25 % робочого часу.

Ситуація з витрачанням робочого часу в органах влади мало чим відрізняється від наведеної. Яскравою ілюстрацією стану справ з виконанням документів в органах влади є оцінка Апарату РНБО України: «Станом на 1 червня 2007 року надійшли строки виконання 433 завдань, з яких за наявною інформацією виконано 188, або 43 % їхньої кількості»[29].

До чого це веде, явно зазначено у Стратегії національної безпеки, де визнається, що на сьогодні в Україні внаслідок неузгодженості дій між різними гілками та органами державної влади має місце низька ефективність механізмів прийняття та виконання державних рішень, зниження професіоналізму державних службовців, поширення корупції, хабарництва, зрощення бізнесу й політики у цьому середовищі.

Як приклад до цього можна навести інформацію про маніпуляції

[28] Джерело — Информзащита.

[29] Довідка до питання порядку денного засідання РНБОУ від 15.06.2007: «Про стан виконання рішень Ради національної безпеки і оборони України» // http://www.rainbow.gov.ua/news/564.html

на державному сайті РФ, що публікує інформацію про тендери, на якому знайдено безліч документів, де частина схожих за начертанням літер кирилиці замінена на латинські, або літера «о» на нуль. Вочевидь, це зроблено для того, щоб їх не могли знайти «непотрібні» виконавці робіт[30]. Також виявлені факти створення перепон пошуковим машинам шляхом блокування індексування більшої частини контенту, або сайт просто закриває потрібний розділ через robots.txt.

Отже нині особливої гостроти набула проблема розриву між демократичною системою влади та її апаратом, що проявляється у постійних суспільних конфліктах, які спричиняються непідготовленістю ухваленого рішення, а іноді й його хибністю або корумпованою спрямованістю, що врешті-решт створює реальну загрозу державній владі. Це відбувається здебільшого не лише через невизначеність початкових умов підготовки рішень, неповну апріорну інформацію про предмет прийняття рішень, про ситуацію, відсутність аналітичного аналізу позицій зацікавлених сторін та обґрунтованого передбачення неминучих наслідків — позитивних, негативних, усіх загроз і ризиків, невизначеність критеріїв оптимальності прийняття рішень, а й через нерегламентоване та неправомірне поводження з інформаційними системами.

Для вичерпної інформованості державного рішення і баченні всіх його наслідків до кожного управлінського рішення в органах влади має бути внутрішній механізм перебору всіх можливих варіантів, а для цього вкрай потрібні й нові технологічні рішення.

Поки ж державні службовці не завжди уявляють, як із застосуванням можливостей сучасних інформаційних технологій аналізувати політичне становище, організовувати консультації з суспільними структурами, працювати з опозицією. Ані уряд, ані урядові структури ще не забезпечують належної інформаційної підтримки своїх рішень.

Водночас, щоб створення «продуктивного контенту» дійсно забезпечувало підтримку прийняття ефективних державних рішень, потрібні оптимізація процедур роботи держслужбовців з інформаційними системами, блокування неправомірних дій з ними, ведення обліку та фільтрації потоків від зовнішніх джерел, тобто впровадження шляхів впорядкування діяльності органів влади, адекватних новим умовам, як необхідних напрямків для забезпечення ефективності роботи влади в умовах застосування засобів ІТ.

[30] Джерело — SecurityLab.

Вочевидь, в умовах, коли обсяги робіт постійно зростають, а часу та ресурсів на їх виконання відводиться усе менше і менше (рис. 1.16), що зараз притаманне держаному управлінню, воно має обов'язково спиратися на регламентовану бюрократичну роботу на базі визначених процедур, дисципліни, певних стандартів документів.

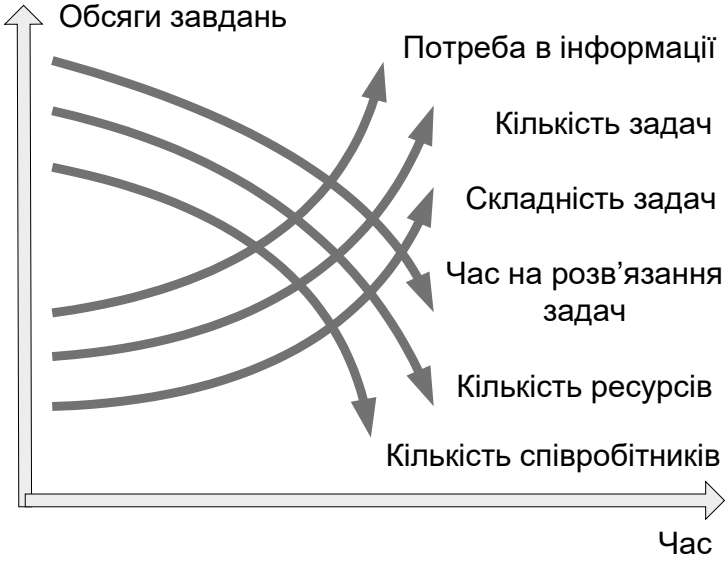

Рис. 1.16. Характеристики стану розв'язання задач в органах влади

У цьому зв'язку вважається за необхідне взагалі формалізувати діяльність державних службовців та розробити стандарти виконання державних функцій із застосуванням ІТ, тобто вичерпний перелік обов'язкових вимог до змісту, порядку здійснення та якості управлінських дій і процедур, що має зробити роботу державних органів максимально прозорою й ефективною. Водночас убачається, що в органах влади має бути введена автоматизована система менеджменту якості відповідно до вимог міжнародного стандарту ISO 9001:2000.

Враховуючи, що інформаційна підтримка діяльності органів влади в сучасних умовах усе більше залежить від засобів автоматизації, автоматизовані системи стають головною ланкою забезпечення ІБ державної влади. У цьому зв'язку слід зазначити. що, мабуть, до традиційних ***засобів забезпечення національної безпеки*** — множини всіх наявних у

державі воєнних, політичних, економічних, правових та організаційних ресурсів, послідовне використання яких спрямовується на реалізацію державної політики національної безпеки, слід віднести й національні інформаційні ресурси, зокрема, інформаційні ресурси органів державної влади.

Потрібно також враховувати, що в кожній із галузей є власні особливості, які насамперед пов'язані з характером вирішення поставлених завдань, наявністю властивих кожному відомству слабких елементів і вразливих ланок з точки зору інформаційної безпеки. Так, у сфері економіки найбільш схильні до впливу порушень інформаційної безпеки система державної статистики, системи збору і обробки фінансової, біржової, податкової, митної інформації, інформації про зовнішньоекономічну діяльність держави і комерційних структур. Значної небезпеки можуть мати наслідки порушень ІБ у силових відомствах, зокрема, вразливими ланками є їхня інформаційна інфраструктура, в тому числі центри обробки і аналізу інформації, пункти управління, вузли і лінії радіозв'язку. Тому у кожній сфері діяльності державної влади потрібна спеціальна організація робіт, а також використання в АІС специфічних форм і методів забезпечення інформаційної безпеки.

При цьому слід звернути увагу на той факт, що віра в те, що установка гарних засобів захисту вирішує проблеми безпеки, вже практично загублена. Збільшення поінформованості фахівців про реальний (і сумний) стан захищеності (а це наслідок збільшення кількості систем захисту інформації) приводить до неминучої думки про те, що самі по собі «залізяка» або програма проблем не вирішують[31]. Вочевидь, ці засоби повинні бути правильно налаштовані, сконфігуровані, надавати персоналу адекватну інформацію про небезпечні інциденти.

Але існує ще один чинник, що є загальним для всіх органів влади і що також значною мірою впливає на рівень інформаційної безпеки влади — це ***ефективність та надійність автоматизованого забезпечення інформаційно-аналітичної діяльності та підтримки прийняття рішень*** державними службовцями всіх категорій. При цьому, якщо звернутися до звіту Pricewaterhouse Coopers, уже в 2008 р. намітився спад придбання компаніями продуктів захисту інформації. На перше місце серед пріоритетів (33 %) виходять питання комплексного забезпечення безпеки користувачів та управління ідентифікацією.

[31] За даними опублікованого в 2008 р. щорічного дослідження з ІБ компанії PricewaterhouseCoopers (The Global State of Information Security 2007).

За тими ж даними Infowatch-2007 найбільш ефективним шляхом запобігання небезпеки інформації є впровадження комплексних рішень на базі сучасних ІТ, зокрема запровадження повнофункціональних DLP-систем (системи запобігання витоків конфіденційної інформації), що мають високу ефективність для захисту від випадкових витоків.

Водночас вказується, що серед головних перепон на шляху впровадження засобів захисту поряд з бюджетними обмеженнями та психологічними чинниками знаходиться й відсутність готових ІТ-рішень.

Поширена загальна думка, що механізмом досягнення інформаційної безпеки є ***захист інформації*** як сукупність засобів, методів, організаційних заходів щодо попередження можливих випадкових або навмисних впливів природного чи штучного характеру, наслідком яких може бути нанесення збитків чи шкоди власникам інформації або її користувачам, інформаційному простору. Як відомо, суттю захисту інформації є забезпечення її доступності при збереженні цілісності інформації та гарантованій конфіденційності.

Але інформаційна безпека перш за все — складова частина національної безпеки, що характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх і внутрішніх загроз. Саме аналіз існуючих джерел загроз дозволяє розглядати поняття інформаційної безпеки значно ширше. У цьому сенсі суть інформаційної безпеки полягає не лише у захисті інформації, що циркулює в інформаційних і телекомунікаційних системах, не лише у захисті інформаційного простору країни та державної влади від небажаного інформаційного впливу, захисті національних інформаційних ресурсів, а й у забезпеченні ефективного функціонування автоматизованих систем, а також у забезпеченні обґрунтованого прийняття рішень в умовах автоматизованої підтримки цих процесів.

Отже, часто використовуваний термін «комп'ютерна безпека», як еквівалент або замінник ІБ, має занадто вузький зміст. Комп'ютери — тільки одна зі складових автоматизованої системи, і безпека інформації, що зберігається, обробляється й передається за допомогою комп'ютерів, визначається всією сукупністю складових інформаційної інфраструктури й процесів, що відбуваються, у першу чергу найслабкішими ланками, якими в переважній більшості випадків виявляється сама людина, чинники опрацювання та зберігання інформації, а також її використання.

Про це свідчить увесь історичний шлях стрімкого розвитку вирішення проблем захисту інформації, що з'явилися з появою комп'ютера

та створення баз даних, а потім й автоматизованих систем, який пройшов від постановки проблеми захисту інформації в автоматизованих системах, ідеї надійного захисту програмними та технічними засобами до усвідомлення теоретичного результату про неможливість абсолютного захисту, до сучасного етапу розуміння багатоаспектності захисту, комплексності та динамічності систем захисту.

Тому з-за навали вищевказаних тенденцій питання інформаційної безпеки набуває усе більшої важливості. Деякі дослідники вважають, що забезпечення інформаційної безпеки необхідно не тільки для того, щоб зберегти недоторканість національного інформаційного простору, але й наполягають на тому, що вірно сформульована національна стратегія в галузі інформаційної безпеки сприяла би більш успішному вирішенню проблем у політичній, економічній, соціальній та інших сферах життя, позитивному ходу розв'язання як внутрішньополітичних, так і зовнішніх конфліктів. У зв'язку з необхідністю забезпечення з боку держави інформаційної безпеки слід розуміти, що в сучасній динамічній ситуації лише шляхом збереження тих явищ та символів, що існують в національній інформаційній сфері, інформаційну безпеку забезпечити неможливо. Нові виклики потребують нових відповідей, тому особливого значення набуває механізм створення в органах влади нової інформації, нових символів, багатоманітність джерел цієї інформації, а для забезпечення інформаційної безпеки особливо важливим є дотримання принципів прозорості в інформаційній сфері та доступності до державної інформації.

Таким чином, якщо система державної влади і, відповідно, ОДВ не еволюціонують разом з навколишнім середовищем (не адаптуються до його змін і викликів) з урахуванням питань інформаційної безпеки, рано чи пізно державна влада буде не здатною виконувати покладені на неї функції. Звідси випливає основна задача державної влади та її ОДВ — постійний розвиток з метою адаптації до змін безпекового середовища, тобто забезпечення обов'язкового здійснення *управління розвитком* [117].

Це обумовлює парадигму *адаптивного органу влади*, який спроможний завдяки застосуванню ІКТ, в умовах постійних трансформацій, змін зовнішнього середовища та невизначеності оперативно пристосовуватись до таких обставин і забезпечувати прийняття в цих умовах обґрунтованих ефективних рішень.

У системі електронного урядування першочерговою задачею органу влади є доступність до інформації у будь-який час будь-якому клієн-

ту з будь-якого місця. В цих умовах рівень розвитку засобів автоматизації в органі влади стає визначальним у реалізації державного управління, а ІКТ виступають головним активом і рушійною силою забезпечення надання управлінських (адміністративних) послуг і підтримки процесів адаптації.

Як відомо, адаптивна або самопристосовуваюча система зберігає працездатність при непередбачених змінах властивостей керованого об'єкта, цілей керування або навколишнього середовища шляхом зміни алгоритму функціонування чи пошуку оптимальних станів. При цьому адаптація з точки зору кібернетики є процесом нагромадження й використання інформації в системі, спрямованим на досягнення деякого, в певному розумінні оптимального, стану чи поведінки системи при зовнішніх умовах, що змінюються, та початковій невизначеності. При адаптації можуть змінюватися параметри і структура системи, алгоритм функціонування, управляючі дії тощо.

Отже, адаптивна система повинна бути керованою, а також спостережуваною і здатною ідентифікуватись по відношенню до самої себе та до зовнішніх впливів. Згідно з цим з метою поліпшення якості роботи органу влади керування ним повинно відбуватися з адаптацією. Це керування має властивості адаптації в тому розумінні, що воно залежить від доступної на даний момент інформації про процес прийняття рішення. Чим повніший інформаційний опис процесу, тим ефективніше рішення буде прийнято. Фактично, забезпечення поліпшення характеристик інформації є суттю адаптації.

Перебудова структури органу влади та алгоритмів роботи з метою адаптації — враховуючи інерційність державного апарата — може відбуватися лише вкрай повільними темпами. Завершені зміни вже можуть виявитись недоречними, тому що у зовнішньому середовищі на той час ймовірно буде панувати інша ситуація. Таким чином, забезпечити процес пристосування органу влади можливо лише завдяки генеруванню в органі влади нового знання та передбачення на основі аналітичних моделей та актуальної і повної інформації.

Тому, фактично, проблема ***автоматизації інформаційно-аналітичного забезпечення прийняття рішень*** у системі влади країни є гострим політичним питанням. Створення інтегрованих інформаційно-аналітичних систем органів державної влади та органів місцевого самоврядування передбачається забезпечити і вже згадуваним Указом Президента України «Про першочергові завдання щодо впровадження новітніх інформаційних технологій».

Тут не буде зайвим привести таку цитату: «Зміни в технологіях відбуваються швидко, і кожен новий крок в їхньому розвитку несе з собою і нові потенційні загрози на додаток до тих, що вже існують. Більшість людей і не усвідомлюють, що до появи багатьох нових технологій можна підготуватися заздалегідь — при грамотному дизайні системи, а також регулярному проведенні оновлень, здатних запобігти виникненню нових проблем»[32].

Отже, питання інформаційної безпеки, зокрема державної влади, обґрунтовано викликають занепокоєння та набувають усе більшої актуальності. Указом Президента України «Про першочергові завдання щодо впровадження новітніх інформаційних технологій» передбачається розроблення нормативно-правових актів і здійснення відповідних першочергових заходів, спрямованих на запобігання злочинності у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж.

У Стратегії національної безпеки України визначається, що життєво важливі національні інтереси України реалізуються у складному внутрішньому та зовнішньому середовищі, яке характеризується низкою викликів і загроз, а забезпечення сприятливих зовнішніх умов для розвитку та безпеки держави передбачає, зокрема, забезпечення інформаційної безпеки при інтеграції до структур глобального інформаційного суспільства. До таких загроз відноситься й наближення до ***критичного стану безпеки інформаційно-комп'ютерних систем у галузі державного управління***, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо.

Враховуючи, що Україна поступово перетворюється на країну з суттєво розвинутим рівнем інформатизації, одну з ключових складових національної безпеки починає займати інформаційна безпека автоматизованих систем у сфері державного управління. Як висновок слід зазначити, що проблема забезпечення інформаційної безпеки державної влади належить до числа проблем, без вирішення яких неможливий повномасштабний і ефективний перехід України до розвинутої економіки, відкритого інформаційного суспільства.

Саме тому Указом Президента України від 23 квітня 2008 року № 377/2008 «Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» передбачається підготовка проекту

[32] Хайнрих Буйсен, менеджер з консалтингу, IDC CEM.

Доктрини інформаційної безпеки України. Таким чином, визначення основних засад розвитку інформаційної інфраструктури державного управління з погляду на вирішення комплексу проблем, пов'язаних із забезпеченням інформаційної безпеки національної інфраструктури, постає досить актуальним.

Забезпечення інформаційної безпеки державної влади має провадитись на основі принципів і положень державної політики з урахуванням усіх заходів щодо захисту інформації в політичній, економічній, оборонній і інших сферах діяльності органів державної влади, що підтримуються відповідними АІС.

І наостанок слід звернути увагу на необхідність у сучасних умовах, з точки зору безпеки, управляти сферою застосування ІКТ в органах влади. На жаль, сьогодні ми ще не завжди знаємо, чим і як управляти... У той же час у США прийнято закон Sarbanes-Oxley (SOX), що регулює створення ефективного контролю в ІС, не заохочує оглядку на витрати по забезпеченню захисту інформації і передбачає досить жорсткі заходи відповідальності за невиконання SOX.

Фактично, мова повинна йти про таке нове питання, як «***ризики процесу інформатизації***»[33]. Воно пов'язане з проблемою протистояння між функціональністю інформаційних систем і їхньою безпекою, тобто суперпозицією «субоптимальності» (коли не можна оптимізувати окремі елементи системи, не погіршуючи при цьому характеристики системи в цілому) і безпеки. Згідно з теорією, можна досягти повної безпеки тільки за умови непрацездатності системи в цілому і навпаки (рис. 1.17). Реально існує якийсь компроміс, знайти який з кожним роком стає все важче, тому що інформаційні системи ускладнюються, а вимоги щодо безпеки ніхто знижувати не збирається.

Зараз питання ризик-менеджменту вступили у той етап розвитку, коли стало необхідним ризики не лише градувати за принципом «малий – середній – великий», а й уводити в практику їхню кількісну оцінку.

Це важливо, зокрема, для обґрунтування ефективності інвестицій в створення АІАС і засоби ІБ та їх співвідношення, що суттєво з огляду на державну бюджетну політику. Адже приклад підприємницького сектору свідчить, що вказані витрати стали останнім часом не просто помітними, а позамежними, наприклад, у банківській або телекомунікаційній сферах.

[33] За матеріалами круглого столу «ИБ на страже бизнеса и госструктур», що був проведений CNews Analytics та CNews Conferences у Москві у 2008 р.

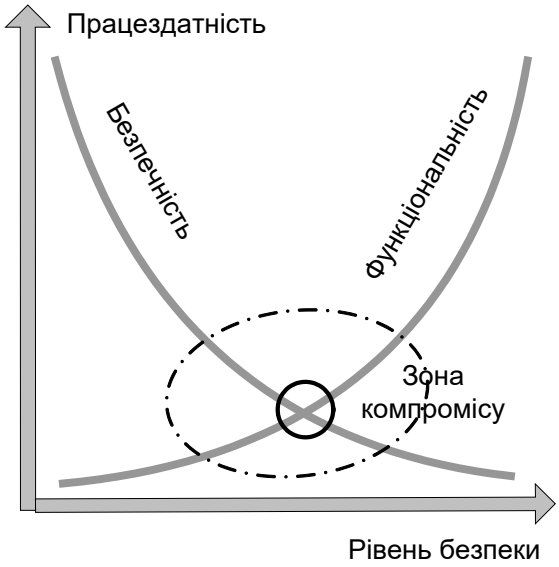

Рис. 1.17. Графік протистояння між функціональністю інформаційних систем та їхньою безпекою

Підсумки до розділу

Взаємозалежність функцій та аспектів державного управління, відкритість влади породжують дуже складне становище, динамічною складовою якого виступає інформація у різних своїх проявах. У сучасних умовах, при необхідності забезпечення стрімкого переходу до інформаційного суспільства, рівень розвитку інформаційно-аналітичного забезпечення управлінської діяльності з використанням нових інформаційних технологій, які дозволяють кардинально змінити взаємовідносини влади та суспільства, набуває вирішального значення. Використання новітніх досягнень комп'ютерної науки та інформаційних технологій у всіх сферах розвитку держави й суспільства, впровадження засобів автоматизації інформаційно-аналітичної діяльності в органах державної влади з метою підвищення ефективності та досягнення якісно нового рівня в управлінні державою привели до необхідності формування в органах державної влади автоматизованих інформаційно-аналітичних систем.

Як складний елемент системи державного управління, як основний засіб у підготовці рішень слід розглядати інформаційний простір державної влади. Його найважливішими складовими є інформаційні потоки, характерна риса яких — їхня масовість. Тому розроблення теоретичних основ інформаційної взаємодії органів державної влади та створення системи інформаційних ресурсів органів державної влади стає актуальним завданням.

Разом з тим, розглядаючи реальні механізми опрацювання інформації в органах влади, слід зазначити, що цільова функція збору, обробки, збереження даних у більшості випадків або вкрай неефективна, або цілком ігнорується. Інформаційні процеси здійснюються спонтанно, без використання наукових розробок, теорії побудови сучасних інформаційних систем. Усе це, зокрема, не дозволяє створити умови для забезпечення необхідного рівня інформаційної безпеки державної влади країни.

У кожній сфері діяльності державної влади потрібна спеціальна організація робіт з забезпечення інформаційної безпеки, використання специфічних форм і методів. Але існує ще один чинник, що є загальним для всіх органів влади, і в не меншому ступені впливає на рівень інформаційної безпеки влади — це ефективність і надійність автоматизованого забезпечення інформаційно-аналітичної діяльності та підтримки прийняття рішень.

У сучасних умовах автоматизовані інформаційно-аналітичні системи в органах влади є головними елементами забезпечення інформаційної безпеки. Але переважна кількість публікацій та досліджень щодо вдосконалення інформаційно-аналітичної діяльності в органах влади на основі автоматизації присвячені лише окремим питанням створення конкретних АІАС, не розкриваючи загальних тенденцій, підходів і положень. Внаслідок цього на теперішній час не існує ані методів інтеграції елементів інформатизації органу державної влади в єдину систему, ані концептуальних чи інформаційних моделей таких систем.

РОЗДІЛ 2

ОСОБЛИВОСТІ СТВОРЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ

2.1. Основні класи задач, що розв'язуються в органах влади, та їхнє інформаційне забезпечення

Деталізація функцій органів державної влади. Процеси управління, що підтримуються органами влади, реалізується в управлінських рішеннях, які є заключною фазою збирання й обробки інформації. Особа, що приймає рішення (керівник підрозділу чи органу влади) у рамках своїх посадових повноважень робить вибір з множини альтернатив, який спрямований на досягнення цілей управління та визначення подальших дій з впливу на об'єкт управління [118–120].

Як вже вказувалося, характерними сучасними умовами діяльності органів влади є збільшення динаміки змін усіх процесів, багатозв'язність, підвищення чутливості до змін не тільки безпосередніх, але навіть непрямих характеристик зовнішнього середовища, збільшення кількості, глибини, інтенсивності, нелінійності зворотних зв'язків і т.д., що потребує значного збільшення кількості інформації для опрацювання та веде до інтенсивного скорочення життєвого циклу прийняття рішень.

У сукупності перераховані тенденції спричиняють, з одного боку, збільшення розмірності й ускладнення процесів управління, а з іншого — роблять життєво необхідним підвищення ефективності управління, під якою, за визначенням В.М. Глушкова [84], розуміється своєчасність, комплексність й оптимальність прийнятих рішень.

Якщо розглянути основні класи задач, що розв'язуються в ОДВ, то слід виділити фактично три класи: 1) отримання інформації та обмін нею; 2) аналіз інформації; 3) прийняття рішень і доведення їх до суспільства (рис. 2.1).

Функціонально ***інформаційні задачі*** є переважаючими. Вони пов'язані із збиранням інформації за напрямками діяльності про ситуацію в суспільстві і в світі, про стан об'єктів управління, первинною обробкою та збереженням інформації, її аналітичним опрацюванням, а також доведенням рішень до суспільства та підлеглих об'єктів.

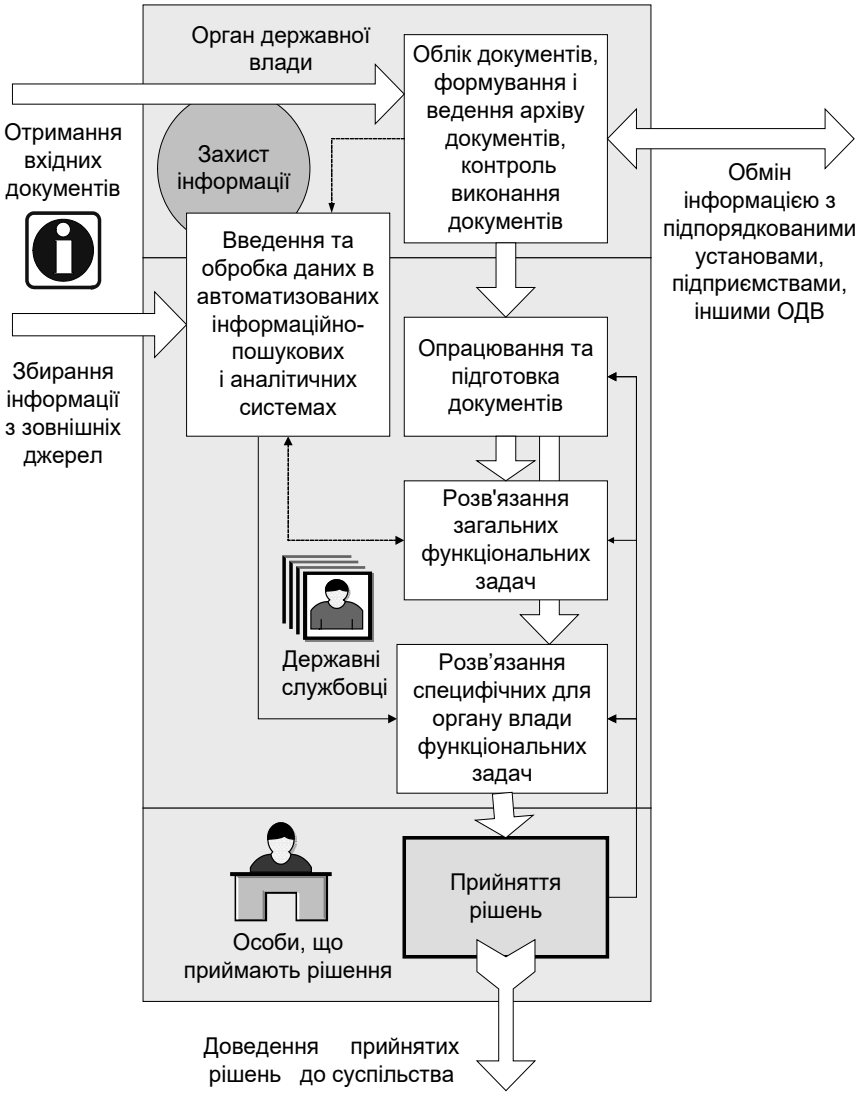

Рис. 2.1. Основні класи задач управління в органі влади

Однак при цьому слід зазначити, що технології розв'язання задач в органах влади ще відстають від розвитку теоретико-методологічного базису та потреб практики, й зорієнтовані в основному на безперспективні спроби адаптації консервативних структур і методів автоматизо-

ваного управління до нових вимог у рамках традиційних підходів, у той час як кардинальні зміни можливі тільки при реалізації принципу нових задач за Глушковим [82].

Слід окремо звернути увагу на задачі прийняття рішень в ОДВ. Зазвичай вони мають не одну, а кілька цільових функцій (критеріїв оптимальності, ефективності й т.ін.), у них не існує єдиного аспекту або єдиної властивості, що оцінює якість прийнятого рішення, тобто вони є багатокритеріальними. Прийняття багатокритеріального рішення полягає у виборі такої альтернативи з множини, яка не є оптимальною (або близької до неї) за жодним з критеріїв, але виявляється прийнятною для всієї множини критеріїв (компромісна альтернатива) [121–128].

У зв'язку з цим центральними задачами управління в ОДВ мають бути аналітичні й розрахункові задачі з аналізу отриманої та зібраної інформації і вироблення управляючих впливів. Оскільки управління державою як складною системою є багатоетапним процесом, розв'язання перерахованих задач циклічно повторюється і може бути пов'язане з оцінкою проміжних результатів прийнятого рішення, переплануванням, виробленням додаткових керуючих впливів і контролю їхнього виконання.

Окремі етапи, що складають цикл прийняття рішень, чимало вивчалися й досліджувалися багатьма вченими й практиками. Однак у цій царині також ще багато недослідженого. Наприклад, потребують додаткового вивчення питання формалізації процедур прийняття рішень, задачі керування за сукупністю показників, діалогові процедури прийняття рішень, дослідження всіх питань життєвого циклу рішень, комплексність їхнього розгляду. При цьому важливими та досить актуальними також вважаються питання вивчення факторів невизначеності й ризику.

Але ці питання не становлять основне завдання викладення, тому не шукатимемо глибоких аналогій. Наведений огляд лише зайвий раз підтверджує, що вирішення проблем прийняття рішень в органі влади можливе лише на шляху автоматизації інформаційно-аналітичної підтримки рішень.

Розглянемо більш детально вищевказані основні класи задач з прив'язкою до типових задач, що розв'язуються ОДВ у процесі діяльності, з точки зору їхньої автоматизації та захисту інформації.

1. Збирання інформації, її первинна обробка й узагальнення**.** Інформація як зведення про стан підлеглих ОДВ організацій, суспільного середовища та міжнародного життя подається в основному у вигляді

документів. Зараз підготовка документів здійснюється переважно з використанням комп'ютерних засобів, тому документи формуються й в електронному вигляді, але поки правовий статус мають лише паперові документи.

У процесі підготовки та опрацювання документів виконуються різні операції переважно з використанням офісних програм (текстових редакторів, електронних таблиць тощо). При цьому аналітичних програмних засобів бракує майже в усіх органах влади за усіма функціональними напрямками.

По завершенні підготовки документа він передається в інші ОДВ або установи засобами звичайної пошти, електронної пошти через комп'ютерні мережі, засобами факсимільного зв'язку і т.д. При цьому, як правило, при передаванні електронних копій заходи з захисту інформації не вживаються.

Інформація, що надійшла у вигляді документів у ОДВ насамперед реєструється (вручну чи за допомогою технічних засобів), піддається сортуванню й розподіляється згідно «зонам відповідальності» структурних підрозділів ОДВ і завданням, які вони вирішують. Але при цьому систем електронного документообігу практично не існує (за винятком електронних картотек), практично відсутня реалізація уведення документів в інформаційно-пошукові й аналітичні системи з метою наступного автоматизованого використання.

Природно, що на всіх етапах обробки і передачі інформація повинна бути захищена від витоку, перекручування й псування. Доступ до неї повинен бути суворо розмежований. Але комплексні рішення для захисту електронних документів в ОДВ також поки не застосовуються.

2. Аналіз даних. В інтересах ухвалення правильного рішення аналізу піддаються перш за все безпосередньо документи в паперовому виді, а також іноді й їхні електронні подання. Останнім часом у зв'язку з поширенням Інтернету при аналізі використовується й додаткова інформація, що отримується з різних джерел. У зв'язку із цим можливості використання існуючої аналітичної інформації, що зосереджена в електронних засобах масової інформації, для забезпечення управління державою постійно зростають. Активне використання джерел Інтернет-простору вимагає вжиття в органах влади заходів з антивірусного захисту.

При аналізі даних, як правило, проводиться їх групування та узагальнення за функціональними задачами загального і специфічного для ОДВ характеру, наприклад, планування бюджету, стратегічного планування галузі і т.ін.

3. Прийняття рішень. Цей процес автоматизовано найменше. У більшості випадків тут використовується людський досвід, і навіть при застосуванні комп'ютерних засобів підготовки проектів рішень посадова особа найчастіше корегує ці рішення, зазвичай на папері.

4. Доведення прийнятих рішень. Рішення оформлюється у вигляді керівних документів (дуже рідко електронних), що оприлюднюються, якщо мають суспільне значення, розсилаються в підлеглі установи чи в інші ОДВ.

При розсиланні підготовлених у вигляді документів рішень використовуються засоби звичайної чи електронної пошти, засоби комп'ютерних мереж, а також стандартні засоби електрозв'язку. На цьому етапі також слід сказати про недостатність захищеності інформації.

Далі починається процес реалізації рішень, що може містити для ОДВ, які отримали рішення, ті ж самі етапи і кроки, що й для ОДВ, який це рішення прийняв. Вищий ОДВ організує контроль виконання прийнятого рішення шляхом збору й аналізу звітної інформації, а також додаткових «коригувальних» впливів на проміжних і кінцевих етапах виконання рішення.

Конкретні напрямки діяльності ОДВ з реалізації рішень забезпечуються виконанням ними ряду встановлених функцій. Згідно з наведеним, а також з урахуванням результатів обстеження органів влади з'ясовано, що до функціонального аспекту їхньої діяльності належать різні групи функцій, які можуть бути розподілені на головні, допоміжні та командні функції. При цьому перелік функцій окремого органу влади та їх різноманітність може бути дуже значними.

Крім того, серед функцій управління, за їхнім загальним змістом, виділяються функції цільові та організаційні (тому, до речі, стратегія інформатизації діяльності органів державної влади має базуватись на цільовому та організаційному підходах).

Таким чином, кількість функціональних задач, що в сучасних умовах розв'язуються органами державної влади в процесі управління, є чималою, а загальну їх кількість просто неможливо перелічити [91]. Так, для прикладу, перелік основних завдань, функцій та задач, що розв'язуються в Міністерстві економіки України, діяльність якого забезпечує реалізацію єдиної державної політики економічного і соціального розвитку України, налічує більше 80-ти, які торкаються найрізноманітніших сфер економічного і соціального розвитку України та діяльності її адміністративно-територіальних одиниць.

Окремі органи державної влади у своєму складі мають підрозділи, що займаються питаннями автоматизації (інформатизації) діяльності. Тому крім перерахованих класів задач у загальний перелік варто додати задачі з підтримки (а іноді й розробки) різних програмних засобів і комплексів для автоматизованого розв'язання функціональних задач. Але при цьому в указаних підрозділах найчастіше немає осіб, що відповідають за питання інформаційної безпеки.

Продовжуючи приклад з Мінекономіки, зазначимо, що з-за великої кількості покладених на нього завдань та наявністю багатоцільових функцій у процесі виконання міністерство функціонально взаємодіє з усіма органами всіх трьох гілок державної влади, органами місцевого самоврядування, міжнародними організаціями, іноземними державами, співтовариствами, союзами, об'єднаннями, внаслідок чого має складну організаційну структуру своїх підрозділів, які територіально розповсюджені.

Останні чинники приводять до того, що інформаційна взаємодія такого органу влади з міністерствами та відомствами, іншими установами є дуже інтенсивною, але здійснюється шляхом обміну в основному паперовими документами та іноді електронними.

У середньому орган влади забезпечує за рік обробку:

а) на рівні міністерства — 80–100 тисяч вхідних документів; 50–80 тисяч вихідних документів і 50–70 тисяч звернень громадян;

б) на рівні державного комітету — 15–25 тисяч вхідних документів; 10–15 тисяч вихідних документів і 5–8 тисяч звернень громадян;

в) на рівні обласної державної адміністрації — 8–12 тисяч вхідних документів; 7–9 тисяч вихідних документів і 5–7 тисяч звернень громадян.

Формат і зміст паперових документів регламентуються відповідними нормативними актами. Окрім регламентованого документообігу, звичайно, існує і нерегламентований, який часто приймається «до відому» і не завжди підлягає подальшому опрацюванню, формуючи такий собі «документний спам». Так, за даними канцелярії Мінекономіки, за 2000 рік було проведено орієнтовно 98700 вхідних і 23000 вихідних документів.

Явища масовості інформаційних потоків і розвитку супутніх проблем опанування «інформаційного вибуху», таких як «астрономічні» цифри обсягу документопотоків, стали взагалі характерною рисою сучасності, тому вони не оминули й органи влади, і не лише в нашій країні, а й за кордоном. Так, за даними джерела «OMB. E-Government Strategy. Simplified Delivery of Services to Citizens», міжвідомча взаємо-

дія в США тільки за ключовими загальнодержавними процесами складається з 28 процесів. У середньому один процес виконують 19 урядових агентств, кожне з них підтримує в середньому 17 процесів, тобто в цілому матриця взаємодії містить 495 процесів, кожен з яких, зрозуміло, виражений у безлічі документів, якими обмінюються агенції.

Тому поняття інформаційно-аналітичної діяльності в органі влади вже сприймається передусім як сукупність дій та заходів на основі методів і засобів збору, накопичення, обробки та аналізу значної кількості даних із застосуванням інформаційних технологій.

2.2. Автоматизовані системи в органах влади

Вихідні дані для аналізу стану інформатизації органів влади. Отримати вихідні дані для проведення аналізу з метою з'ясування стану інформатизації органів влади, наявності функціонуючих автоматизованих інформаційних систем, оцінки інформаційної взаємодії (документообігу) між ОДВ, виявлення потреб ОДВ у спільних інформаційних ресурсах, необхідних даних для побудови телекомунікаційного середовища поки що є непростою задачею. На початку 2000-х років фахівцями Інституту кібернетики ім. В.М. Глушкова було проведено спеціальне обстеження певної частини органів влади, серед яких Секретаріат Кабінету Міністрів, Апарат Ради національної безпеки і оборони, Рахункова палата, Міністерство внутрішніх справ (МВС), Міністерство економіки, Міністерство з надзвичайних ситуацій (МНС), Міністерство оборони, Міністерство транспорту, Міністерство фінансів, Держкомзв'язку, Держкомкордон, Держкомстат, Державна служба експортного контролю, Київська міська держадміністрація, Одеська облдержадміністрація[34], деякі результати якого наведені у [129]. Крім того, Державним департаментом з питань зв'язку та інформатизації (Держзв'язку) Міністерства транспорту та зв'язку України щорічно проводиться моніторинг стану інформатизації регіонів України. Також упродовж 2007 року за ініціативи та підтримки Міжнародного фонду «Відродження», допомоги Секретаріату Кабінету Міністрів України проведено дослідження «Електронне урядування в Україні: аналіз та рекомендації».

За результатами цих обстежень складено уявлення про загальний стан інформатизації органів влади та інформаційної безпеки, про існуючі тенденції у створенні автоматизованих систем в органах влади країни.

[34] Такі назви і статус органи влади мали на період обстеження

Автором проведено також аналіз та оцінку існуючих підходів до побудови автоматизованих ІАС в органах державної влади з виявленням особливостей використання сучасних інформаційних технологій та автоматизації інформаційно-аналітичної діяльності в органах державного управління різних країн, у тому числі далекого зарубіжжя та СНД.

Ґрунтуючись на результатах проведеного аналізу, складність і розміри проблем створення систем автоматизації державного управління у масштабах цілої держави породжує ряд суттєвих труднощів при створенні таких систем, об'єктивно притаманних даного роду системам не тільки в Україні, а й у всьому світі. Ці проблеми пов'язані із визначенням цілей, особливостями проектування, з характером і шляхами використання таких систем.

Попри ці та інші об'єктивні труднощі, як показує вітчизняний та світовий досвід, завдання автоматизації та інформатизації сфери державного управління набувають усе більшої актуальності і потребують вирішення на найвищому організаційному, науковому та технологічному рівні.

Особливості автоматизації інформаційно-аналітичної діяльності в закордонних органах державного управління. Розглянемо на конкретних прикладах, які підходи до використання сучасних інформаційних технологій застосовуються в урядових установах розвинутих країн.

Світовим лідером у сфері автоматизації урядових інституцій є Канада. Відправною точкою процесів автоматизації є урядова ініціатива Government On-Line (GOL), тобто створення системи електронного уряду, що впроваджується ще з кінця минулого століття і базується на всебічній інформатизації як органів влади, так і інших державних установ. Ця ініціатива законодавчо відрегульована актом про доступ до інформації (*Access to Information Act*), прийнятим ще в 1983 р. з уведенням у дію через три роки, в який після цього вносились правки. Головна мета цього акту — забезпечення більш інформованого діалогу між політичними лідерами й громадянами, поліпшення прийняття рішень і збільшення відповідальності федерального уряду і його установ.

У 2000 р. урядом Канади було оголошено про створення Цільової групи огляду доступу до інформації (Access to Information Review Task Force) з мандатом розглядати існуючі законодавчі та адміністративні проблеми щодо доступу до інформації. Звіт групи, оприлюднений у 2002 р., містить фундаментальні дослідження щодо реалізації права до-

ступу громадян до урядової інформації в Канаді та в інших країнах і рекомендації для вдосконалень цього процесу [130].

Ключовим моментом цього документу, що став керівним при створенні систем *е*-уряду в різних країнах, є забезпечення своєчасного і адекватного опрацювання в урядових агенціях запитів громадян з усіх питань (*request processing*). Для цього визначені такі принципи:

- якщо Канада має процвітати й конкурувати, урядова інформація повинна бути доступною широко й легко, наскільки це можливо, через розмаїтість каналів;
- сучасні технології забезпечують потужні й рентабельні способи поширити великий обсяг урядової інформації;
- не може існувати гарного доступу до інформації без ефективного інформаційного управління;
- після 20 років Акт усе ще не дуже добре розуміється громадянами, третіми сторонами, які поставляють уряду інформаційні засоби, і навіть органами місцевого управління й обслуговування. Є невідкладна потреба в збільшенні освіти у питаннях доступу до інформації;
- кількість запитів населення до уряду постійно зростає, але і їхній фокус також усе більше є різноманітним. Запити стали гострішими і суттєвішими. Шляхи використання інформації, також ускладнюються;
- державні службовці скаржаться на час і ресурси, необхідні для відповіді на дедалі більш великі й складні запити, на нестачу ясності в правилах, на шляхи, якими розслідуються скарги тих, хто робить запити;
- критичним є зміцнення культури таємниці в урядових закладах, а також нестача зобов'язань відносно слідування принципам Акту;
- забезпечення доступу канадців до інформації повинне бути визнане як законний і основний аспект щоденної роботи кожного державного службовця;
- офіс Спеціального уповноваженого з питань інформації — важлива установа канадського уряду, що має підтримуватися й забезпечуватися повноваженнями й ресурсами для виконання його стимулюючої ролі нагляду;
- адекватне забезпечення ресурсами всіх компонентів системи (автоматизовані системи, програми, центральні агентства, що забезпечують підтримку, офіс Спеціального уповноваженого з питань інформації) є критичним. Доступ до інформації повинен бути забезпечений ресурсами так само, як і будь-яка інша програма, що проводиться урядом;

- забезпечення інформаційного режиму федерального доступу є в значній мірі подібним як у Канаді, так і за кордоном. Виклики й проблеми разюче ті ж самі: своєчасність відповідей, управління інформацією, прозорість нових сервісів органів влади, зростання керівних запитів, ресурси реалізації програм доступу, ефективний нагляд і вирішення суперечок, нарешті, необхідність вирівнювання стану зі створенням і підтримкою доступу до інформації як на політичному рівні, так і в комунальному обслуговуванні.

Хоча безпосередньо питання створення автоматизованих інформаційних систем та технологій у звіті не розглядаються, але, по-перше, визначений перелік проблем, рекомендацій, шляхів реалізації доступу до урядової інформації обумовлює вичерпне зведення вимог до їхнього створення. Зокрема у звіті визначено низку бар'єрів, що існують на шляху забезпечення одержання й обробки запитів за допомогою автоматизованих засобів, а саме:

- необхідність перевіряти статус того, хто робить запит, як будь-якого громадянина-канадця, постійного резидента або будь кого, хто фізично перебуває в Канаді;
- нестача у багатьох урядових установах коштів на оплату за послуги електронної пошти;
- нестача у багатьох урядових установах автоматизованих систем управління обробкою запитів або невідповідність існуючих технологій обробці великого обсягу запитів;
- відсутність інформаційних стандартів усіх урядових установ і сумісності програмного забезпечення з обробки запитів;
- необхідність забезпечення проведення ефективних електронних досліджень відповідей на запити, що залежить від наявності системи надійного електронного керування документами, яка забезпечує гарантію, що всі існуючі версії всіх документів можуть бути знайдені і що цілісність звітів буде захищеною.

Важливе місце у звіті приділяється розвиткові Інтернету та створенню веб-сайтів у всіх урядових агенціях, урядового веб-порталу, а також принципів їхнього ведення. Тому уряд Канади забезпечує надання найбільш потрібних послуг для населення через Інтернет, при цьому урядові веб-сайти легко ідентифікуються та прості в навігації, що забезпечує значний відсоток користувачів урядових послуг (рис. 2.2)[35]. Трансакції з ними надійно захищені, забезпечуючи й захист персональ-

[35] Джерело — генеральне консульство в м. Сіетл, Канада та компанія Microsoft.

них даних. У країні є й чимало веб-сайтів «канадського електронного уряду», що ведуть неурядові організації.

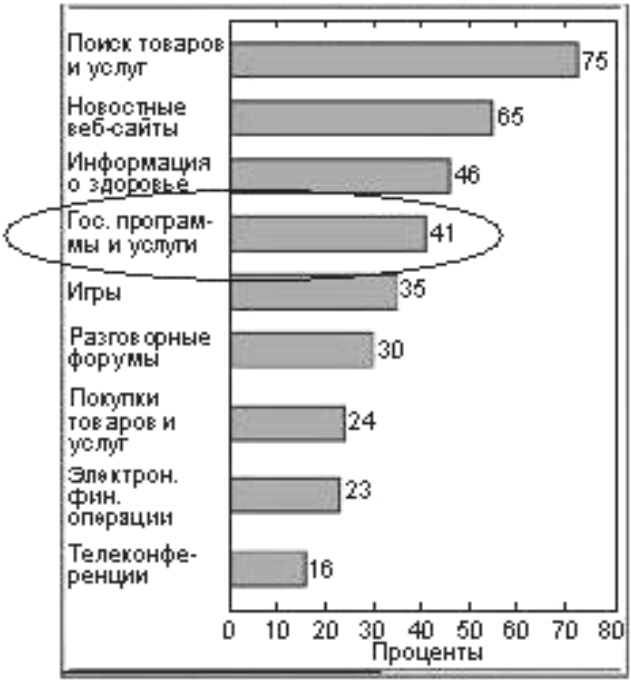

Рис. 2.2. Користування громадянами Канади ресурсами Інтернету

Таким чином, головними пріоритетами канадського уряду щодо формування електронної інфраструктури визначено:

- структура для керування інформацією (*Information Management — IM*);
- формування співтовариства IM/IT;
- інфраструктура відкритих ключів (*Public Key Infrastructure — PKI*);
- електронний уряд (*Government On-Line — GOL*);
- доступ до інформації;
- нормативна база та стандарти IM/IT.

Слід зазначити, що питання керування інформацією є головним з наведених пріоритетів, воно проходить «червоною ниткою» через усі

електронні ініціативи канадського уряду. Достатньо процитувати з цього приводу висновок Міжнародної ради архівних установ (*International Council on Archives*)[36]: «*The management of recorded information is a cornerstone of any government's ability to ensure the degree of openness, accountability and integrity necessary to fulfill the government's basic responsibility to serve the public interest*».

Концепція безпеки канадської електронної інфраструктури **передбачає** реалізацію технологій захисту інформації на всіх рівнях інформаційної системи та забезпечує:

1) автентифікацію суб'єктів;

2) контроль доступу до об'єктів;

3) підтвердження цілісності документів із застосуванням електронного цифрового підпису;

4) захист інформації за допомогою засобів шифрування.

Реалізація цих вимог значною мірою пов'язана із застосуванням засобів інфраструктури відкритих ключів. Використовуючи PKI, урядова агенція забезпечує:

1) захист персональної (не класифікуємої) інформації й комунікацій, внутрішніх і зовнішніх;

2) захист конфіденційної та таємної інформації;

3) гарантії конфіденційності й ідентифікації, цілісності даних і автентичності.

Однією з перших урядових автоматизованих систем стала започаткована ще у 1998 р. за ініціативою Казначейства Канади система RDIMS (Records/Document/Information System), що інтегрувала 6 компонент — керування електронними документами, керування інформацією, WorkFlow, Imaging, керування контентом, звітність (Reports) та підтримувала 100 тис. робочих місць.

Система призначена для поліпшення інформаційних методів управління у канадському уряді за допомогою розвинутої загальної інфраструктури інформаційних технологій і керування інформацією (IM/IT), а також для поліпшення доступ до інформації, розподіленої по всім урядовим агенціям.

Система полегшує процеси одержання, зберігання, організації, класифікації, відновлення, використання інформації, оптичного розпізнавання, захисту інформації, автоматично класифікує інформацію, за-

[36] http://www.ica.org

безпечує санкціонований доступ публікою, забезпечена законодавчою та нормативною базою, інтегрується з іншими системами.

Система будується на базі таких продуктів, як Documentum RM, OpenText Livelink, Hummingbird RM. Для формування звітів використовується Crystal Enterprise Pro 10 Crystal Reports. Системне програмне забезпечення складається з Microsoft SQL Server та СКБД Oracle, Windows 2000 Server/Advanced Server, Windows 2003 Server, Novell NetWare, Microsoft Internet Information Server.

Іншою великою урядовою системою є Проект стратегії фінансової інформації (Financial Information Strategy Project — FIS), спрямований на забезпечення формування корпоративною й відомчою фінансовою інформаційною інфраструктурою уряду Канади (рис. 2.3)[37].

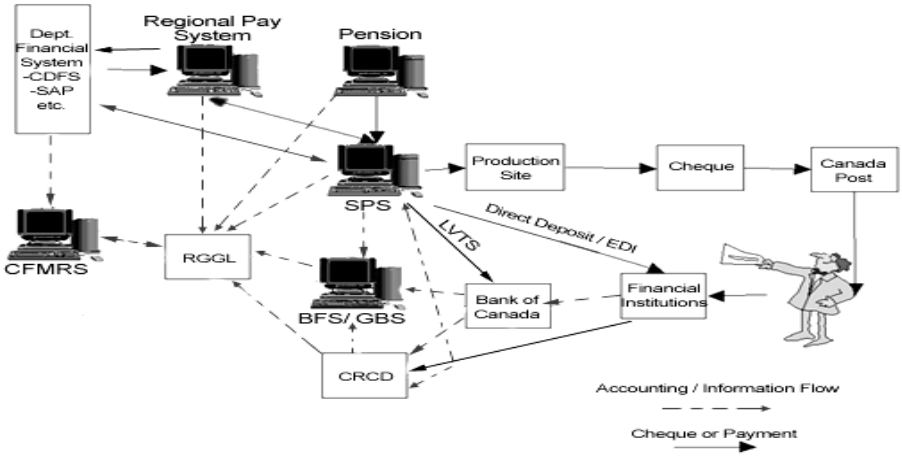

Рис. 2.3. Загальна схема Проекту стратегії фінансової інформації канадського уряду

Проект складається з відомчої фінансової системи (Common Departmental Financial System — CDFS), яка побудована на клієнт/серверній архітектурі, містить приблизно 4000 програм, що опрацьовують 240 таблиць і 2000 елементів даних, а також фінансову систему керування звітами (Common Financial Management Reporting System — CFMRS), що побудована також на клієнт/серверній архітектурі, складається з приблизно 1100 програм, 61 таблиця й 500 елементів даних.

[37] Джерело — Public Works and Government Services Canada.

Позиція американського уряду — іншої провідної держави у сфері комп'ютеризації сектора державного управління — краще всього пояснюється у висловлюванні колишнього віце-президента США Ела Гора, що постійно цитується. За Гором, уряд повинен не тільки використовувати інформаційні технології для своїх потреб, але й «взяти на себе функції лідера в освоєнні технологій, які змінять обличчя демократії в усьому світі й розширять можливості малого бізнесу на світових ринках».

Використання в своїй діяльності інформаційної системи і впровадження нових інформаційних технологій органи державного управління США почали одними з перших — ще з 60-х рр. XX століття.

У 1995 році в США були прийняті два ключових закони — про реформу управління інформаційними технологіями США (Information Technology Management Reform Act) та про скорочення обігу документів (Paperwork reduction Act of 1995), що визначили основні напрями подальшої інформатизації органів влади, а саме: підвищення ефективності інформаційно-технологічного забезпечення урядових структур через переорієнтацію «від процесу на результат», вдосконалення управлінських процесів і роботи в цілому за рахунок використання інформаційних технологій, зведення до мінімуму кількості документів, що складаються в урядових агенціях, забезпечення рівня послуг, що надаються федеральним урядом, на рівні найкращих взірців із приватного сектора, застосування міжвідомчого підходу до створення та використання інформаційних ресурсів, запровадження єдиного підходу до управління ними та забезпечення їхньої доступності для загального користування, захист прав й інтересів окремих громадян, підприємств та суспільства в цілому щодо доступу до інформації та ін.

Уряд США головною поставив абсолютно конкретну задачу — перевести в Інтернет як можна більше операцій щодо взаємодії з суспільством. Серед них такі, як отримання форм і бланків офіційних документів, оплата податків із відправкою податкових декларацій і проведенням оплати по кредитній картці через Інтернет, забезпечення трекінга (відстеження статусу) документів, які посилаються в державні структури, що дозволяє у будь-який момент дізнатися, в якому статусі знаходиться даний документ.

Підвищення оперативності роботи державних установ у США стосується не тільки уряду, а й розглядається як одна з важливих задач на рівні регіональних і місцевих органів управління.

Особливої уваги приділено організаційним питанням. Одна з головних осіб у системі виконавчої влади — директор Офісу управління та

бюджету США (Director of the Office of Management and Budger) — відповідає за оцінювання капіталовкладень в інформаційні технології для урядових органів. У кожному урядовому агентстві призначаються керівники з питань застосування інформаційних технологій (Cher Information Officer — CIO) з обов'язками керувати розробленням та створенням інформаційної інфраструктури відомства, консультувати керівництво щодо питань придбання технологічних засобів, управління інформаційними ресурсами.

Для координації та обміну досвідом, вирішення питань інтеграції створена Рада CIO, до якої входять представники різних агенцій.

Електронні ініціативи урядів європейських країн також офіційно оголосили про намір забезпечити цілодобове обслуговування громадян в режимі онлайн (Bund Online в Німеччині, концепція UK Online — Великобританія в Мережі та ін.). Більша частина проекту Європейського Союзу, відомого як «Обмін даними між Адміністраціями», має відношення до надання урядових послуг у режимі онлайн.

Шлюз державних служб (Government Gateway) Великобританії є системою-посередником для організації взаємодії різнорідних несумісних систем і являє собою ключову ланку, що забезпечує стандартний спосіб доступу до державних організацій за допомогою централізованої інфраструктури. Одним з її елементів є загальнодержавна база знань Whitehall — доступне у 24-часовому режимі єдине електронне джерело інформації про законодавство, факти, статистику. Вона призначена для надання вищому рівню уряду швидкого доступу для прийняття політичних рішень, забезпечення тісної міжвідомчої взаємодії, для оперативного управлінського реагування.

Австрійський уряд створив Єдиний Федеральний комп'ютерний центр, що підтримує Єдину державну інформаційну систему Finanz Online, яка забезпечує подачу електронних податкових декларацій з інтуїтивно зрозумілим доступом через Інтернет для фізичних і юридичних осіб. Ця система є доступною 24×7 у будь-якій точці країни.

Про велику увагу, що приділяється забезпеченню автоматизованими засобами взаємодії урядів із своїми громадянами, свідчить також той факт, що питаннями електронного урядування опікуються чимало міжнародних організацій, зокрема підрозділи ООН та Світового банку. Так, ООН створено важливу програму, названу Мережа державних адміністрацій (United Nations Public Administration Network — UNPAN), довготривалим завданням якої є побудова такої інфраструктури цих регіональних і національних установ, щоб вони змогли звертатись, об-

робляти і поширювати доречну інформацію за допомогою сучасних ІКТ для просування парадигми кращої адміністрації.

Зрозуміло, що наведений огляд висвітлює лише «вершину айсбергу», адже для забезпечення вказаних процесів потрібне створення в органах влади автоматизованих систем, що здатні не лише забезпечувати взаємодію з населенням, а й реалізувати підтримку всіх процесів, пов'язаних із документообігом, управлінням інформацією та її захистом, аналітикою та звітністю органу влади.

У зв'язку з цим, розглядаючи світовий досвід інформатизації державної влади в розвинутих країнах, можна виділити загальний підхід, який полягає перш за все в організації державного регулювання застосування ІТ у цій сфері[38].

Як правило, основний натиск робиться на описі міжсистемної взаємодії як найбільш важливого елемента державної інформатизації, необхідного для забезпечення міжвідомчої взаємодії й взаємодії із громадянами. У тім або іншому вигляді в більшості документів, які формують державне регулювання, визначається функціональна архітектура, що встановлює правила класифікації специфікацій і функцій, для виконання яких вони призначені. Каталог базових специфікацій, що є однією з основних частин майже всіх систем регулювання, призначений для визначення умов використання стандартів, а також їхнього життєвого циклу, що відповідає темпам розвитку інформаційних технологій.

Найбільш розвинену архітектуру серед документів регулювання має американський документ FEA (Federal Enterprise Architecture)[39], в якому наведено не тільки опис технологічних підходів, але й порядок проектування адміністративних процесів держави. Він містить набір довідкових моделей, присвячених різним аспектам проектування й функціонування інформаційних систем. Технічна довідкова модель містить певний набір вимог до використовуваних технологій.

Першим європейським документом, що встановлює загальні вимоги до державних інформаційних систем, став *e*-GIF (*e*-Government Interoperability Framework)[40], прийнятий в Англії. Він має найбільш вагомий статус, а відповідність йому систем, що створюються, забезпечується механізмами контролю й фінансового заохочення.

У Німеччині для проектів, розроблювальних у рамках урядової ініціативи BundOnline, опубліковано документ SAGA (Standards and

[38] http://www.info-foss.ru/quickstart/standart/interoperability_regulation
[39] http://www.whitehouse.gov/omb/egov/a-1-fea.html
[40] http://www.govtalk.gov.uk/schemasstandards/egif.asp

Architectures for *e*-government Applications)[41]. SAGA відрізняється широтою регулювання й монолітністю — цей цілісний багатосторінковий документ містить вимоги й рекомендації не тільки до інтерфейсів систем, але й до порядку їхнього проектування.

У Франції вводиться регулюючий документ нового покоління RGI14 (Référentiel Général d'Interopérabilité)[42]. Він буде мати обов'язковий статус для всіх органів державної влади, при цьому розробляється у відкритому порядку із залученням зацікавлених представників громадськості. У силу цього RGI може стати найбільш якісним документом у сфері регулювання інформаційних систем держави не тільки в Європі, але й у світі.

Датський документ The Interoperability Framework[43] відрізняє технологічна опрацьованість. Він найбільш послідовно дотримується принципу пріоритету відкритих стандартів, але, з іншого боку, він не має обов'язкового характеру і є лише довідковим керівництвом при розробці державних інформаційних систем.

Для забезпечення взаємодії й сумісності інформаційних систем на загальноєвропейському рівні Єврокомісією опубліковано документ EIF[44] (European Interoperability Framework) як «надбудову» над національними зведеннями приписів по системах.

Існують й інші національні проекти, що переслідують ті ж цілі. Серед них можна назвати The Hong Kong Special Administrative Region Interoperability Framework[45] спеціального адміністративного району Гон-Конг у Китаї, новозеландський New Zealand E-government Interoperability Framework[46], австралійський Australian Government Technical Interoperability Framework[47] й ін. В Україні ж, як і у більшості країн, що розвиваються, подібних документів, на жаль, ще немає.

Автоматизація інформаційно-аналітичної діяльності в органах влади України. Як вказувалося, в Україні різними директивними документами передбачена широка програма реформування державного управління, які також ставлять завдання забезпечити доступ до інформації про діяльність органів усіх гілок влади на всіх її щаблях.

---

[41] http://www.kbst.bund.de/saga

[42] ttps://www.ateliers.modernisation.gouv.fr/ministeres/domaines_d_expertise/architecture_fonctio/public/ rgi

[43] http://standarder.oio.dk/English

[44] http://europa.eu.int/idabc/en/document/3473/5585

[45] http://www.ogcio.gov.hk/eng/infra/eif.htm

[46] http://www.e.govt.nz/standards/e-gif

[47] http://www.agimo.gov.au/publications/2005/04/agtifv2

Хоча результати аналізу свідчать, що пошук, зведення й узагальнення в ОДВ усіх необхідних фактів проводиться переважно «вручну», «просіваючи» купи паперових документів, спираючись в основному на знання, досвід й інтуїцію співробітників, а інформаційна взаємодія органів влади у процесі виконання покладених на них завдань з іншими організаціями та підприємствами здійснюється переважно шляхом обміну паперовими документами, вже сьогодні рівень їхнього опрацювання — це у більшості випадків сфера застосування нових технологій.

При обстеженні інформаційної взаємодії органів влади України було виявлено низку недоліків існуючої системи збирання електронної інформації, до основних з яких відносяться такі:

1) значні витрати часу і недостатня якість даних при перенесенні з паперових носіїв, особливо на регіональному рівні;

2) багаторазове введення та дублювання даних у різних галузевих автоматизованих системах обробки інформації, що призводить, в окремих випадках, до суперечності зібраної інформації;

3) відсутність централізованої системи ведення та використання класифікаторів, довідників, регістрів і кадастрів, що не дає можливості спільного використання даних різних галузей, а також даних різних статистичних і аналітичних форм.

Як приклад слід зазначити, що одним з основних напрямків інформаційно-аналітичної діяльності органів державної влади є моніторинг соціально-економічного стану галузі або регіону України, який перш за все ведеться за затвердженими основними показниками. Але при обстеженні була виявлена неефективність розповсюдження статистичної та аналітичної інформації, що виникає внаслідок несвоєчасності її надходження до користувачів, надання її не в потрібній формі, недоступності інформації для сприйняття всіма користувачами.

Ці недоліки значною мірою впливають на стан захищеності інформації, не лише забезпечення її конфіденційності, а й доступності для легальних користувачів.

Проведений аналіз показує, що типовий склад інформаційної бази кожної ІАС, що використовується для підтримки функціонування органів влади, крім типових та загальних інформаційних об’єктів (вхідні і вихідні документи, кадрова інформація, інформація з бухгалтерського обліку), звичайно має свою специфічну внутрішню інформацію (про поточний стан об’єктів керування, про планування повсякденної діяльності), яка може не виходити за її межі, а також специфічну інформа-

цію, яка інтегрується та розповсюджується тільки вертикально до вищих органів влади.

До складу інформаційної бази ОДВ, крім власних інформаційних ресурсів, що ведуться засобами ІАС, як правило, входять і зовнішні бази даних, що містять необхідну інформацію для реалізації функцій ІАС та більш ефективного функціонування органу влади, але формуються і ведуться за їхніми межами. Зазвичай це інформація довідкового характеру (класифікатори типів підприємств, форм власності та організаційно-правових форм, адміністративно-територіального устрою України та ін.). До цих зовнішніх баз даних відносяться й інформаційні ресурси міжвідомчих ІАС (наприклад, реєстр суб'єктів підприємницької діяльності — юридичних і фізичних осіб).

Слід також зазначити, що ефективна робота інформаційної служби ОДВ залежить не стільки від технічного забезпечення й інтенсивності інформаційних потоків, що обробляються, скільки від чіткої постановки задач, безпосередньої взаємодії із споживачами інформаційно-аналітичних матеріалів, «настроювання» на їхні інформаційні потреби, на специфіку технології обговорення питань і прийняття рішень.

Але апріорно сформулювати вимоги до інформації, що потрібна в органі влади, досить складно. Їх частіше за все не усвідомлюють і самі користувачі, тому визначення специфічних інформаційних інтересів конкретного кола споживачів є однією з найскладніших задач інформаційної служби органу влади. Повноцінно вирішити цю проблему заважає, як правило, не лише відсутність часу на ґрунтовне попереднє вивчення інформаційних інтересів держслужбовців, але й в цілому недостатньо висока їхня інформаційна культура. Нарешті, треба ще вказати на різнорідність форм подання інформації, яка надходить, що створює певні перепони на шляху її інтегрованого опрацювання.

Що стосується сучасного рівня забезпеченості технічними і програмними засобами інформатизації органів влади, аналіз свідчить, що в цілому в Україні має місце позитивна динаміка збільшення кількості персональних комп'ютерів в органах влади, хоча існує й дуже велика розбіжність у ступені «комп'ютерізації» різних ОДВ.

Так, за даними дослідження «Електронне урядування в Україні: аналіз та рекомендації» 70–90 % робочих місць держслужбовців в органах влади усіх рівнів обладнано комп'ютерами. Темпи збільшення кількості службовців, які мають доступ до Інтернету, за останні роки суттєво зросли. Кількість службовців, які використовують для внутрішнього і зовнішнього документообігу локальні і корпоративні мережі,

електронну пошту, становить (у середньому) 70 %. Водночас комп'ютерної техніки не вистачає в районних органах виконавчої влади, в районних селищних і міських органах місцевого самоврядування, кількість робочих міст, підключених до Інтернету, є замалою за для того, щоб забезпечувати через Інтернет як зовнішній документообіг, так і послуги бізнесу та громадянам.

Серед операційних та офісних систем, що використовується, слід відмітити, що однозначну перевагу мають розробки компанії Microsoft. Серед засобів для ведення інформаційних ресурсів переважають СКБД MS Access, FoxPro, іноді Oracle, а також використовуються електронні таблиці MS Excel.

Автоматизована технологія діловодства і документообігу як головна складова інформаційно-аналітичної діяльності також має різні ступені впровадження. В органах влади використовуються вже до десятка різних систем автоматизації діловодства, серед них такі, як OPTIMA WorkFlow, «Lotus Notes», «ДокПроф», «Мегаполіс», «Діло» та ін.

Але при цьому слід зазначити, що легітимність програмного забезпечення, що використовується в ОДВ, є ще дуже низькою. Тільки окремі державні служби мають значення коефіцієнту легітимності більше 0,8. За існуючими даними загальна кількість комп'ютерних програм, що легально використовується, становить лише приблизно 28 % усіх інсталяцій.

Доступ до Інтернету мають практично всі органи влади. Майже усі мають й веб-сайти та використовують електронну пошту. У питанні ведення веб-сайтів важливу роль зіграв спільний наказ Державного комітету інформаційної політики, телебачення і радіомовлення України та Державного комітету зв'язку та інформатизації України, яким було затверджено Порядок інформаційного наповнення та технічного забезпечення Єдиного веб-порталу органів виконавчої влади та Порядок функціонування веб-сайтів органів виконавчої влади. Але в цілому присутність ОДВ в Інтернеті є ще дуже незначною (рис. 2.4). Крім того, багато органів районного (і нижче) рівня взагалі не мають своїх веб–сайтів.Восени 2008 р. студентами Національної академії управління було проведено аналіз веб-сайтів органів влади України за низкою показників, що є важливими для забезпечення присутності органів влади, зокрема, в системі електронного уряду. Узагальнені результати аналізу на вибірці з 20 органів влади (11 міністерств, 4 державних комітети, 4 органи зі спеціальним статусом, 1 орган судової влади) наведені у табл. 2.1.

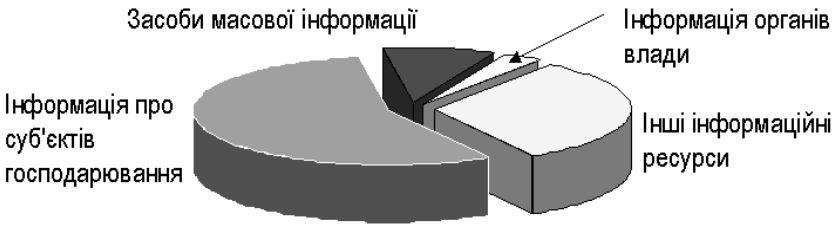

Рис. 2.4. Співвідношення інформаційної присутності органів влади в Інтернеті

Таблиця 2.1. Узагальнені результати аналізу веб-сайтів органів влади України

Показник		Результат аналізу
№	Назва	
1.	Структура сайта	стандартна — 12 (60 %), розвинута — 8 (40 %)
2.	Інформація про організацію і діяльність органу влади	стандартна — 9 (45 %), розвинута – 11 (55 %)
3.	Послуги для громадян	розширені — 2 (10 %), Інтернет-приймальня — 6 (30 %), довідкова інформація — 10 (50 %), немає — 2 (10 %)
4.	Наявність документів нормативної бази	стандартні — 8 (40 %), галузеві — 12 (60 %)
5.	Доступ до баз даних	є — 7 (35 %), немає — 13 (65 %)
6.	Застосування геоінформаційних ресурсів	немає — 20 (100 %)
7.	Мультимедійні функції	немає — 20 (100 %)
8.	Посилання на інші ресурси державних установ	стандартні — 7 (35 %), розширені — 8 (40 %), розвинуті — 5 (25 %)
9.	Наявність централізованої пошукової системи	стандартна — 12 (60 %), розвинута — 3 (15 %), немає — 5 (25 %)
10.	Загальний обсяг інформації	незначний — 3 (15 %), значний — 17 (85 %)
11.	Кількість відвідувачів	незначна — 2 (10 %), середня — 2 (10 %), значна —1 (5 %), лічильника немає — 15 (75 %)

При аналізі прийнято:

— у показнику 2 «Інформація про організацію і діяльність органу влади» стандартна — відомості про керівників та контактна інформація, розвинута — плюс інформація про плани діяльності, звітна інформація, фотогалерея та ін.;

— у показнику 4 «Наявність документів нормативної бази» стандартні — акти вищих органів влади, галузеві — плюс докладна збірка галузевих нормативних актів;

— у показнику 8 «Посилання на інші ресурси державних установ» стандартні — лінки на сайти Кабінету Міністрів, Секретаріату Президента, Верховної Ради, розширені — плюс посилання на деякі інші органи влади, розвинуті — плюс посилання на підприємства та установи галузі;

— у показнику 11 «Кількість відвідувачів» наведені дані про тих респондентів, що мають лічильник відвідувань.

Цей аналіз дав більш-менш очікувані результати. Хоча сайти органів влади вже інформаційно суттєво наповнені, адже створені вони були в основному ще у період 2001–2004 рр., просування їх у бік забезпечення надання онлайнових адміністративних послуг населенню дуже незначне. Більшість веб-сайтів знаходяться на першому, а деякі на другому етапі розвитку із чотирьох визначених в Європі, тобто на етапі розміщення інформації та односторонньої взаємодії. Заходи щодо забезпечення двосторонньої взаємодії, а тим більше здійснення трансакцій в електронному вигляді, в Україні майже не розпочались.

Тому ці сайти цікаві переважно представникам ЗМІ, а для візитів на них пересічних громадян немає соціальної потреби. Про це свідчить й незначна статистика відвідувань (може з-за цього й лічильники відсутні на більшості сайтів).

Тим не менш стан інформатизації органів влади України з урахуванням розвитку національного сегменту Інтернету обумовили базу для розгортання в останні роки робіт зі створення в країні інформаційної системи «Електронний уряд». Затверджено перелік послуг, що мають надаватись органами влади громадянам та підприємствам з використанням веб-сайтів. На більшості сайтів наведено каталоги цих послуг. Створено й Урядовий портал www.kmu.gov.ua як центральну частину системи електронного урядування.

Іноземні агенції ще 2004 року вважали рейтинг розвитку *e*-Government в Україні на середньому світовому рівні. Але з того часу, на жаль, цей показник не змінився у кращий бік, скоріше навпаки. Такі ж справи і з усією електронною інфраструктурою країни. У світовому

рейтингу країн з «електронної готовності» (який відсоток населення користується Інтернетом, скільки громадян використовують послуги електронного банкінгу, наскільки розвинена система здійснення податкових платежів через глобальну мережу й т.д.), складеному англійським журналом The Economist і корпорацією IBM за 2005 р., Україна зайняла 57-ме місце з 65 можливих[48].

Справа скоріше за все в тому, що в системі державної влади проблеми розвитку ІКТ і *е*-уряду поки що не сприймають в контексті трансформування і розвитку країни в цілому і їхнього впровадження й досі не визнане одним із пріоритетних напрямків розвитку України, а інформатизація зводиться до часткової задачі комп'ютеризації владних інституцій. Типовий кошторис державних установ «на інформатизацію» зазвичай виявляється таким: 70 % витрачається на закупівлю комп'ютерної техніки, 20 % — на створення локальних мереж, по 5 % іде на підключення до Інтернету й закупівлю програмного забезпечення. Тобто, як і раніше, держустанові значно простіше одержати гроші на закупівлю обладнання, ніж на створення інформаційних систем і баз даних, на навчання службовців користуванню цими ресурсами в повсякденній практиці.

Тобто й досі має місце технократичний підхід до вирішення проблем інформатизації влади, захоплення технічним боком справи. Щодо його ефективності досить згадати гасла й результати реалізації минулих програм «АСУ-нізації», «ПіСі-зації», «Інтернетизації» країни (і, в основному, на базі засобів іноземного виробництва).

Як висновок вже згаданого дослідження «Електронне урядування в Україні: аналіз та рекомендації» вказується: «Аналіз міжнародного

[48] Таке становище має місце й у багатьох країнах колишнього СРСР (за винятком, мабуть, Естонії). Так, на вже згадуваному засіданні Ради з питань розвитку інформаційного суспільства при Президенті Росії Дмитро Медведєв заявив: «За ключовими показниками ми ще страшно далекі від більшості розвинених держав». «За індексом розвитку електронного уряду ми були в 2005 р. на 56-му місці, а в 2007 р. досягли 92-го. Про що це говорить? Це говорить про те, що в нас ніякого електронного уряду немає, все це — химера. У рейтингу готовності країн до мережного світу ми теж на «почесному» 72-му місці». Перейшовши до подробиць, Медведєв відзначив, що весь документообіг в органах державної влади дотепер ведеться на папері, а «комп'ютери в основному використовуються як друкарські машинки». Відсутні сучасні системи планування й сучасні системи фінансово-управлінської звітності. Для громадян немає можливості відправити з особистого комп'ютера заяви або простежити за проходженням свого запиту в тому або іншому відомстві, одержати електронну довідку по системі електронного єдиного вікна. «Ми повинні були створити єдиний портал державних і муніципальних послуг, який повинен був запрацювати з 1 січня цього року. Цього теж не сталося».

досвіду, української практики впровадження технологій *е*-урядування, інтерв'ю показали, що однією з причин гальмування процесу розвитку *е*-урядування в Україні є недосконаліть координування усіх його складових (дослідницько-експертної, організаційної, технологічної, навчальної, консультативної і просвітницької), тобто відсутність такої установи (центру), яка б за дорученням уповноваженого органу влади, за участі науковців, експертів і фахівців-практиків забезпечувала науково-методичне супроводження розроблення концептуальних засад, національних програм і проектів, уніфікованих технологічних рішень, підвищення кваліфікації державних службовців і посадових осіб із впровадження технологій *е*-урядування».

При використанні послуг Інтернету практично всі ОДВ так чи інакше вирішують питання захисту своєї внутрішньої комп'ютерної мережі від зовнішнього втручання. Але зазвичай це стандартні способи такого захисту — з використанням можливостей proxy-сервера та міжмережних екранів (FireWall).

Як спеціалізовані системи, що автоматизують різні напрямки діяльності ОДВ, використовуються власні розробки чи зроблені на замовлення різними фірмами системи. Хоча найбільше поширення в ОДВ мають інформаційні системи з законодавства України, бухгалтерії та діловодства, одначе в агенціях державної влади незалежно одна від одної створюються та розвиваються чимало систем, які можна віднести до класу інформаційно-аналітичних — Мінекономіки і Мінфіну, Пенсійного фонду, Мінпраці, Державної податкової адміністрації, митних служб, Міноборони, МВС, Рахункової палати та ін.

Широко впроваджуються засоби автоматизації і в регіональних органах виконавчої влади, органах місцевого самоврядування, чому певною мірою сприяють й розроблені типові рішення для створення систем інформаційно-аналітичного забезпечення місцевих органів виконавчої влади [131–133]. Ці рішення передбачають створення регіональних інформаційно-аналітичних центрів, системи локальних і регіональних телекомунікаційних мереж, інтерфейсів місцевих держадміністрацій з територіальними органами міністерств й інших центральних органів виконавчої влади, створення, зокрема, автоматизованого класифікатора адміністративно-територіального устрою України на основі картографічних даних, алгоритмічного забезпечення підтримки прийняття рішень з питань управління адміністративно-територіальною одиницею, систем електронного документообігу та захисту інформації.

Одначе поки що кожне відомство займається розробкою власних ІАС, в основному виходячи з проблем, пов'язаних із головним «виробничим процесом», за який відповідає той чи інший ОДВ, як, наприклад, Державна податкова адміністрація чи Пенсійний фонд. Різні ОДВ мають різні ступені впровадження засобів інформатизації та інформаційно-аналітичних систем. Так, цілком природно, що найбільш розвинута комп'ютерна локальна мережа впроваджена у Секретаріаті Кабінету Міністрів та у Верховній Раді України.

Але в цілому слід зазначити, що систем, які, по-перше, готові працювати в системі електронного уряду, а, по-друге, комплексно автоматизують інформаційно-аналітичну діяльність держслужбовців в органах влади, майже немає, а існуючі мають переважно локальний характер, використовуються окремими підрозділами, не інтегровані у єдину відомчу ІАС. Ті елементи й окремі технології *е*-уряду, які впроваджуються окремими структурами, носять вибірковий неуніфікований в архітектурному плані характер, що викликає проблеми щодо сумісності цих елементів між собою.

Тобто існуючі приклади успішного створення та застосування в органах влади ІАС ще розрізнені, не складають взаємопов'язаного єдиного комплексу, характеризуються різноманітністю у підходах, темпах розвитку й оснащенні, а тому й недостатні для задоволення нового рівня вимог.

Локальність автоматизованих систем обумовлює й наявність в органах влади лише локальних електронних інформаційних ресурсів, що не зведені до єдиного державного сховища даних.

Як ілюстрацію деяких рішень, що були реалізовані, розглянемо зараз та на подальших сторінках декілька автоматизованих систем, які створювалися в органах влади в різні роки.

Однією з перших таких систем слід назвати ***Урядову інформаційно-аналітичну систему з питань надзвичайних ситуацій (УІАС НС)***, що почала створюватись Міністерством з питань надзвичайних ситуацій та в справах захисту населення від наслідків Чорнобильської катастрофи ще в 90-х роках минулого століття [134]. Потреба в такій системі обґрунтована необхідністю успішного запобігання виникненню надзвичайних ситуацій (НС) і ліквідації їхніх наслідків, адже Україна є одним з найбільш критичних регіонів Європи з техногенного навантаження та потенційної небезпеки шкідливих виробництв для населення і природного середовища, що створює об'єктивні передумови зростання кількості різних НС.

Метою створення УІАС НС визначено оперативне забезпечення Адміністрації Президента України, Верховної Ради України, Кабінету Міністрів України, Ради національної безпеки і оборони України, центральних органів виконавчої влади експертно-аналітичною, прогнозною, довідково-статистичною, фактографічною, контрольно-звітною та управлінською інформацією з використанням сучасних інформаційних технологій для вирішення задач, пов'язаних з техногенно-екологічною безпекою та НС.

Основні функції системи полягають в інформуванні, аналізі та прогнозуванні, плануванні заходів і у підготовці рішень, контролі за їхнім виконанням, а також у забезпеченні цих процесів. У системі вирішується низка таких задач, як автоматизація процесів отримання достовірної інформації щодо НС та доступу до неї фахівців та аналітиків підрозділів міністерства, систематизація даних про НС, експертна оцінка характеру НС і необхідних ресурсів для усунення їхніх наслідків, аналіз, прогноз і моделювання НС і вплив найбільш небезпечних НС на стан потенційно-небезпечних об'єктів, контроль за ходом ліквідації наслідків НС та за ходом виконання рішень керівництва щодо вирішення задач, пов'язаних із НС, тощо.

Організаційно-функціональна структура УІАС НС складається з таких підсистем, як центральна, функціональних та територіальних підсистем, віддалених інформаційних вузлів, пересувних комплексів зв'язку та управління, мережі передачі інформації.

Центральна підсистема складається із центрального та резервного вузлів інформаційно-аналітичної обробки інформації, а також забезпечуючої підсистеми.

Функціональні підсистеми створюються в центральних органах виконавчої влади, а територіальні — в облдержадміністраціях, Раді Міністрів АРК, у держадміністраціях міст Києва та Севастополя. Таким чином, структурно-функціональна схема УІАС НС утворюється із чотирьох рівнів: урядового, відомчого, територіального та об'єктового.

Центральним вузлом виконуються основні функції інформаційно-аналітичної обробки інформації (рис. 2.5).

До них відносяться такі, як реєстрація та первинна обробка інформації про загрозу та наявність НС, що надходить до вузла згідно з регламентом, термінове інформування керівництва вищих органів влади, облдержадміністрацій та органів виконавчої влади про загрозу та виникнення НС, моделювання процесів розвитку НС і проведення експертних оцінок їхніх наслідків, забезпечення процесу підготовки управлін-

ських рішень щодо попередження та ліквідації наслідків НС, аналіз наслідків НС для господарських об'єктів та оцінки їхнього впливу на бюджет держави, контроль цільового спрямування коштів державного бюджету на ліквідацію наслідків НС, контроль виконання рішень та заходів щодо запобігання та ліквідації НС, обмін інформацією з компетентними органами інших держав щодо НС, загроз їхнього виникнення та ліквідації.

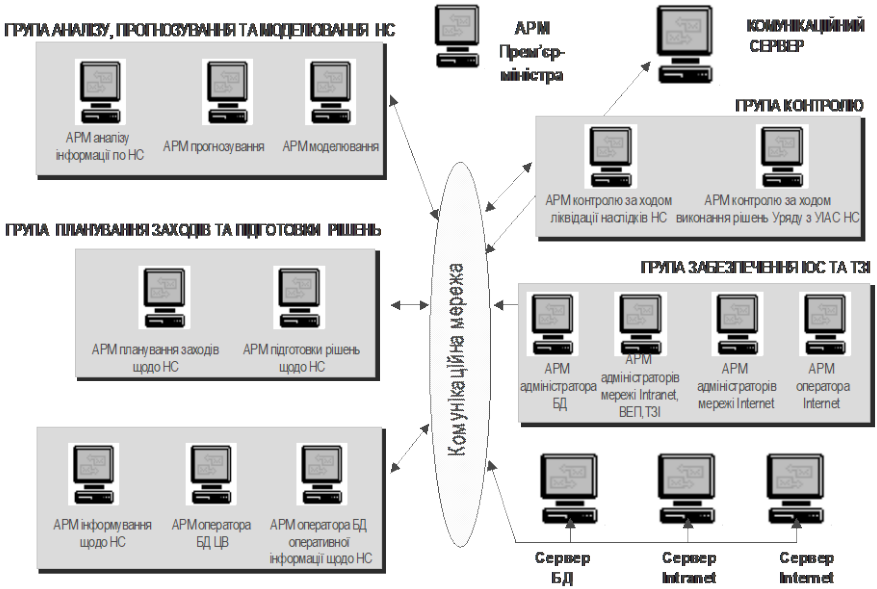

Рис. 2.5. Структурно-функціональна схема центрального вузла УІАС НС

Характерною рисою УІАС НС є використання принципів інформаційної взаємодії структурних елементів, інтеграції функціональних, інформаційних і програмно-технічних засобів окремих функціонально-структурних елементів (ФСЕ) [135, 136].

Принцип інформаційної підтримки процесів прийняття рішень щодо НС полягає у виконані таких вимог:

а) БД кожного ФСЕ повинна відображати рішення і директиви, прийняті (вироблені) відповідним йому рівнем управління;

б) результати відпрацювання рішень і директив відповідного рівня управління фіксуються у БД як відомості, що одержані та/або реалізовані внаслідок виконання відповідних управлінських рішень і вони є

вхідними (вихідними) даними для відпрацювання відповідним ФСЕ УІАС НС;

в) оцінка результатів виконання рішень і директив здійснюється з урахуванням відомостей, що накопичені в БД відповідного ФСЕ, як результат виконання відповідної інформаційно-статистичної задачі або моделювання.

Принцип функціонально-аналітичного забезпечення базується на сучасних математичних, програмних і картографічних засобах побудови забезпечуючих підсистем підтримки прийняття рішень, прогнозування НС і геоінформування.

Принципи єдиного програмно-технічного забезпечення базуються на застосуванні сучасних типових проектних рішень, що забезпечують максимально можливу сумісність програмно-технічних засобів ФСЕ УІАС НС.

Ефект від впровадження УІАС НС перш за все полягає у підвищенні рівня ефективності та оперативності державного управління у сфері техногенно-екологічної безпеки та надзвичайних ситуацій, що є найважливішою сферою забезпечення національної безпеки. Особливо ефективним є забезпечення прогнозної діяльності щодо НС шляхом застосування методів соціально-економічної статистики, економетрії і математичного моделювання, суттєве підвищення оперативності та надійності ліквідації наслідків НС.

Майже водночас з УІАС НС Міністерством внутрішніх справ почала створюватись ***Єдина державна автоматизована паспортна система (ЄДАПС)***, мета якої — забезпечення централізованого автоматизованого виготовлення документів, що засвідчують особу та підтверджують громадянство України (далі — паспортні документи), а також створюють умови для виготовлення інших персоніфікованих документів громадян, в яких застосовуються міжнародні стандартні формати біометричних і відцифрованих «фотографічних» даних для ідентифікації власника паспорта, що відповідає вимогам Європейського Союзу щодо виготовлення паспортних документів [137].

Як інформаційно-аналітична система ЄДАПС передусім забезпечує моніторинговою підтримкою управління у сфері правових і соціальних питань, контролю і прогнозування заселеності територій, відстеження динаміки міграційних і еволюційних процесів тощо. Тому до основних завдань ЄДАПС також відноситься формування баз даних спеціального призначення, що дає змогу організувати інформаційне обслуговування різноманітних запитів користувачів ЄДАПС, які вима-

гають аналізу і узагальнення. Крім того система забезпечує інформаційне обслуговування запитів користувачів, автоматизацію проведення масових заходів: вибори, референдуми тощо.

Цьому сприяє наявність інтегрованої бази даних, в якій концентруються всі інформаційні ресурси. З використанням зазначеної бази даних проектуються функціональні модулі на індивідуальне замовлення користувача чи для розв'язання конкретного завдання, реалізуються довільні запити в будь-якому часовому розрізі чи за окремими категоріями даних (соціальні групи, території, вікові групи тощо).

Структурний принцип побудови ЄДАПС передбачає модульну організацію й поетапне нарощування функціональних можливостей. Це дає змогу сконцентрувати технічні і фінансові ресурси на розв'язанні конкретного завдання паспортизації й одночасно започаткувати проектування та створення інших загальнодержавних інформаційно-аналітичних систем.

ЄДАПС являє собою трирівневу систему, що функціонує в режимі реального часу, основою якої є цільовий банк даних, де зберігається вся ідентифікаційна та облікова інформація про громадян. Цільовий банк даних створюється на центральному рівні і передбачає ведення резервного банку даних, який з міркувань безпеки повинен бути територіально віддаленим від центрального вузла (рис. 2.6).

Завданням центрального рівня є ведення інтегрованої бази даних та управління всіма вузлами системи. У разі надходження запитів від суб'єктів нижчих рівнів стосовно окремої особи на центральному рівні провадитиметься верифікація отриманої інформації. За позитивних результатів перевірки відбуватиметься запис (або модифікація) у базу даних центрального рівня. Інформація ж про цей факт автоматично передається на відповідні регіональний і місцевий рівні.

Реалізація основних завдань центрального рівня покладається на головний центр паспортизації, який на першому етапі створення ЄДАПС виконує функції головного обчислювального центру, зокрема, збирання і накопичення інформації.

Регіональний рівень забезпечує підтримування бази даних з обліковою інформацією про громадян, які проживають у відповідному регіоні. Ці дані надходять з місцевого рівня, передаються до бази даних центрального рівня і після їхньої всебічної перевірки накопичуються в базі даних центрального, регіонального та місцевого рівнів.

Місцевий рівень є основним для введення і первинної обробки інформації. Особисті дані громадян заносяться до бази даних цього рівня

для обробки й виготовлення паспортів. Після одержання підтвердження дані автоматично фіксуються в базі даних усіх рівнів і можуть бути доступними для використання в інших системах.

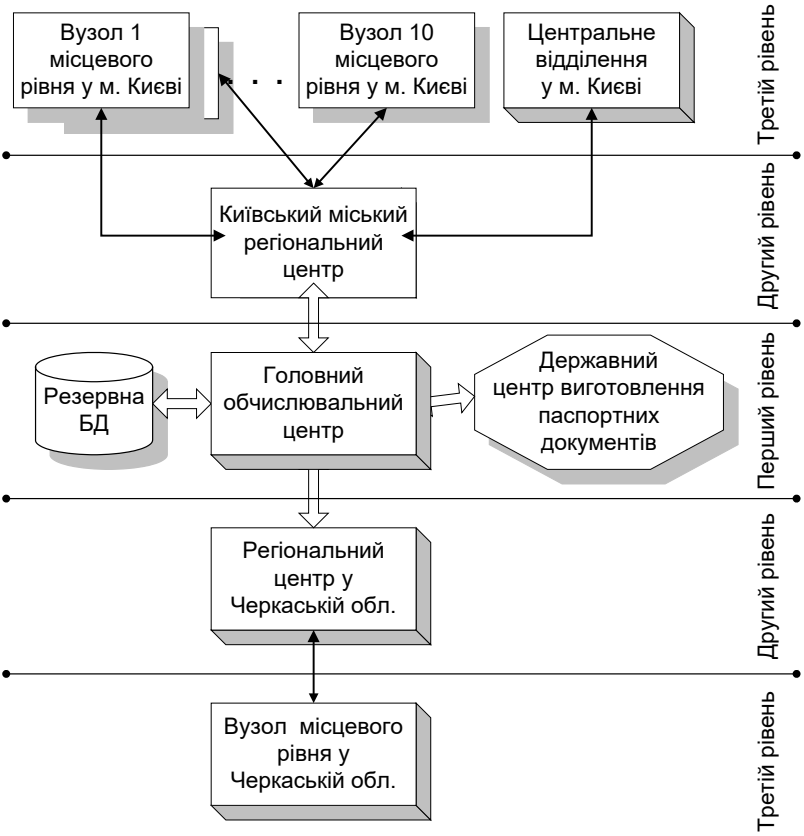

Рис. 2.6. Схема першого етапу реалізації ЄДАПС

Згідно з організаційними та економічними умовами створення системи, а також враховуючи необхідність гарантування безпеки циркулюючої інформації, ЄДАПС будується відповідно до таких вимог, як забезпечення повного циклу збирання, обробки, відображення, реєстрації, зберігання та розподілу інформації, використання обладнання з високою надійністю, реалізація принципу розподілених обчислень для підвищення надійності і життєздатності системи в цілому, оперативність забезпечення користувачів необхідною інформацією, надання її в

зручному для сприйняття вигляді, подання допомоги в аналізі та виробленні можливих варіантів рішень із використанням «людино-машинних» інтерфейсів і процедур прийняття рішень.

Ефект від впровадження ЄДАПС, крім підвищення рівня ефективності державного управління в сфері ведення облікової інформації про особу, полягає у забезпеченні формування за рахунок ведення довідкових картотек і баз даних спеціального призначення аналітичних і статистичних звітів і довідок, ведення моніторингу основних показників міграційної служби, синхронізації організаційно-інформаційних процесів у структурах МВС. Крім того, система може забезпечувати інформаційне обслуговування та автоматизацію проведення таких масових заходів, як вибори, референдуми тощо.

Також однією з перших систем в державній владі стала ***Автоматизована система експортного контролю України (АСЕК)***, метою створення якої є автоматизація повсякденної діяльності Державної служби експортного контролю України (ДСЕК) при розв'язанні завдань, пов'язаних з обробкою заяв суб'єктів ринку експорту та імпорту товарів військового призначення та подвійного використання, а також документообігу, накопичення, перегляду, коригування та відбору даних за заявами та документами [138].

ДСЕК проводить у встановленому порядку експертизу в галузі державного експортного контролю, видає суб'єктам здійснення міжнародних передач товарів відповідні дозволи (висновки), а також вирішує питання щодо скасування, тимчасового припинення, продовження дії цих дозволів (висновків). Відповідно до законодавства ДСЕК видає міжнародні імпортні сертифікати та інші документи, які містять державні гарантії щодо використання товарів у заявлених цілях, вирішує питання про відкликання таких гарантій, а також здійснює державну атестацію систем внутрішньофірмового експортного контролю, створених суб'єктами здійснення міжнародних передач товарів, і видає свідоцтва про таку атестацію. ДСЕК проводить реєстрацію суб'єктів здійснення міжнародних передач товарів, що підлягають державному експортному контролю, веде облік юридичних осіб, громадян України та їхніх іноземних партнерів, які під час здійснення міжнародних передач товарів, що підлягають державному експортному контролю, порушили законодавство України, міжнародні договори України.

Сукупність структурних підрозділів ДСЕК, для автоматизації діяльності яких призначається АСЕК, має певні функціональні особливості, що визначаються їхнім статусом і задачами. Ці особливості визна-

чають архітектурні рішення системи. АСЕК забезпечує автоматизацію підготовки визначених формалізованих документів у складі задач, орієнтованих на виконання певних людино-машинних операцій над даними, у вигляді комплексів програм (КП), що створюють певні підсистеми та реалізованих АРМами за відповідною схемою взаємодії (рис 2.7), а саме:

1) автоматизованої підтримки експертизи (АРМ «Експерт»);

2) реєстрації вихідних документів;

3) контролю проходження і відпрацювання вхідних документів;

4) складання опису документів у справі;

5) контролю виконання доручень і наказів в АСЕК;

6) вводу та аналізу інформації звітів з реалізації, що надходять від Державного комітету статистики України та Митної служби України до ДСЕК;

7) пошуку та відображення інформації бази даних АСЕК;

8) ведення реєстру суб'єктів здійснення міжнародних передач товарів;

9) ведення реєстру юридичних осіб, що мають повноваження для проведення недержавної експертизи;

10) аналітичної звітності за інформацією бази даних АСЕК;

11) перевірки цілісності бази даних АСЕК;

12) контролю проведення розслідувань;

13) ведення бази даних з питань експортного контролю країн світу;

14) обліку даних про відмови;

15) керування веб-сайтом ДСЕК.

Впровадження АСЕК дозволило, з одного боку, значно розширити доступність експертам національних і міжнародних інформаційних ресурсів у галузі озброєнь, військової техніки, продукції та матеріалів, що можуть бути використані при створенні зброї масового знищення та засобів їхньої доставки, а з іншого — забезпечити оперативний обмін інформацією з відповідними міжнародними організаціями.

Враховуючи необхідність здійснення численних завдань державного управління та проведення державної політики в галузі зв'язку, виконання функцій Адміністрації зв'язку України Державним комітетом зв'язку та інформатизації України (Держкомзв'язку[49], ДКЗІ) започатковано створення відповідної ІАС.

[49] Таку назву і статус мав на період обстеження і початку створення відповідної ІАС. У подальшому реорганізовано спочатку у Державний департамент з питань зв'язку та інформатизації, а потім у Державну адміністрацію зв'язку Міністерства транспорту і зв'язку України.

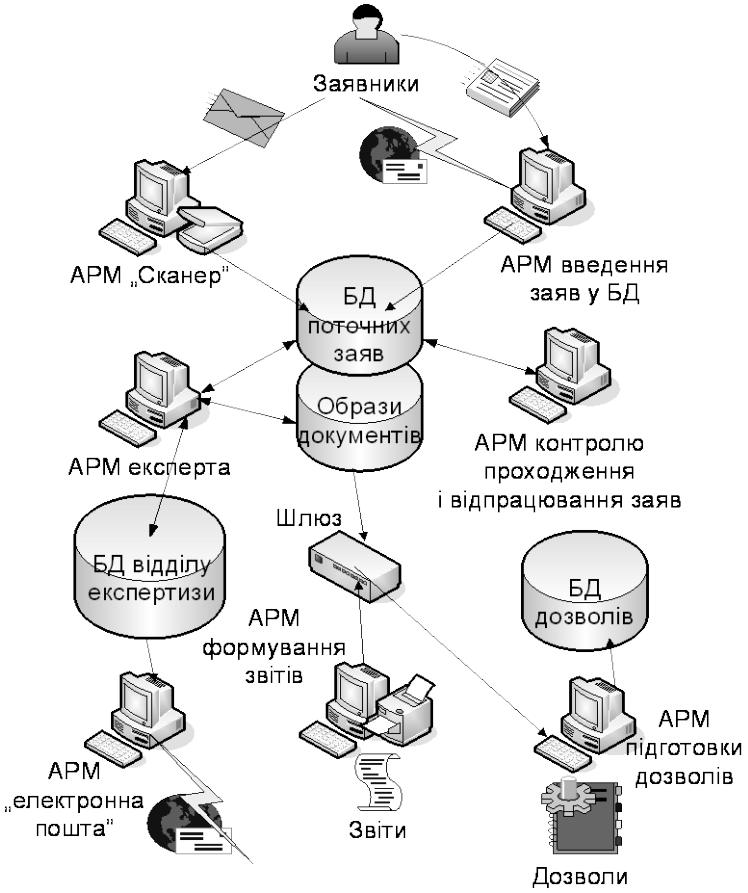

Рис. 2.7. Схема взаємодії АРМів АСЕК

Головною метою створення ***ІАС Держкомзв'язку*** є забезпечення оптимальних умов для задоволення інформаційних потреб і реалізації посадових обов'язків працівників Держкомзв'язку в напрямку оперативності, достовірності, доступності та конфіденційності інформації, а також підвищення ефективності та досягнення якісно нового рівня прийняття рішень на основі формування і використання єдиного інформаційного середовища, застосування сучасних засобів автоматизованого управління та електронного документообігу [139].

Таким чином, ІАС ДКЗІ призначена для автоматизації оперативного забезпечення працівників достовірною інформацією та матеріалами,

які містять довідкову, аналітичну, прогнозну, рекомендаційну та іншу інформацію, що надходить із відповідних підрозділів Держкомзв'язку, підпорядкованих підприємств та організацій; формування звітів; проведення аналізу та прогнозування за різними розрізами та аспектами звітів.

Структурно ІАС ДКЗІ складається із підсистем [140]:

1) інформаційної мережі;

2) електронного документообігу та контролю доручень;

3) ведення галузевого веб-порталу;

4) ведення сховища інформаційних ресурсів;

5) захисту інформації.

Метою створення інформаційної мережі (ІМ) системи є надання будь-якому користувачеві, у відповідності із захищеною технологією обробки інформації, потенційної можливості доступу до інформаційних ресурсів усіх комп'ютерів, що об'єднані в мережу.

Слід зазначити, що основні рішення щодо створення та ведення галузевого веб-порталу були одними з найперших в органах влади, а загальний дизайн головної сторінки веб-порталу було розроблено з урахуванням уніфікованих вимог до веб-сайтів органів влади, що знайшло застосування й в інших розробках.

Вимоги інтеграції та забезпечення аналітичної обробки у ДКЗІ значної кількості інформаційних ресурсів викликали необхідність створення та впровадження підсистеми ведення сховищ інформаційних ресурсів. За результатами проектування першої черги системи до сховища інформаційних ресурсів входять бази даних «Облік операторів та абонентів галузі», «Документообіг», «Нагороди працівників галузі».

У системі також запропоновані основні рішення щодо підсистеми захисту інформації. Захист інформації в ІАС ДКЗІ — це комплекс заходів, спрямованих на забезпечення підтримки цілісності, доступності та конфіденційності інформації і ресурсів, що використовується для введення, зберігання, обробки і передачі даних.

Ефект від впровадження ІАС ДКЗІ полягає, крім іншого, у забезпеченні суттєвого підвищення якості аналітичної обробки інформації, призначеної для розробки і дослідження моделей життєдіяльності галузі шляхом застосування різних методів (факторний, кореляційний і регресійний аналіз, дослідження тимчасових рядів, лінійне програмування, сіткове планування і керування й ін.) та формування на їх основі аналітичних і статистичних звітів і довідок, ведення моніторингу основних показників діяльності галузі, забезпечення контролю своєчасності опрацювання документів та їхньої цілісності, захисту інформації.

Однією з «наймолодших» є *Інформаційно-аналітична система Національної комісії з питань регулювання зв'язку України (ІАС НКРЗ)*, проектування якої проведено для вирішення проблем державного регулювання у сферах телекомунікацій та надання послуг поштового зв'язку згідно з Законами України «Про телекомунікації» та «Про радіочастотний ресурс України».

В умовах стрімкого розвитку телекомунікаційних технологій і ринку телекомунікацій, швидких змін у структурі попиту та пропозиції на ринку, що вимагає від постачальників телекомунікаційних послуг застосування різноманітних ринкових стратегій, виконання НКРЗ та його підпорядкованими установами покладених завдань неможливе без забезпечення вичерпної інформаційної підтримки та автоматизації процесів, пов'язаних із об'єктивною оцінкою ситуації на ринках і прийняттям відповідних рішень [141].

ІАС НКРЗ являє собою сукупність технічних, технологічних, програмних засобів, інформаційних баз даних, економіко-математичних методів і моделей, організаційних і методологічних заходів [142].

Мета створення ІАС НКРЗ досягається, зокрема, за рахунок створення централізованих засобів уведення, накопичення та інтегрування інформації, отриманої з різних джерел і в різних форматах, створення і ведення централізованого інтегрованого сховища даних і розподіленої системи їх використання, що підтримує багатокористувачевий та віддалений доступ, зокрема, з використанням веб-технологій, а також створення розподіленої системи технологічного електронного документообігу з використанням електронного цифрового підпису, яка охоплює усі організації НКРЗ. Велика увага приділяється створенню спеціального аналітичного програмного забезпечення, що забезпечує аналіз інформації, аналітичне її опрацювання, моделювання й прогнозування ринку послуг зв'язку тощо.

Архітектура ІАС спрямована на забезпечення одночасного розподіленого захищеного доступу співробітників НКРЗ та інших організацій і підприємств у відповідності з наданими правами доступу до актуальної структурованої інформації щодо основних інформаційних сутностей, а також можливість спільного контрольованого захищеного опрацювання вхідних і створення вихідних документів НКРЗ (рис. 2.8). Основу архітектури ІАС становить інфраструктура зв'язку між робочими місцями та множина прикладних програм і БД, що працюють у ній. З точки зору розподіленості архітектура системи є трирівневою (рис. 2.9).

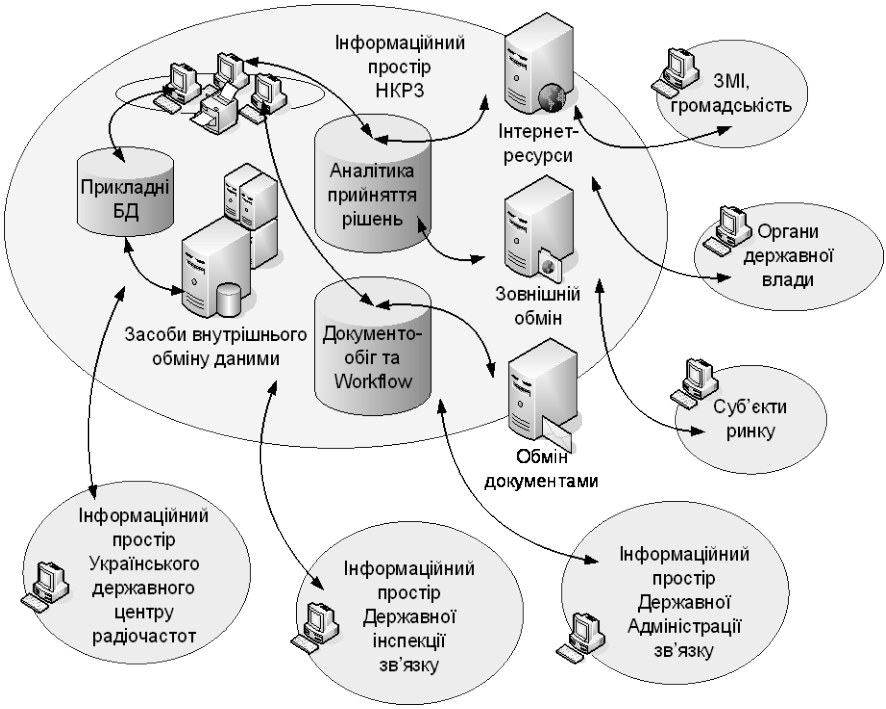

Рис. 2.8. Загальна архітектурна схема ІАС НКРЗ

Важливе місце в системі займає підсистема аналітичного супроводження підготовки і прийняття рішень (СППР), призначена для обробки та підготовки інтегрованої аналітичної інформації для осіб, що приймають стратегічні рішення відносно сфери регулювань у галузі зв'язку за умов штатних, позаштатних і критичних ситуацій, із-за суттєвих невизначеностей, наявності множини суперечливих цілей та багатофакторних ризиків на основі даних, отриманих від групи визначених інформаційних джерел. В основу розробки вказаної системи покладена системна методологія передбачення та методологія сценарного аналізу. СППР є людино-машинним комплексом, інтегрованим із іншими автоматизованими інформаційними підсистемами ІАС.

Ефект від впровадження ІАС НКРЗ враховується при забезпеченні такого показника, як створення інформаційного базису для побудови прикладних задач, що дозволять ефективно та своєчасно аналізувати ситуацію, приймати рішення та оперативно реагувати на події, пов'яза-

ні із наданням послуг у галузі телекомунікацій для забезпечення ефективної та оперативної регуляторної політики держави.

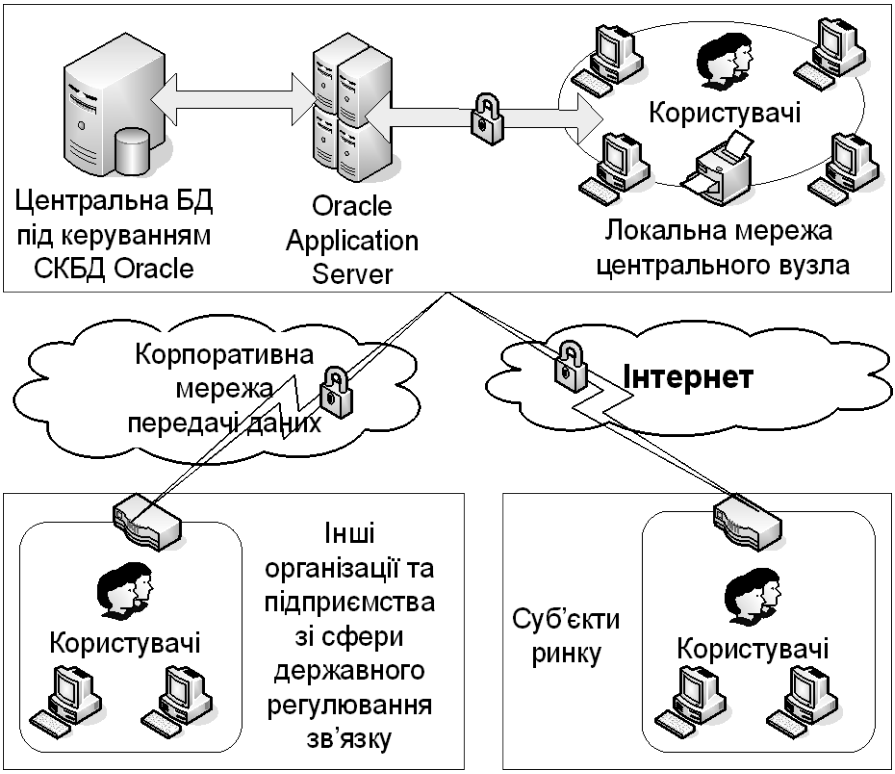

Рис. 2.9. Схема трирівневої архітектури ІАС НКРЗ

Підсумовуючи викладені факти, слід звернути увагу на те, що з наведених прикладів систем лише дві — ІАС Держкомзв'язку та ІАС НКРЗ — можна віднести до класу систем, що саме автоматизують інформаційно-аналітичну діяльність в апараті органу влади з метою підтримки прийняття рішень. До них можна віднести й УІАС НС, але вона є «класичною» міжвідомчою системою. Що стосується ЄДАПС і АСЕК, то ці системи хоча й мають інформаційно-аналітичні задачі, зорієнтовані переважно на підтримку «виробничих» процесів з підготовки дозвільних документів. Подібні реалізації, до речі, є найбільш розвинутими в системі державної влади.

2.3. Необхідні передумови побудови АІАС

Аналіз причин сучасного стану ефективності автоматизації інформаційно-аналітичної роботи в органах влади. Таким чином, слід зазначити, що незважаючи на окремі приклади успішної реалізації автоматизованих систем, технологізація процесів управлінської діяльності та загальний рівень автоматизації інформаційно-аналітичної діяльності органів державної влади в Україні в даний час ще відстають від сучасних потреб державного управління і сучасного рівня розвитку інформаційних технологій.

На це є низка об'єктивних причин, які неминуче обмежують ефективність інформаційно-аналітичної роботи в ОДВ. До них слід віднести й відсутність розвиненої аналітичної бази, й систематизованого і вичерпного інформаційного фонду з довідковим апаратом, обмежене використання сучасних фактографічних, геоінформаційних і текстових пошукових систем. Відсутній й електронний документообіг із застосуванням електронного цифрового підпису.

Підсумовуючи викладене, оцінку існуючих ІАС в органах влади можна звести до переліку показників, наведених у табл. 2.2.

Окремо слід зупинитися на питаннях щодо зміцнення стану інформаційної безпеки в органах влади України, в державних організаціях і на підприємствах (останній пункт табл. 2.2).

Слід зазначити, що за останні роки на державному рівні реалізовані деякі практичні заходи та розпочате формування нормативно-правового забезпечення інформаційної безпеки. Успішному вирішенню питань інформаційної безпеки органів влади сприяє створення Державної системи захисту інформації в Україні від іноземних технічних розвідок і від її витоку по технічних каналах, а також системи ліцензування діяльності підприємств у сфері захисту інформації і сертифікації засобів захисту інформації.

Разом з тим аналіз стану інформаційної безпеки органів влади свідчить, що в цей час її рівень не відповідає життєво важливим потребам держави, суспільства і особистості сьогоднішнім умовам розширення вільного обміну інформацією і необхідності збереження певних обмежень на її поширення з боку держави. Відсутність дійових механізмів регулювання інформаційних відносин у системі державної влади призводить до багатьох негативних наслідків.

Таблиця 2.2. Стан інформатизації органів державної влади

Показник		Характеристика
1.	Стан ІАС	Загалом незадовільний. Здебільшого ІАС розпадаються на окремі підсистеми, що слабо інтегровані навіть на єдиній інформаційній базі. Майже відсутній досвід створення «корпоративних» систем органів влади.
2.	Розробка ІАС	Частина розробок ІАС проводиться власними силами ОДВ. Для підтримки решти функцій переважно використовуються комерційні «коробочні» програмні продукти (оболонки, що адаптуються до потреб ІАС).
3.	Терміни створення або модернізації ІАС	Кожен з ОДВ або вже застосовує відомчу ІАС, або проводить її розробку чи дослідне впровадження. Але більшість ІАС потребує суттєвої модернізації та функціонального розвитку. При цьому ці заходи здійснюються вкрай повільно.
4.	Підрозділи ОДВ і підприємства галузі, що підключені до ІАС	Спостерігається намагання підтримати діяльність насамперед вищої ланки керівників, зокрема забезпечити бухгалтерський облік та управління кадрами, що автоматизовані майже у всіх ОДВ.
5.	Інформаційні ресурси	Переважають тематичні або періодичні звіти за певними показниками діяльності, довідки та документи оперативного інформування, підтримка листування. Аналітичні документи здебільшого готуються вручну. Відчувається гостра потреба в довідкових і картографічних БД, класифікаторах, словниках і довідниках за широким спектром показників.
6.	Формати даних	Форми обміну даними у переважної більшості ІАС специфіковані за механізмом експорту даних з інформаційних баз (SQL-інтерфейс).
7.	Протоколи доступу	Переважно використовуються система Інтернет-протоколів TCP/IP
8.	Доступність систем для спільного використання органами влади	Більшість ІАС є локальними і не пристосовані для спільного використання різними ОДВ.
9.	Інформаційна безпека	У повному обсягу проблеми інформаційної безпеки кожної ІАС і зінтегрованих комплексів вирішуються не завжди.

Слабке забезпечення органів державної влади і управління достовірною, своєчасною і повною інформацією, відомчий монополізм на інформацію, нерозвиненість інформаційних відносин у державній сфері утруднюють прийняття обґрунтованих рішень. Відсутність механізму внесення державних інформаційних ресурсів в господарський оборот призводить до втрат надходжень до державного бюджету.

Недостатня захищеність державних інформаційних ресурсів призводить до втрати важливої політичної, економічної і науково-технічної інформації. Втратам такої інформації сприяють безсистемність у забезпеченні захисту даних, слабка координація в загальнодержавному масштабі заходів щодо захисту інформації, відомча роз'єднаність у забезпеченні конфіденційності інформації. Незадовільно організовано захист персональних даних, податкової, митної, майнової інформації. Відставання вітчизняних інформаційних технологій вимушує прямувати шляхом закупівель незахищеної імпортної техніки та програмних засобів, внаслідок чого підвищується ймовірність несанкціонованого доступу до баз і банків даних, а також зростає залежність від іноземних виробників комп'ютерної і телекомунікаційної техніки й інформаційної продукції.

Отже, можна навести чинники, які впливають на створення ІАС органів влади в Україні та створюють труднощі, що існують на цьому шляху, а саме:

а) відкритість цих систем, вимоги динамічних змін складу, підпорядкованості та цілеспрямованості функціонування структур державного управління;

б) неможливість повного розмежування сфер відповідальності органів державної влади, що означає часткове перекриття цих сфер і певне дублювання роботи;

в) неточність і неповнота інформації, з якою працюють органи державної влади, породжувані як недостатністю ресурсів для її одержання, так і недостатністю взаємодії органів між собою;

г) обмеження реального часу, в яких повинні бути прийняті управлінські рішення незалежно від складності вирішуваних питань і обсягів оброблюваної інформації;

д) нерівномірність розвитку різних сфер управління та неоднакова ступінь підготовленості органів управління до втілення засобів автоматизації управління;

е) фактор постійної недостатності нормативно-правової бази, породжуваний об'єктивним відставанням засобів правового регулювання

від розвитку технологій;

є) багатокритеріальність при прийнятті управлінських рішень на всіх рівнях державної влади;

ж) інерційність управлінських механізмів у методологічному, кадровому і технологічному відношеннях.

Але, крім наведеного переліку, є один чинник, який можна визначити як головний. Він полягає у ***відсутності єдиних уніфікованих архітектурних рішень щодо побудови таких систем***. З цього приводу доречно навести досвід лідерів в інформатизації органів влади, наприклад США, який наведено у висновку федеральної ради керівників з питань інформатизації: «*Якщо федеральний уряд продовжить робити те, що робить (тобто створювати безархітектурні рішення), то ми будемо продовжувати отримувати те, що маємо (тобто непрацездатні, зайво дорогі й назавжди зв'язані в заплутаний клубок дані, додатки й технології*)»[50].

Звертаючись до поняття архітектури, слід зазначити, що його потрібно розуміти так, як визначено у міжнародному стандарті IEEE Standard 1471–2000: «Фундаментальна організація системи, втілена в її компонентах, їх взаємозв'язках один з одним і оточенням, і принципах її створення».

Таким чином, згідно з проведеним аналізом до основних напрямків, що мають враховуватися при створенні АІАС і визначати її архітектуру, належать наступні.

1. Автоматизація (електронізація) документообігу в органах влади всіх рівнів та його інтеграція. Разом з використанням електронного цифрового підпису це дасть можливість реального втілення ідей безпаперової інформатики та різкого підвищення ефективності систем державного управління.

2. Забезпечення єдиного поля програмно-інформаційного моделювання управлінської діяльності органів держаного управління, що має на меті реалізувати принцип формування і зміни документної бази на основі застосування програмного моделювання і автоматичного генерування документів для зняття неузгодженостей управлінських документів різної відомчої підпорядкованості.

3. Автоматизований моніторинг стану управління системами державної влади на основі вироблених критеріїв і показників роботи за допомогою автоматизованих засобів і технологій, що має на меті досяг-

[50] USA Federal CIO Council.

нення якомога об'єктивнішого аналітичного відображення стану справ у різних ділянках державної діяльності.

4. Прогнозно-аналітична діяльність на основі інтелектуалізованих програмно-інформаційних технологій, ділових ігор та інших форм здобуття узагальненої і прогнозної інформації у вигляді нових знань для упереджувального планування роботи державних органів.

5. Проведення колективних експертиз та обговорень в автоматизованому режимі при виробленні і прийнятті рішень на різних рівнях державного управління.

6. Ведення і поповнення джерел державної інформації на основі нових технологій сховищ даних, репозитаріїв та електронних бібліотек з метою забезпечення постійного уточнення й розширення інформаційної бази для підтримки прийняття рішень і для інформування населення.

7. Проведення соціологічних досліджень на основі електронних засобів інформації та широкого доступу до Інтернету з метою одержання додаткової інформації та її використання при обґрунтуванні прийняття рішень.

8. Забезпечення прозорості управління на основі розширення зв'язків із громадськістю на зразок «електронного уряду» та розвиток на цій базі демократичних засад управління державою.

Роль держави в інформатизації органів влади. Як вказувалося, аналіз завдань інформатизації органів влади свідчить про кількість і складність проблем, які необхідно вирішувати в сфері інформатизації. Це передбачає необхідність запровадження довгострокового процесу інтеграції та координації зусиль багатьох органів влади, наукових кіл, громадськості. Підтвердженням тому є ставлення В.М. Глушкова до реалізації започаткованого ним проекту ОГАС «общегосударственной автоматизированной системы», коли він казав, що це перевищує за своєю складністю та ступенем інтеграції космічну і ядерну програми. До речі, В.М. Глушков вважав виконання цього завдання головною справою свого життя, адже він розраховував, що ОГАС може врятувати економіку Радянського Союзу, що слабшала, і намагався довести це керівництву країни[51].

Ілюстрацією складності інформатизації влади може слугувати рис. 2.10, на якому показано місце АІАС органу влади, «вкладеної» у складну ієрархію оточуючих систем, які у різні часи ініціювалися урядом і

[51] З книги члена-кореспондента НАНУ Б. Малиновського «Очерки по истории компьютерной науки и техники в Украине».

мають бути створені за підтримкою держави [143]. Про ці системи мова піде на подальших сторінках книги.

Рис. 2.10. Ієрархія оточення АІАС

Таким чином, є всі підстави сформувати висновок, що лише державне регулювання сфери інформатизації може привести до створення

відповідної інфраструктури та формування в країні інформаційного суспільства [144].

З урахуванням цього, для забезпечення передумов широкого створення та ефективного використання АІАС в органах влади вважається за необхідне здійснення державою послідовних кроків у таких напрямках:

1) остаточно сформувати і постійно забезпечувати реалізацію державної політики у сфері інформатизації органів влади;

2) інтенсифікувати перехід українського суспільства до спілкування з «електронним урядом»;

3) спрямувати завдання Національної програми інформатизації в першу чергу на реалізацію проектів АІАС з урахуванням питань «електронного уряду» та інформаційної безпеки державної влади;

4) забезпечити створення нормативно-правової та нормативно-технічної бази сфери інформатизації органів влади;

5) підсилити регіональну складову інформатизації органів влади;

6) здійснювати заходи, спрямовані на захист інформації та забезпечення інформаційної безпеки державних органів в умовах застосування інформаційних технологій;

7) забезпечити керованість процесу інформатизації органів влади.

Особливу увагу з боку держави має бути приділено питанням інформаційної безпеки влади, що безпосередньо пов'язані з напрямками державної політики у сфері інформаційної безпеки України, визначених Доктриною інформаційної безпеки України.

Ситуація, що існує в сфері інформаційної безпеки органів державної влади України, вимагає невідкладного вирішення таких ключових проблем, як розвиток науково-практичних основ інформаційної безпеки державної влади, що відповідає сучасним умовам політичного і соціально-економічного розвитку країни, формування нормативно-правової бази забезпечення інформаційної безпеки органів влади, в тому числі розробка регламенту інформаційного обміну для органів державної влади і управління, нормативного закріплення відповідальності посадових осіб органів влади за дотриманням вимог інформаційної безпеки, розробка механізмів реалізації прав громадян на державну інформацію в системі «електронного уряду» та збереження персональної інформації, розробка сучасних методів і засобів, що забезпечують комплексне розв'язання задач захисту інформації в автоматизованих системах органів влади, розробка критеріїв і методів оцінки ефективності автоматизованих систем і засобів інформаційної безпеки в органах влади, комплексне дослідження діяльності персоналу орга-

нів влади в умовах функціонування автоматизованих інформаційно-аналітичних систем, у тому числі методів підвищення мотивації використання ними усіх можливостей інформаційних технологій з одночасною морально-психологічною стійкістю в питаннях захисту державної інформації, зокрема секретної і конфіденційної.

Електронна інфраструктура держави. Формування інформаційно-аналітичних систем органів державної влади як бази формування в країні системи «Електронний уряд» свого часу передбачалось серед головних завдань і пріоритетів державної довгострокової програми «Електронна Україна»[52], що фактично спрямовувалась на забезпечення формування електронної інфраструктури держави (рис. 2.11) [145].

Рис. 2.11. Електронна інфраструктура держави

Найважливішими умовами для забезпечення безпечного доступу широких верств населення до інформації органів влади є розвиток в Україні сучасної національної інформаційної інфраструктури шляхом створення у першу чергу системи національних інформаційних ресур-

[52] З-за фінансових питань проект не пройшов узгодження в комітетах Верховної Ради України.

сів, підвищення ефективності використання державних, корпоративних і приватних інформаційних ресурсів і формування вітчизняної індустрії інформаційних послуг (*e-Content*), розвиток інфраструктури на засадах стимулювання вітчизняних виробників і користувачів новітніми інформаційно-телекомунікаційними засобами і технологіями, комп'ютерними системами і мережами та всебічного розвитку національного сегмента Інтернету (рис. 2.12). На це спрямовані й напрямки державної політики у сфері інформаційної безпеки, визначені Доктриною інформаційної безпеки України.

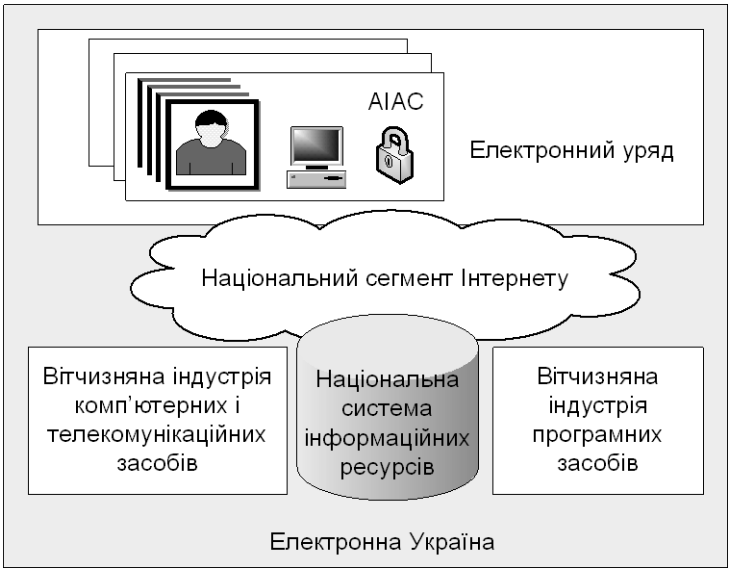

Рис. 2.12. Найважливіші умови для забезпечення безпечного доступу широких верств населення до інформації органів влади

З іншого боку, ІАС органів влади як найважливіші елементи електронної інфраструктури країни, що мають забезпечувати ефективне розв'язання задач аналізу, моделювання, прогнозування, планування заходів, підготовки рішень, контролю за виконанням рішень і заходів, документування, можуть використовуватися різними структурами як державними, так і комерційними.

Багатофункціональність, значні обсяги інформації, що мають опрацьовуватись у режимі майже реального часу вимагають не лише використання в органах державної влади для забезпечення автоматизації

інформаційно-аналітичної діяльності новітніх досягнень комп'ютерної науки, математичних методів та інформаційних технологій, а також інтеграції інформаційно-аналітичних систем органів державної влади в єдину загальнодержавну систему (рис. 2.13). Без створення такої інтегрованої інформаційно-аналітичної системи державної влади (ІІАС) забезпечити надання населенню адміністративних послуг буде неможливим.

Рис. 2.13. Інтегрована інформаційно-аналітична система органів державної влади у системі «електронного уряду»

Фактично електронна інфраструктура надання послуг державними органами в системі електронного уряду з урахуванням вимог ІБ має базуватись на трьох основних складових. По-перше, це сховище державних інформаційних ресурсів, що територіально розподілене. По-друге, це система центрів, що підтримують надання населенню й організаціям послуг з використання електронного цифрового підпису. Нарешті, це національна ідентифікаційна система для авторизованого доступу.

В умовах *е*-уряду люди прагнуть ефективних засобів заміни підпису і печатки, що використовуються на папері, які б були захищені та надійні. Побудована подібним чином інфраструктура має сформувати довірче середовище інформаційної взаємодії як між органами влади, так і між державою, бізнесом і населенням.

Існує думка, що для того щоб Інтернет «запрацював» на соціальні потреби, необхідно перетнути бар'єр кількості користувачів у 20 відсотків. У цьому відношенні цікавим є досвід скандинавських країн, у яких дуже добре розвинені інформаційні технології завдяки тому, що в них було реалізовано низку важливих і успішних кроків на державному рівні.

Наприклад, у Швеції був прийнятий закон стосовно того, що комп'ютери й оргтехніка амортизуються за прискореною схемою. Після цього підприємствам дозволили передавати цю техніку безкоштовно своїм співробітникам. У підсумку за дуже короткий термін громадяни за низькими цінами або навіть безкоштовно придбали особисті комп'ютери. А коли вдома з'являється комп'ютер, виникає можливість і бажання підключитися до Мережі.

Щоб зробити реальністю захищену ідентифікацію особи державичлени Європейського союзу інвестують у великий проект створення єдиної електронної системи управління ідентифікацією (Electronic Identity Management — eIDM), який включено до Плану дій ЄС щодо прискорення створення електронного уряду до 2010 р.[53]

Основою цієї системи є електронний цифровий підпис, ідентифікаційні старт-картки, сертифікація електронних документів (що видаються державними органами) та технології фіксації часу.

Відомі також програми типу «Народний комп'ютер», мета яких — фінансова підтримка, що дозволяє зробити комп'ютер дешевше за рахунок спрощення конфігурації. Цю програму проводять у різних країнах

[53] i2010 e-Government Action Plan: Accelerating e-Government in Europe for the Benefit of All / Brussels, 25.04.2006. COM(2006) 173 final.

такі компанії, як Intel, Hewlett-Packard, Microsoft.

У зв'язку з цим слід зазначити, що стимулюючими чинниками для зростання соціальних потреб використання населенням державної інформаційної інфраструктури та досягнення вказаних перспектив, зокрема, інтенсифікації інформатизації органів влади, є принаймні два — це запровадження електронного нотаріату та подання суб'єктами господарювання та фізичними особами електронної звітності до податкових органів.

Так, наприклад, передача електронної звітності засобами телекомунікацій є важливим і таким, що динамічно розвивається, сегментом реальних послуг. У Європі й Америці електронна звітність, як правило, обов'язкова для всіх платників податків (як у Німеччині) або для значної їхньої частини (крім найдрібніших, як у США), і ніде вона не є безкоштовною.

Подання електронної звітності каналами зв'язку пов'язано з вирішенням для платника податків таких проблем, як застосування засобів криптографічного захисту інформації, ключів електронного цифрового підпису, підготовка відповідно до встановленого формату файла звіту, нарешті, забезпечення доступу до Інтернету. Для забезпечення такого складного технологічного процесу електронного документообігу в країні доцільно запроваджувати інституцію спеціальних операторів. Це підтверджує й світова практика: у всіх країнах, де успішно впроваджені системи електронної звітності, є й обслуговуючі їх оператори, що конкурують між собою за клієнтів.

Спецоператори виконують роль системних інтеграторів — підтримують сервери, технологічну інфраструктуру, надають засоби захисту інформації й електронного підпису. Вони виступають також як незалежні арбітри у суперечках про дату проходження документа (на сервері фіксується факт його надходження в зашифрованому вигляді), забезпечують цілісність документообігу й вирішують проблемні ситуації.

На спецоператорів покладаються такі функції[54]: технічна та юридична підтримка документообігу (транспорт, моніторинг своєчасності доставки документів, розбір конфліктних ситуацій, пошук зниклих звітів), юридично значуща фіксація дати й часу проходження документів (як незалежна третя сторона), поставка засобів криптографічного захисту інформації та електронного цифрового підпису, забезпечення безпеки при передачі електронних документів і забезпечення їхньої юри-

[54] Джерело — www.directum-journal.ru

дичної значущості, постачання й супровід прикладних програмних засобів, призначених для формування звітності та її перевірки на відповідність установленим форматам.

Запровадження такого механізму дозволяє вести мову про побудову загальнодержавної інфраструктури надання послуг електронного документообігу, що має значний потенціал розвитку аж до системи «єдиного вікна», призначеної для зручної взаємодії господарюючих суб'єктів і всіх державних органів на базі такого документообігу.

До вказаних двох головних чинників, що мають стимулювати зростання соціальних потреб використання населенням державної інформаційної інфраструктури, слід віднести ще дві соціально значущі системи — надання послуг телемедицини та дистанційна освіта.

Телемедицина являє собою «комплекс рішень, що поєднує можливості інформаційних технологій, медичного діагностичного обладнання, телекомунікаційних мереж з метою підвищення якості й доступності медичних послуг. За рахунок сучасних можливостей інфокомунікацій, телемедицина дозволяє довести медичні послуги найвищої якості до самих віддалених територій, у тому числі проводити діагностику пацієнтів на відстані, дистанційний прийом висококваліфікованими фахівцями, навіть закордонних медичних центрів, вести електронну базу медичних даних»[55].

На сьогодні розвиток цього напрямку визнано як один з найперспективніших у національній медичній політиці багатьох країн. Так, клінічні телемедичні програми зараз існують майже в кожному штаті США, введено десятки потужних мереж для цих цілей. Великі лікувальні клініки мають і свої власні програми з телемедицини.

З тих соціальних проектів, що отримали в Україні відчутний розвиток, дистанційна освіта мабуть займає перше місце. Практично всі великі навчальні заклади пропонують такі послуги, якими користується вже значна частина населення.

Для реалізації названих чинників потрібна національна система ідентифікації. Її основою може стати проект уніфікованої соціальної картки. Інтегрована інформаційна система підтримки надання й обліку соціальних послуг населенню з використанням інтелектуальної картки може створити юридично значущий інформаційний простір надання послуг з обов'язковою авторизацією користувачів, що викликало б довіру громадян і організацій.

[55] Джерело — «Накануне.ру», 12.07.2004.

Вирішення вказаних проблем неможливо без всебічного застосування Інтернет-технологій. Інтернет є найменш впливовою з боку держави сферою інформатизації і в Україні розвивається за законами ринкової економіки. Може через це, однак темпи його розвитку поки що недостатні, рівень розвитку національного сегмента все ще відстає від багатьох європейських країн. Це часто пояснюється пов'язаністю як з економічною ситуацією в країні, так і з низьким рівнем розвитку інфраструктури зв'язку в регіонах. Водночас, наприклад, уряд Нової Зеландії визначив, що розвиток всесвітньої мережі Інтернет для Нової Зеландії у 21 столітті «все одно, що заморожена вівця наприкінці 19-го» (йдеться про спосіб транспортування м'яса на далеку відстань за допомогою рефрижераторів, встановлених на судах, що дозволило перетворити сільське господарство цієї країни на стратегічно важливу експортну галузь)[56]. Як наслідок, Нова Зеландія за розвитком електронного уряду йде впритул за Канадою і США.

Повільний розвиток національного сегмента Інтернету пов'язаний ще й з відсутністю соціальної потреби населення в його використанні. У зв'язку з цим запровадження системи «Електронного уряду» має стати тією рушійною силою, що дасть новий поштовх до активізації діяльності Інтернет-сервіс-провайдерів і розвитку Інтернет-послуг (рис. 2.14).

Однак для забезпечення рівних прав доступу громадян до Інтернету потрібні додаткові заходи з боку держави, зокрема, щодо впорядкування адміністрування національного домену (*ua*), створення національної магістральної мережі передачі даних (*backbone*), створення центрів і точок суспільного доступу до ІКТ (*e-Access*), зокрема створення мережі пунктів колективного доступу (ПКД) до Інтернету [146–148], особливо у сільських і віддалених районах країни, як суттєвого кроку на шляху до забезпечення доступу населення до ІАС органів влади.

При цьому увагу держави має бути спрямовано на створення ПКД на базі відділень «Укрпошти» та сервісних центрів ВАТ «Укртелеком», а також на забезпечення умов для значного поширення Інтернет-кіосків (*e*-кіосків, інфоматів) у торговельних центрах, аеропортах, на вокзалах, а також у бібліотеках та освітніх закладах [149]. Для України реалізація ідеї ПКД означає необхідність забезпечити такими послугами перш за все мешканців близько 28 тис. населених пунктів, які знаходяться в сільській місцевості. На вирішення проблем загального доступу до ін-

[56] The Knowledge Economy, a submission to the new Zealand Government by the Minister for Information Technology's / IT Advisory Group. — August, 1999.

фокомунікаційних технологій і послуг орієнтовані Національна програма створення Єдиної національної системи зв'язку України, Національна програма інформатизації (НПІ).

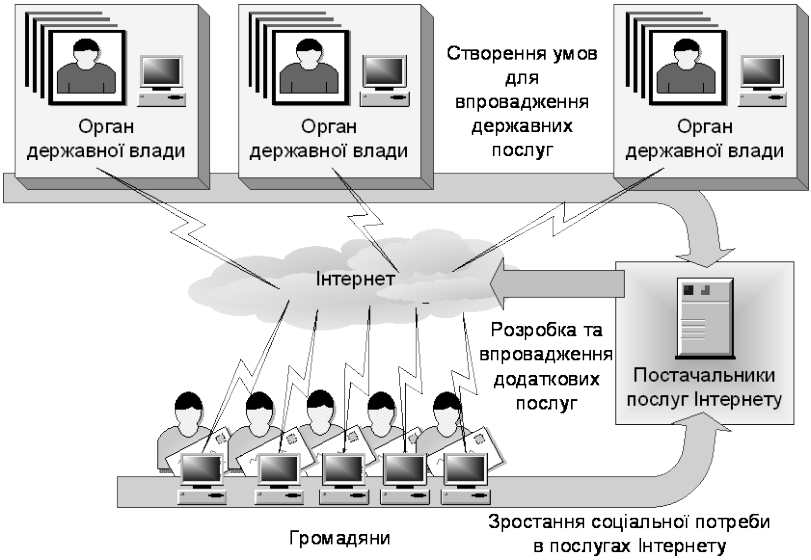

Рис. 2.14. Стимулювання розвитку національного сегмента Інтернету в системі «електронного уряду»

Реалізація цих програм має бути спрямованою на створення уніфікованого програмно-апаратного комплексу ПКД, що забезпечує надання типового переліку управлінських та інших послуг, які повинні бути реалізовані із застосуванням сучасних технологій. Дослідження можливості застосування вільного програмного забезпечення та, зокрема, операційного середовища «Linux» у ПКД різних типів і формування висновків і рекомендацій щодо можливості та доцільності застосування цього операційного середовища при створенні різних типів ПКД повинні забезпечити питання інформаційної безпеки ПКД.

Підсумки до розділу

Деталізація функцій органів державної влади показує, що загальна кількість функціональних задач, які розв'язуються органами державної

влади в процесі управління в сучасних умовах, є чималою, а інформаційні задачі складають найбільшу їх частину.

Багатофункціональність, значні обсяги інформації вимагають використання в органах державної влади для забезпечення автоматизації інформаційно-аналітичної діяльності новітніх досягнень комп'ютерної науки та інформаційних технологій, а також інтеграції інформаційно-аналітичних систем органів державної влади до єдиної загальнодержавної системи.

Аналіз особливостей автоматизації інформаційно-аналітичної діяльності в органах державного управління різних країн, зокрема, таких провідних як Канада та США, показує, що головним з пріоритетів урядів цих країн є формування систем *е*-уряду, питання керування інформацією та документами та забезпечення доступу громадян до урядової інформації з одночасним забезпеченням автентифікації користувачів та захисту інформації.

Аналіз сучасного рівня забезпеченості технічними і програмними засобами інформатизації органів влади України свідчить, що в цілому зараз у більшості органів влади, а також й обласних держадміністраціях, проведена лише часткова інформатизація з установкою обладнання та програмно-інформаційних засобів для розв'язання окремих комплексів задач. Деякими органами влади проведені або ведуться роботи з проектування та створення ІАС. Особливості автоматизації інформаційно-аналітичної діяльності в органах державного управління України полягають переважно у створенні локальних інформаційних ресурсів.

Аналіз сучасного стану інформаційної взаємодії між органами державної влади свідчить про наявність низки недоліків існуючої системи збирання інформації, про неефективність розповсюдження статистичної та аналітичної інформації, про незадовільність інформаційних потреб органів влади, про недостатній рівень забезпечення інформаційної безпеки.

Для забезпечення ефективного функціонування АІАС мають стати елементами загальної електронної інфраструктури країни, що певним чином повинна розвиватися за рахунок підтримки держави. Вирішення проблем формування та розвитку інформаційного забезпечення органів влади, доступу до державних інформаційних ресурсів неможливе без широкого застосування Інтернет-технологій.

РОЗДІЛ 3

ФОРМАЛІЗАЦІЯ ТА МОДЕЛЮВАННЯ АІАС

3.1. Підходи до формалізації та моделювання АІАС

Проблеми аналізу та моделювання при створенні АІАС. Хоча на практиці, в технічній документації та в наукових публікаціях поняття «інформаційно-аналітична система органу державної влади» широко використовується, але його чіткого загального визначення та наукового обґрунтування досі не існує. Це часто-густо призводить до неоднозначних тлумачень і трактувань, що є стримуючим фактором у процесі формування систем інформатизації органів влади та подальшої їх інтеграції для забезпечення підтримки державного управління, та ускладнює вирішення загальних проблем інформатизації влади.

Відправною точкою для визначення вказаного поняття, згідно з аналізом існуючих публікацій, має бути сформоване уявлення, з одного боку, про інформаційно-аналітичну діяльність в органі влади як систему підтримки прийняття рішень, а з іншого боку — про АІАС як складну соціотехнічну систему. Процес прийняття рішень, зокрема, на рівні великих організаційних систем, де задачі управління є слабо структурованими і має місце суперечливість, неоднозначність і неповнота даних і знань, та відповідні технології науково достатньо опрацьовані.

Відомо, що проектування складних соціотехнічних систем неможливе без етапу системного аналізу. Однак головною проблемою як підтримки прийняття рішень, так і для створення таких інформаційних систем залишається пошук відповідних моделей.

Методи формалізації задач структурного синтезу мають суттєву наукову базу, починаючи з методів дискретного програмування, багатокритеріальної оптимізації та імітаційного моделювання до сучасних комп'ютерних технологій типу SADT, IDEF, HIPO із графічними засобами структурного подання.

Однак практично всі відомі методи для успішного застосування вимагають наявності або точних величин, які можна поставити у відповідність суттєвим ознакам, або відповідних правил, або формалізації знань тощо. Враховуючи специфіку інформаційно-аналітичної діяльності в органах влади та, відповідно, їхньої АІАС, задовольнити стосовно них усі такі вимоги найчастіше буває неможливим.

Крім того, системи автоматизованого управління в суспільній сфері та на рівні структур влади завдяки своїй структурній складності наштовхуються на високий рівень ентропії, адже, як відомо, загальна невизначеність системи є сумою окремих невизначеностей елементів V_i:

$$H_{\Sigma} = \sum_{i=1}^{n} H_{V_i} .$$

Високий рівень ентропії як міри релевантності стану управління його цільовим установкам часто-густо зводить нанівець увесь ефект автоматизації [118]. Але, як відомо, взаємна невизначеність залежних елементів системи є меншою, ніж незалежних. Іншими словами, за наявності ефективного керованого взаємозв'язку між елементами система стає більш організованою. Тому при проектуванні треба розглядати АІАС не лише як систему, що розв'язує аналітичні задачі, а й як систему, яка вимагає управління.

Тоді задача управління у системі може бути сформульована як задача визначення оптимальних структурних змін динамічної системи $S(t_0) \xrightarrow{R_o} S(t_n)$ й формування скоординованих пропозицій щодо її удосконалення та розвитку.

До АІАС, як не до якої іншої системи, має відношення принцип нових задач за В.М. Глушковим. Впровадження засобів інформатизації в органах державної влади має на меті, в першу чергу, не забезпечення рутинних операцій, а створення нових технологій підтримки прийняття рішень. Згідно з цим, вирішення проблеми моделювання такої системи управління як АІАС полягає не стільки у формалізації структури об'єкта, як в її концептуальному проектуванні, визначенні нових задач і критеріїв управління. У цьому сенсі вбачається перспективним застосування ідей та механізмів штучного інтелекту, інтелектуальних систем та гіпотетичного моделювання.

Таким чином, можна зробити висновок, що на цей час ще не існує ані методів інтеграції елементів інформатизації органу державної влади в єдину систему, ані концептуальних чи інформаційних моделей таких автоматизованих інформаційно-аналітичних систем. У зв'язку з цим постає задача не лише розробки вказаних моделей, а й розробки, на базі запропонованих моделей, парадигми, до якої належали б сукупність архітектурних рішень і методологія формування як окремих АІАС ор-

ганів державної влади, так і міжвідомчих інформаційно-аналітичних систем.

Усе це дає підстави вважати, що створення концептуальної моделі АІАС та відповідних парадигм на її засадах, що стали б основою побудови конкретних архітектур АІАС кожного органу влади, вироблення теоретично обґрунтованих методів організації технологічного процесу обробки інформації і планування створення та модернізації систем на всіх стадіях її життєвого циклу, є гостро актуальною проблемою, вирішення якої сприятиме більш стрімкому узгодженому розвитку інформатизації владних структур, забезпеченню інформаційної безпеки влади і через це більш динамічному зростанню соціально-економічного рівня та добробуту населення.

Розробка основ побудови АІАС, що базуються на сучасних інформаційних технологіях, засобах формалізації процесів функціонування органів влади, на відповідних концепціях та моделях має сприяти не лише забезпеченню подальшого розвитку інформатизації органів державної влади та безпеки її інформаційного простору, а й формуванню розвинутого інформаційного суспільства в країні та інтеграції її до світового інформаційного простору.

Для досягнення поставленої мети перед науковцями та фахівцями постає необхідність вирішення цілої низки конкретних завдань, а саме:

- дослідити особливості застосування архітектурних рішень для створення автоматизованих інформаційно-аналітичних систем окремих органів державної влади України;
- визначити шляхи підвищення ефективності розвитку ІІП ДВ та забезпечення необхідного рівня його інформаційної безпеки;
- формалізувати процес інформаційної взаємодії ОДВ;
- розробити та теоретично обґрунтувати концептуальну та інформаційну моделі АІАС;
- структурувати керований технологічний процес опрацювання інформації в ОДВ і подати його у вигляді інформаційно зв'язаних слабоформалізованих завдань;
- визначити умови існування скоординованого набору регулюючих впливів на процес опрацювання інформації в ОДВ;
- розробити формалізований опис процесів опрацювання інформації в ОДВ;
- визначити основи інформаційної взаємодії органів державної влади та створення системи інформаційних ресурсів органів державної влади;

- визначити основні засади регламенту такої взаємодії, особливості забезпечення управління системами інформаційних ресурсів;
- розробити моделі і методи ідентифікації інформаційного навантаження в ОДВ;
- розробити методологічні принципи організації й створення АІАС;
- розробити методологію побудови технічних і організаційних підсистем АІАС;
- дослідити підходи до побудови апаратного та програмного забезпечення технологічних складових АІАС.

Теоретико-множинна модель органу влади як системи управління. Як відомо, під керуванням[57] (управлінням) в кібернетичному сенсі розуміють процес впливу керуючого органу на керований об'єкт для досягнення деяких цілей. Необхідною умовою цього процесу є наявність в керуючому органі інформації про стан керованого об'єкта та формування керуючим органом інформації, яка може змінювати стан об'єкта залежно від цілей керування в деяких властивих для нього межах.

Існуючи в просторі та часі, система управління взаємодіє з навколишнім середовищем, складовою частиною якого вона є. Зміна стану зовнішнього середовища впливає на всі елементи даної системи. У свою чергу, система управління може впливати на стан зовнішнього середовища. При цьому стан кожного елементу системи управління та зовнішнього середовища можна характеризувати деякими визначеними наборами параметрів.

Метою керування є або підтримання заданих значень деяких параметрів системи при різних станах зовнішнього середовища, або виконання системою заданої програми дій щодо змін значень власних параметрів чи параметрів зовнішнього середовища. Таким чином можна зазначити, що систему державного управління можна описати з використанням кібернетичного підходу. Потрібно лише відмітити, що при кібернетичному підході до керуючих систем кінцеві цілі керування звичайно виступають як задані.

За своєю структурою керуючі системи можуть буті як простими — одноконтурними, так і складними — багатоконтурними. З названих позицій систему державного управління слід відносити до багатоконтур-

[57] З розвитком автоматизованих систем, зокрема у сфері виробничо-соціальній, здебільшого почав застосовуватись термін «система управління».

них складних систем управління, в яких кожен державний орган — це, у свою чергу, складна система.

Вочевидь, найбільш загальним є визначення системи, що було надано М. Месаровичем: системою називається відображення на не порожніх (абстрактних) множинах:

$$S \subset \times\{V_i : i \in I\}, \tag{3.1}$$

де × — символ прямого (декартового) добутку; V_i — елемент системи з індексом *i*; *I* — множини індексів.

Система державної влади містить у собі сукупність (кінцеву множину) суб'єктів управління, тобто органів державної влади, об'єктів управління, тобто сфер і галузей суспільного і державного життя, що знаходяться під організуючим впливом держави, і процесів управлінської діяльності.

Для кінцевої множини елементів відображення (3.1) можна переписати у вигляді

$$S \subset V_1 \times V_2 \times ... \times V_n. \tag{3.2}$$

Згідно з (3.2) стає очевидним визначення системи державної влади як множини елементів V_i, що знаходяться у взаємодії один з одним. Ці взаємодії в системі державної влади являють собою форми і процедури суспільних відносин, завдяки яким реалізуються прямі і зворотні зв'язки між суб'єктами й об'єктами управління (рис. 3.1). Основними елементами є суб'єкти управління, тобто органи влади.

Кожний елемент V_i може бути представленим як

$$V \supset (x, y, z, f, g), \tag{3.3}$$

де $x = x(t)$ — вхідний вплив (інформаційний потік); $y = y(t)$ — вихідний інформаційний потік (реакція системи на вхідний вплив); $z = z(t)$ — внутрішній стан системи. Ці складові подаються у вигляді кінцевої множини функцій часу *t* (наприклад, $x = \{x_i(t),...,x_k(t)\}$). Через *f* і *g* визначаються функціонали, що відображають поточне значення внутрішнього стану $z(t)$ і вихідного потоку $y(t)$.

Рис. 3.1. Система державної влади як система управління

Як зазначалось, органи державного управління слід віднести до класу складних соціальних систем [69]. Системи такого типу відносяться до нетрадиційних систем завдяки своїй унікальності (непереносності), здатності еволюціонувати у часі, змінюючи структуру і функції, разом із цим змінюючи й самі процеси управління. Елементи таких систем мають активну природу, і їх поведінка може протистояти цілям управління. Таким чином, орган державного управління має діяти в умовах постійної адаптації.

Важливим елементом таких систем управління є наявність ОПР — особи, що приймає рішення (рис. 3.2). Перед ОПР постає спочатку проблема пошуку поля задовольняючих дій (стратегії), а потім — проблема вибору кращої дії, тобто рішення в цьому полі (тактики). Розв'язуючи по черзі зазначені задачі, ОПР будує конкретну модель дій для конкретної ситуації (виробляє структуру задачі). У створенні такої моделі важливу роль відіграє досвід ОПР, його загальні й спеціальні знання, свобода волі. Вони істотно впливають на доведення до кінця міркувань (дедуктивні й індуктивні умовиводи) у процесі ухвалення рішення. Са-

ме вони при прийнятті рішень є вирішальним фактором їхньої ефективності (або неефективності) і водночас ще одним чинником, завдяки якому систему можна віднести до класу нетрадиційних.

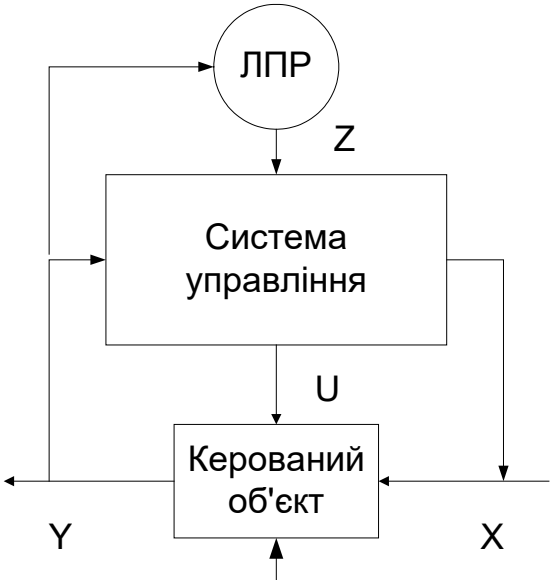

Рис. 3.2. Роль ОПР у системі управління

«Управління складними об’єктами принципово неможливе без залучення інформації, яка не може бути представлена кількісно. Це семантична, тобто змістовна, якісна інформація» [150, с. 4].

Згідно з цим, у складі системи управління органу влади поряд з певним механізмом породження чинників управління (рішень) (*MS*) має бути й модель знань (*MK*), яка використовується процесами управління (рис. 3.3).

Отже, система, що розглядається, відноситься до класу систем семіотичного типу з адаптацією. При цьому вибір з набору процедур керування, що реалізується механізмом *MS*, здійснює певний адаптер *A*, а постійні модифікації моделі *MK* забезпечуються інтерпретатором *I*. Вказана взаємодія системи управління та керованого об’єкта реалізується певною множиною інформаційних потоків.

Управління функціонуванням ОДВ вимагає знань про його структуру, найбільш істотні аспекти побудови, функціонування та динаміки

розвитку. Широкі можливості мови теорії множин дозволяють отримати опис ОДВ, що має всі типові риси складних систем, із різним ступенем деталізації.

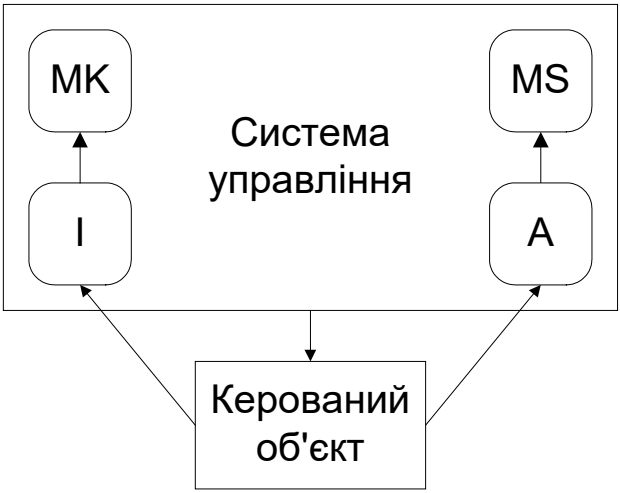

Рис. 3.3. Система семіотичного типу з адаптацією

Самим загальним є теоретико-множинне визначення [119], коли нецілеспрямована система визначається як

$$S = (E, R), \tag{3.4}$$

де E — деяка множина елементів; R — деяка множина бінарних відношень $R \subset E \times E$, що реалізована на множині E.

Для систем, які прийнято називати складними, елементами множини E є множини $E = \{E_1^1, E_2^1, ..., E_N^1\}$, які є множинами 1-го рівня системи. Кожна з множин 1 рівня, у свою чергу, може складатися з елементів, які є множинами, тобто множинами 2-го рівня і т.д. На множинах кожного з рівнів діють відношення (бінарні й багатомісні).

Для складних систем, до яких відноситься й ОДВ, зазвичай кількість рівнів не вичерпується двома. При цьому відношення діють не тільки на множинах одного рівня, але й між елементами множин різних рівнів.

Пара множин $C = (E, R)$ може бути названа ***структурою***. Структура має деякі множини властивостей, які не випливають прямо із властивостей елементів, що її складають, а є результатом взаємодії елементів на базі реалізованих відношень. Ці властивості називаються системними, інтегральними або емерджентними [69].

Якщо задано мету системи, відображення даної мети на множину властивостей виділяє деяку підмножину $M \subset P$. Саме ця підмножина властивостей M дозволяє системі змінюватися відповідно меті системи, тобто бути цілеспрямованою. Така система може бути визначена як

$$S = (E, R, M). \tag{3.5}$$

Під впливом зовнішнього середовища й процесів, що відбуваються в самій системі, пари (E, R) можуть бути, а можуть і не бути статичними, вони можуть змінювати в часі, тобто може відбуватися зміна структури системи.

Встановлення об'єктивних закономірностей формування властивостей системи як явних або неявних функцій якісних і кількісних характеристик елементів, з яких вони складаються, і відношень, які їх упорядковують і організують у цілісну систему, відкриває перспективу усвідомленого синтезу цілеспрямованих штучних систем, призначених для досягнення деяких заданих цілей.

Згідно з визначенням цілеспрямованої системи первинним при її синтезі є задання мети (цілей) системи. Досягнення будь-якої мети в принципі можливо тільки в тому випадку, якщо система має деякий певний набір властивостей. Визначення й формалізація цих властивостей є найважливішим етапом синтезу системи.

Розрізняють зовнішні (екзогенні) і внутрішні (ендогенні) цілі системи. ОДВ є елементом метасистеми державної влади, для якої у свою чергу справедливе визначення абстрактної системи, тобто системи, яка є множиною однорідних або різнорідних елементів, упорядкованих множиною відношень, і, як наслідок цього, такою, що має деякий набір властивостей.

Це означає, що метасистема визначає якісний склад і інтервал можливих кількісних значень властивостей ОДВ як елемента. Це екзогенні цілі. Внутрішні цілі ОДВ полягають у деталізації зовнішніх і виборі більш вузького інтервалу або конкретного кількісного значення всієї сукупності властивостей. Таким чином, метасистема формує припус-

тиму цільову область, у рамках якої ОДВ формує свою власну локальну мету.

Із-за того, що ОДВ є динамічною системою, кількісні характеристики елементів, з яких складається система, й інтенсивність відношень змінюються у часі. Таким чином, властивості системи так само змінюються у часі, тобто кожному поточному стану структури ОДВ відповідають фактичні поточні значення властивостей. Порівняння цих значень із цільовими дозволяє визначити величину інтервалу неузгодженості (***проблемної ситуації***), мінімізація якого й є задачею поточного (оперативного) управління в ОДВ.

Фактичні властивості є кортежем різнорідних показників, що мають різні зміст, розмірність, напрямок домінування, вимірювальні шкали й у загальному випадку є суперечливими. У зв'язку з цим, для конструктивного аналізу стану ОДВ виникає необхідність формування деякої системи узагальнених скалярних, ситуаційно орієнтованих показників. Останнє означає, що кожному рівню аналізу й проблемної ситуації відповідає агрегований набір оцінок, що враховують як окремі показники (властивості), так і їхні різні групи, аж до повної їхньої множини. Ця множина показників є базовою для ідентифікації стану ОДВ і виступає, по-перше, як множина показників ефективності функціонування, а по-друге, як множина оптимізаційних цільових функцій при розв'язанні задач управління ОДВ.

Указана проблема для свого вирішення потребує організаційних заходів, які полягають у стандартизації зазначених показників, тому що тільки в цьому випадку можна побудувати цілісну ієрархію агрегованих моделей і отримати конструктивні абсолютні й відносні оцінки стану ОДВ.

Концепція інформаційної взаємодії органу влади. Якщо розглядати інформаційну взаємодію системи державної влади (ДВ) з навколишнім світом (рис. 3.4), то можна визначити, що вона складається на виході з двох інформаційних векторів ($Ð_{âèõ}$ та $N_{âèõ}$) впливу на суспільну систему (СС) як керований об'єкт і підпадає під дію двох векторів (G та I) зворотного зв'язку — від громадської думки та засобів масової інформації (ЗМІ). Водночас ДВ відпрацьовує запити на обслуговування, звернення та скарги від підприємств і населення (вектори $Ð_{âõ}$ та $N_{âõ}$). Треба також враховувати міжнародну діяльність держави, яка визначається збурюючою дією впливу міжнародних організацій та відношень з іншими державами ($Ì_{âõ}$) і вектором $Ì_{âèõ}$ відпо-

відних державних рішень. Нарешті, враховуючи складне зовнішнє оточення, система влади піддається загрозам інформаційної безпеки $W_з$. Враховуючи наявність і внутрішніх загроз, у системі державної влади можуть циркулювати й негативні потоки $W_{вн}$.

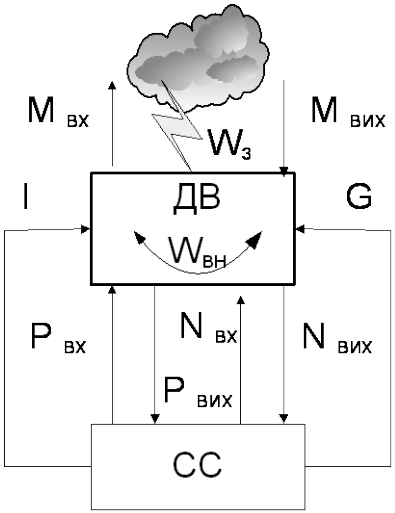

Рис. 3.4. Інформаційні потоки в системі державної влади

Органи державної влади як суб'єкти державного управління є елементами системи державної влади і на них також поширюється зазначена схема взаємодії. Але з множини відношень, що описуються векторами $P_{âèõ}$, $N_{âèõ}$, G, I, $P_{âõ}$, $N_{âõ}$, $\hat{I}_{âõ}$, $\hat{I}_{âèõ}$, $W_ç$, $W_{âi}$, кожному органу влади в межах його компетенції, визначеної для нього відповідними нормативно-правовими актами (наприклад, положенням про орган влади), відводяться певні підмножини $P'_{âèõ}$, $N'_{âèõ}$, G', I', $P'_{âõ}$, $N'_{âõ}$, $M'_{âõ}$, $M'_{âèõ}$, $W'_ç$, $W'_{âi}$ (рис. 3.5). Крім того, органи влади в структурі державного апарату мають взаємодію з вищими органами, наприклад, Кабінетом Міністрів (вектори $\hat{A}_{âõ}$, $\hat{A}_{âèõ}$) та з іншими органами влади (вектори $\hat{I}_{âõ}$, $\hat{I}_{âèõ}$), а також з підвідомчими підприємствами зі сфери управління (вектори $\tilde{N}_{âõ}$, $\tilde{N}_{âèõ}$).

Безпосередньо в структурі органа влади циркулюють похідні інформаційні потоки як результат прогнозно-аналітичної діяльності (F), програмно-інформаційного моделювання (L), службового документообігу (D), а також заходів щодо захисту інформації (Z).

З урахуванням наведеного, розвиваючи теоретико-множинне визначення системи (3.5), узагальнену модель системи S можна описати виразом:

$$S =< A, E, R, P_s, P_a, M >, \tag{3.6}$$

де A — активні елементи системи; E — пасивні елементи системи; R —

зв'язки між елементами; P_s — цілісний процес функціонування системи як набір паралельно взаємодіючих процесів P_a.

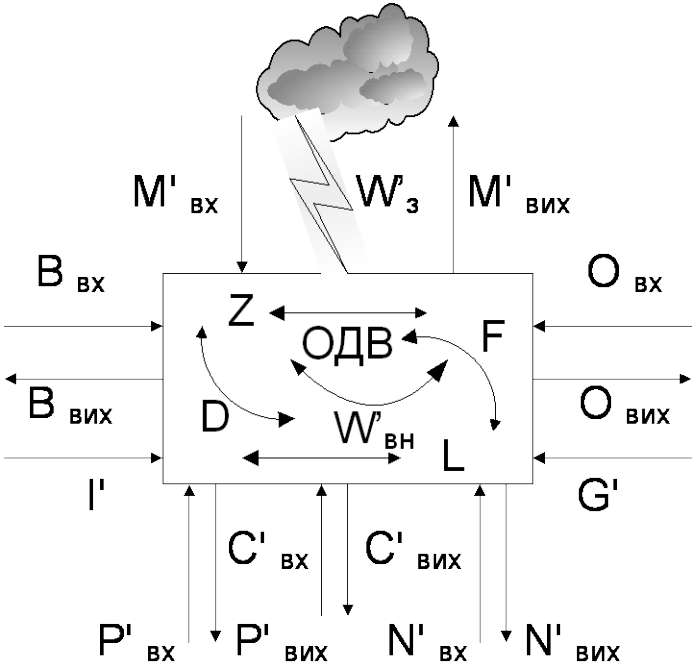

Рис. 3.5. Схема взаємодії органу влади в системі державної влади

При цьому

$$S = G(A, r); A = G'(A', r'), r \in R. \tag{3.7}$$

Таким чином, ураховуючи опис (3.6) та модель, що наведені на рис. 3.5, процес функціонування інформаційної системи P_s' деякого органа влади можна описати кортежем паралельно взаємодіючих процесів:

$$P_s' = \{P_{âõ}', P_{âèõ}', N_{âõ}', N_{âèõ}', G', I', M_{âõ}', M_{âèõ}', B_{âõ}, B_{âèõ}, O_{âõ,} O_{âèõ}, C_{âõ}, C_{âèõ}, W_ç', W_{âí}', F, D, L, Z\}. \tag{3.8}$$

Пріоритетність інформаційного підходу. Кожна із проблемних ситуацій вимагає управління системою. Під управлінням будемо розуміти зміну якісних і кількісних характеристик елементів і відношень, що утворюють структуру системи. Залежно від проблемної ситуації змінюється інтенсивність управління, починаючи від відбивання випадкових зовнішніх і внутрішніх збурювань, що пов'язане з адаптивною зміною кількісних характеристик елементів й інтенсивності відношень у порівняно вузьких межах, без зміни структури системи, до не тільки кількісних, але й якісних змін структури, що вимагає зміни числа елементів, їхніх функцій, кількісних і якісних характеристик, а також характеру й інтенсивності відношень.

У таких системах як ОДВ управляючими впливами є прийняті рішення у визначених точках траєкторії функціонування системи. Власне процес прийняття рішень у загальному випадку може бути структурованим на такі три основні етапи:

1) формування множини припустимих рішень U;

2) визначення метрики, у якій провадиться порівняння припустимих рішень $u \in U$ (задача оцінювання);

3) вибір із припустимої множини ефективного (найкращого) рішення $u^0 \in U$ (задача оптимізації).

Множина припустимих рішень U задається на основі змістовного аналізу конкретної задачі, найчастіше у неявному вигляді як підобласть області існування системи, обмежена певними співвідношеннями.

Розв'язання задачі оптимізації, тобто визначення найкращого рішення $u^0 \in U$, пов'язане з формалізацією поняття «найкраще». Для цього необхідно визначити метрику, у якій здійснюється порівняння якості рішень $u \in U$. У загальному випадку побудувати модель оцінювання, що дозволяє одержати скалярну, кількісну оцінку будь-якого рішення $u \in U$, не завжди є реальною задачею.

У традиційній постановці задача оптимізації як задача математичного програмування передбачає детермінованість об'єкта, а, отже, і відповідної математичної моделі, що означає визначеність структури й кількісних характеристик моделі на інтервалі планування. ОДВ належить до класу систем, для яких характерною є динамічна зміна в процесі функціонування структури, складу й кількісних значень параметрів, цільових настанов і т.ін. Тому для ОДВ реалізувати задачу прийняття рішення необхідно шляхом вибору ефективної стратегії поведінки з урахуванням часового сценарію поведінки зовнішнього середовища $w(t)$.

Кожному сценарію буде відповідати деяка оптимальна поведінка системи, тобто траєкторія зміни структури, параметрів, керованих змінних.

Але, як вказувалось, зовнішнє середовище є не повністю контрольованим навіть із позицій метасистеми. Це означає, що на рівні конкретної локальної системи точний сценарій зміни зовнішнього середовища невідомий і через зазначені вище причини погано піддається прогнозу. Тому можна робити тільки евристичні припущення про можливі значення $w(t)$. У таких умовах рішення u^0, обране для конкретного сценарію $w(t)$, для іншого сценарію $w'(t)$ може виявитися неприйнятним. Це обумовлено тим, що екстремальне рішення задачі умовного математичного програмування завжди перебуває на межі припустимої області U.

Це означає зокрема, що невеликі зміни $u(t)$ приводять до непропорційно великих змін вихідних змінних, що для соціально-економічних систем може призвести до катастрофічних наслідків. Таким чином, для нестаціонарних систем необхідні спеціальні проблемно-орієнтовані методи прийняття рішень.

Як критерій ефективності прийняття рішень виступає сформульований В.М. Глушковим принцип «своєчасності, оптимальності і комплексності рішення». Питання якості рішень, що приймаються, як складової зазначеного принципу, хоча й значною мірою опрацьовані, знаходяться у постійному розвитку і мають чимало невирішених проблем, що заслуговує окремих досліджень. Однак вони не є предметом нашого розгляду. А от безпосередньо своєчасність та оперативність інформаційної обробки потоку документів та, опосередковано, інформаційна обґрунтованість, прозорість рішень, що приймаються, опрацьовані значно менше. Тому у моделі оцінювання будемо враховувати її кількісні параметри, що пов'язані саме з оцінкою своєчасності прийняття рішення (опрацювання певного документа). Тобто визначення найкращого рішення $u^0 \in U$ будемо вважати пов'язаним із формалізацією поняття «найкраще» у сенсі «своєчасне».

Для забезпечення оптимізації моделі оцінювання необхідне застосування певних методів управління у системі. Деякі методології розв'язання проблем управління є добре опрацьованими. Так, свого часу набуло поширення *оперативне управління* (60-ті роки минулого століття), що широко застосовувалось у системах управління підприємствами [151]. Але із-за таких особливостей ОДВ як соціальної системи — консервативність, велика інерційність, необоротність деяких процесів, традиційні для технічних і технологічних систем методи — оперативне

управління, адаптивне керування — виявляються неефективними й не можуть бути застосованими в органах влади.

Наприкінці минулого століття також набув інтенсивних досліджень метод *ситуаційного управління*, що враховує поняття проблемної ситуації як сукупності станів процесів управління та оточуючого середовища у деякий момент часу. Основу ситуаційного управління становить поняття семіотичної моделі — на відміну від традиційних методів теорії управління, в основі яких знаходяться формальні моделі. Як вже вказувалося, метод ситуаційного управління достатньо опрацьований і може застосовуватись в органах влади, зокрема, для організації так званих ситуаційних центрів.

Але, згідно з [152], методу ситуаційного управління притаманні такі особливості:

1) необхідні великі витрати на створення бази даних (відомостей) щодо об'єкту управління;

2) рівень опису ситуацій має відображати усі основні параметри та зв'язки, необхідні для здійснення класифікації ситуацій;

3) мова опису повинна містити не лише кількісні параметри, а й якісні характеристики ситуацій;

4) класифікація ситуацій, а також формування кореляційних правил відбувається на суб'єктивній основі (експертами);

5) системи ситуаційного управління в принципі не можуть оптимізувати сам процес управління.

Виходячи з наведеного переліку, враховуючи особливо створення відповідної мови опису органу влади як об'єкта управління, галузевих і суспільних ситуацій, що враховувала би людські чинники, еволюцію об'єкта у часі, можна зробити висновок про існування значних проблем на шляху застосування методу ситуаційного управління в органах державної влади. Також слід зазначити, що для багатьох об'єктів однокрокові рішення не можуть визначати стратегію управління. Потрібна побудова ланцюжків однокрокових рішень, адже «проблема пошуку оптимальної узагальненої стратегії управління є основополагаючою в теорії ситуаційного управління» [150, с. 6]. Цей чинник також суттєво ускладнює застосування методу ситуаційного управління в органах влади.

Слід ще раз нагадати ті суттєві чинники, що впливають на діяльність органів влади, які були визначені на попередніх сторінках. По-перше, в сучасних умовах роль державного апарату все більше зводиться не до прямого управління галузями, а до забезпечення створення умов для їхнього вільного конкурентного розвитку, тобто до ре-

гулювання відношень у динамічному ринковому середовищі. З іншого боку проблемою, що виходить на передній план, є вичерпна інформаційна підтримка рішень в урядових структурах. Нарешті, для забезпечення прозорості в органах влади має бути налагоджено регламентовану бюрократичну роботу на базі визначених процедур, дисципліни, певних стандартів документів.

Отже, у сучасних умовах для аналізу ситуацій, підтримки прийняття рішень, оцінки їхньої ефективності, забезпечення послідовної управлінської стратегії необхідні інформаційний супровід державними експертами проблемних ситуацій у галузі, регіоні та аналіз інформації зворотного зв'язку — тобто має використовуватися накопичена в базах даних структурована аналітична інформація.

У зв'язку з цим вбачається, що при проведенні досліджень системи управління в ОДВ має застосовуватись системний підхід з використанням процедур інформаційного аналізу вхідних/вихідних інформаційних потоків із задіянням методів моделювання і порівняльного аналізу [153].

Ураховуючи, що діяльність органу влади має базуватись на технології стабілізуючого впливу на інформаційний простір власної сфери компетенції, вона, як наслідок, має містити певний «інформаційний регулятор» [154]. Як інформаційний регулятор виступає саме АІАС, що в організаційній структурі управління органу влади виконує функції центрального інформаційного вузла.

Лише із застосуванням АІАС стає можливим забезпечити циркуляційний тиск органу влади в інформаційній системі суспільства, незалежність його від суб'єктивізму влади, а також забезпечити синхронізацію інформаційного обміну. Погоджений процес інформаційної підтримки прийняття рішень дозволяє раціонально враховувати інтереси всіх учасників, зробити «людський фактор» передбачуваним і керованим за рахунок якісного опрацювання інформації зворотного зв'язку.

Для забезпечення динамічної стійкості системи державного управління стимулюючий вплив АІАС як інформаційного регулятора має сприяти боротьбі з інформаційною ентропією і дозволити розширити доступ до процесів прийняття рішень експертному співтовариству, засобам масової інформації, громадським організаціям. А перенос акценту на інформаційне забезпечення має сприяти застосуванню широкого спектра новітніх технологій і алгоритмів на аналітичній стадії підготовки рішень.

Також зазначимо, що для забезпечення визначення ситуацій, у

яких має застосовуватися механізм інформаційного регулятора, при формуванні системи треба передбачати створення деякого «вимірювача інформаційного навантаження», який діє за тріадою «оцінка – діагностування – передбачення». Дана концепція являє собою систему технологічних методів і засобів, що забезпечують на основі певної інформаційної моделі розрахунок навантаження, наприклад, якщо використовувати методи телетрафіку, за відомою формулою Ерланга, та «включення» регулятора при досягненні деяких порогових значень.

Як зазначалось, при розробці й впровадженні АІАС необхідно використовувати методологію інформаційної моделі оточуючого середовища, яка пов'язана з базовою інформацією (що має орган влади незалежно від даного процесу прийняття рішень) та поточною інформацією. Базова інформація формує «екран знань» експертів-держслужбовців, а поточна проектується на «екран знань», і для ефективного керування процесом розробки та прийняття управлінських рішень слід досліджувати зв'язок обсягу «екрану знань» (інформованості експертів з проблеми, що розглядається), продуктивності «екрану знань» (спроможностей експертів оперативно «роздобути» необхідну інформацію) з оцінкою критичності інформації, що оперативно надходить.

Тому в пов'язаних із «над навантаженням» обставинах потрібно забезпечувати найбільш повне інформування експертів, а також ефективну роботу як окремих автоматизованих робочих місць, так і усієї АІАС в цілому. Отже, поряд із запуском суспільного інформаційного регулятора, має передбачатись застосування заходів, направлених на скорочення часу на пошук експертами органу влади потрібної інформації у сховищі даних і в зовнішніх джерелах, забезпечення автоматичних публікацій з проблеми, що розглядається, на внутрішньому сайті, визначення регламентованих режимів роботи усього програмно-технічного комплексу АІАС тощо.

Проблему підвищення ефективності функціонування систем робить досить важливою й великий обсяг устаткування і програмного забезпечення, використовуваного в таких системах. Інформаційна система або її окремі частини обслуговують інформаційні потоки (документів, файлів даних і ін.), характерною рисою яких є їх безперервна зміна в часі як за обсягом, так і за напрямками. Загальне збільшення обсягів вимог на обробку потоків протягом деякого часу компенсується запасами технічних засобів (мережні засоби, обчислювальне устаткування), а надалі повинно бути враховане черговим розвитком системи, тому що структура системи та її технічні засоби в процесі функціонування сис-

теми можуть розвиватися і збільшуватися за обсягами тільки через визначені проміжки часу. Таким чином, правильно спроектована система, що щонайкраще обслуговує задані інформаційні потоки, є оптимальною лише протягом деякого, порівняно невеликого періоду часу.

Також до зменшення відповідності структури системи зміненому розподілові потоків, зниженню ефективності функціонування системи і погіршенню якості обслуговування призводить й перерозподіл потоків у межах приблизно однакових загальних обсягів, в свою чергу це приводить до проблеми відновлення відповідності між розподілом потоків і структурою системи. Таким чином, зазначені проблеми можна вирішити за рахунок уведення відповідного управління в системі.

Управління в автоматизованій системі може здійснюватися як за рахунок керування ресурсами системи (технічними і програмними засобами), так і за рахунок керування інформаційними потоками (зміна шляхів передачі й обробки практично без обмеження обсягу потоків). Можливо одночасне керування і потоками, і ресурсами.

Проблема підвищення ефективності автоматизованих систем у сфері державного управління важлива не тільки тому, що дозволяє одержати істотний економічний і політичний виграш. У деяких випадках це — єдина можливість забезпечити обробку інформації в необхідних обсягах. Тобто без забезпечення відповідного рівня ефективності побудова системи взагалі втрачає сенс. Тому методи аналізу, синтезу й оптимізації автоматизованих систем в ОДВ здобувають виняткове значення, а в зв'язку з цим і відповідні методи, що дозволяють вирішувати окремі задачі дослідження таких систем.

В основі теорії складних систем лежить низка принципів: декомпозиція, подвійність керування, ідентифікація, координація, агрегація та дезагрегація, спеціалізація, оптимізація. Складні системи типу ОДВ є практично такими, що не формалізуються, тому до них треба застосовувати метод декомпозиції на більш прості системи, які можна формалізувати. У свою чергу декомпозиція викликає необхідність координації, коли узгоджуються виходи одних підсистем із входами інших. В ОДВ глобальна задача (виконання встановленого регламенту опрацювання документів) подається послідовністю відносно незалежних задач меншої розмірності (опрацювання окремих документів чи груп документів окремими експертами), і тому необхідно здійснювати координацію (узгодження) їх розв'язань в єдину цілісну систему, спрямовану на ефективне розв'язання вихідної глобальної задачі. Така координація забезпечується в процесі реалізації управління в системі.

Необхідність управління системою (зміна структури, використання адаптивної структури, зміна напрямку передачі інформаційних потоків й ін.) ставить цілий ряд складних, специфічних задач. Більшість цих задач дотепер ще не вирішено, а частина з них навіть не сформульована належним чином. Тому доцільно вести мову скоріше про методи ***регулювання*** у системі, які пов'язані з координацією [155, 156].

Як відомо, ціль регулювання полягає у формуванні таких законів, при яких вихідні регульовані змінні мало відрізнялися б від необхідних значень. Методи регулювання в технічних системах (теорія автоматичного регулювання) пройшли значний шлях свого розвитку, починаючи від методів аналізу стійкості, якості й точності регулювання безперервних лінійних систем, аналізу дискретних і дискретно-безперервних систем, до аналізу нелінійних систем. Застосування для нелінійних систем принципів максимуму й динамічного програмування, коли визначається оптимальний з погляду заданого критерію якості закон регулювання, забезпечує верхню межу якості системи, до якої необхідно прагнути при її функціонуванні. Однак розв'язання цієї задачі для організаційних систем — таких як ОДВ — практично неможливе через складність математичного опису технологічних процесів у системі, неможливості розв'язання самої задачі оптимізації й труднощів обчислювальної реалізації, якщо нелінійний закон регулювання все ж таки знайдено.

Разом із тим, враховуючи пріоритетність інформаційного підходу та декомпозиції, розв'язання окремих задач, пов'язаних з керуванням (регулюванням) у системі, може бути проілюстровано, наприклад, методами теорії телетрафіку як складової теорії масового обслуговування, і в деяких випадках існує можливість оцінити ефект від використання того або іншого способу регулювання в системі [157].

Отже, підсумовуючи викладене, слід перш за все зазначити, що враховуючи частоту виникнення певних проблем (ситуацій) у галузі та суспільстві, які існують в інформаційному навантаженні у системі, мають формуватися пропозиції щодо перебудови структури органу влади та власне АІАС (переліку функціональних задач, складу АРМів, структури сховища даних), а також щодо реформування всієї системи державного апарату та реконфігурування інтегрованої ІАС органів влади.

З теоретичної та практичної точки зору, для забезпечення взаємодії всіх зацікавлених інтегрованих учасників у роботі органу влади у процесі підготовки прийняття рішення пріоритетною є інформаційна стадія. Таким чином, головні задачі, які необхідно розв'язувати в

органах влади і які визначають основні вимоги до регулювання в АІАС, можуть бути такими:

1) формування, структурування та переміщення інформаційних потоків по індивідуальним режимам;

2) застосування при визначенні шляхів розв'язання ситуацій з урахуванням властивостей оточуючого інформаційного середовища комплексного критерію, який враховує технологічні та організаційні можливості органу влади та АІАС;

3) встановлення та ведення виконавчого регламенту як основного документу контролю виконання доручень та інших документів.

У зв'язку з цим необхідно визначити ключові параметри АІАС як інформаційного регулятора, її функції й організаційні особливості. До цих основ повинні належати, передусім, концептуальні та інформаційні моделі АІАС, а також архітектурні рішення АІАС з підвищеною ефективністю функціонування.

Разом із тим, використовуючи інформаційний підхід для аналізу і моделювання АІАС, не слід забувати про перехід від традиційного уявлення про систему як ієрархічну організацію об'єктно-предметно об'єднаних елементів до неієрархічного середовища, певної «віртуальної реальності», який відбувається в нових умовах масового використання інформації як ресурсу [158]: «Адже інформація в комп'ютерному середовищі, що може вільно змінюватися та миттєво переміщуватися, вже більше не є об'єктом, більше не є предметом, не є відношенням, не є фактом. У цьому випадку користувач знаходиться в позиції віртуальної реальності, оскільки він спроможний не просто змінити інформацію на рівні сервера або його сторінки, але й зв'язати їх, наприклад, з іншим сервером або іншою сторінкою в іншому підрозділі установи і навіть в іншому місті країни. Він не просто змінює інформацію саму по собі, він віртуалізує її, реструктуризує в системі зв'язків установи, нарешті, він змінює й саму реальну структуру зв'язків у цій інформації».

У цьому випадку якщо традиційно реалізація системи виходить зі схеми, що містить тріаду «аналіз структури – теорія (ідея) – синтез нової структури» та завершується безпосередньо відтворенням (реалізацією) ідеальної структури в реальності, то інформаційний підхід породжує принципово іншу діяльність — віртуалізацію та передбачає віртуальний аналіз. Передусім віртуальний аналіз — це непредметний аналіз. Його напрямком дослідження виступає деяке середовище, а його головна функціональна відзнака — відсутність ідеального плану структури, відсутність чіткої ідеї. Проект системи являє собою уривковий,

фрагментарний план віртуальної і неструктурованої мети, а сама система уявляється як рухоме утворення, що змінюється кожен раз, як тільки змінюється стан інформаційного середовища.

Детальний опис функціонування динамічної системи спирається на багаторазове повторення однотипних процесів, а глобальні характеристики системи, які становлять інтерес за змістом задачі, формуються як сукупний результат на основі таких елементарних процесів.

Таким чином, не важко дійти висновку, що структура такої системи, як АІАС органу влади, не може бути визначеною однозначно й назавжди. Її лише можна подати як деяке віртуальне середовище у вигляді таких аспектно-атрибутивних переплетінь структур реальності, де уточнення чи зміна будь-якого з атрибутів або аспектів будь-якої структури реальності по атрибутивним ланцюжкам веде до миттєвого поновлення всього зведення знань. Власне з цього середовища в процесі декомпозиції можна лише виділити ряд предметів аналізу, які в реалізації набудуть вигляду реальних структур (підсистем, АРМів, задач) системи.

У зв'язку з цим важливою науковою та прикладною проблемою постає розробка концепцій, методології та методів створення АІАС на основі прогресивних інформаційно-комунікаційних технологій як ***нового класу*** складних соціотехнічних систем обробки інформації. Таким чином, автоматизована система, що реалізує в органі влади СППР, має являти собою інформаційно-аналітичну систему, яка в режимі реального часу вирішує задачі класифікації об'єктів, діагностування ситуацій, прогнозування розвитку подій, виділення закономірностей та ін. Водночас, на її виході повинна функціонувати система моделювання рішень, що здійснює вибір із множини недомінуючих рішень відповідно до множини критеріїв. Теорія свідчить про те, що на даний час ця задача є нерозв'язуваною.

3.2. Концептуальні засади формалізації та моделювання АІАС

Теорія ситуаційного регулювання. Слід ще раз звернути увагу на те, що найважливішою функцією управління в складних системах є проблема узгодження цілей, функцій, систем, елементів. Ми вже визначили її як регулювання, під яким розуміється апарат установлення законів, правил взаємодії елементів системи, які спрямовані на приведення локальних цілей окремих елементів до глобальної мети, що

стоїть перед системою в цілому, і таких, що забезпечують узгодження (координацію) їхніх дій з реалізацією цих цілей [155, 156].

Згідно з викладеним, виникає необхідність розробки нової теорії, що має забезпечити розкриття закономірностей управління в системах автоматизації функціонування органів влади, розробки принципів визначення технологічних операцій, організаційних заходів, структурних перебудов у конкретних галузевих ситуаціях в умовах послідовно-паралельного підключення різних підрозділів та експертів органів влади для вирішення проблем.

Запропоновано наступні наукові гіпотези [159]:

1) функціонування ОДВ відбувається відповідно до встановленого регламенту, який передбачає контрольні терміни виконання документів, організаційні заходи, технологічні параметри підготовки документів;

2) при виникненні проблемної ситуації необхідно оцінювати інформаційне навантаження на складові автоматизованої системи, прогнозувати його зміни, та, зіставивши з вимогами регламенту, розробляти комплекс заходів для запобігання його порушень;

3) аналіз ситуацій та пов'язаних інформаційних навантажень мають дозволяти розробляти комплекс рекомендацій щодо здійснення відповідних технологічних і структурних перебудов у складі системи.

На основі проведених досліджень, аналізу науково-технічних джерел за таку теорію запропоновано теорію ***ситуаційного регулювання (СР)*** технологічних процесів в органі влади при автоматизованій обробці інформаційних потоків.

Ідея, як основний елемент теорії, полягає в тому, що в органі влади необхідно з інформації (документів), яка постійно надходить, формувати відповідні інформаційні потоки шляхом їх структурування та переміщати між підрозділами по індивідуальним режимам. При цьому забезпечення виконання органом влади виконавчого регламенту в будь-який наперед заданий інтервал часу є синтезуючим принципом теорії, що об'єднує всі її елементи.

Суттєві стійкі чинники, що мають місце у процесі діяльності органу влади, у структурі теорії показані відповідними умовами та закономірностями. Теорія, що розглядається, базується на наступних умовах.

1. Безумовність і своєчасність виконання документів. Дія цієї умови проявляється через сувору необхідність виконання органом влади своїх функціональних обов'язків.

2. Дотримування технології обробки документів. Дія цієї умови про-

являється через необхідність виконання типових процедур, операцій, правил, визначених відповідними директивами та інструкціями.

3. Безперервність впливу інформаційних потоків. Ця умова базується на частковому об'єктивному законі безперервності функціонування державного апарату та суспільних інститутів.

4. Дискретність реалізації функцій органу влади проявляється при прийнятті рішень (опрацюванні документу).

Ідея, синтезуючий принцип та умови є ядром теорії СР. Іншими елементами, що можуть бути використані в теорії, є накопичені гіпотези, наукові та практичні дані щодо специфіки обробки інформації та її захисту в органі влади, відповідні категорії і поняття, що розкривають властивості технологічних процесів обробки інформації.

Вивчення проблеми регулювання в АІАС таких складних об'єктів, як ОДВ, необхідно проводити разом з вивченням зв'язку між поведінкою ОДВ в цілому й поведінкою окремих його елементів (підрозділів), до аналізу елементарних ефектів, що обумовлені взаємодією елементів.

Процес регулювання в АІАС може бути представлений наступними етапами.

1. Аналіз стаціонарності стану технології опрацювання документів в ОДВ. Прийняття рішення про необхідність регулювання з метою оптимізації технології.

2. Регулювання технологічної діяльності в плановану періоді. Розрахунок показників стану інформаційного навантаження, аналіз стаціонарності стану системи й активних елементів за результатами регулювання.

3. Порівняння оптимальних значень показників стану з фактичними (відрегульованими). Локалізація збуджених станів і прийняття рішень про оптимізацію технологічного процесу в ОДВ.

4. Визначення «вузьких місць» у технології опрацювання документів. Координація й оптимізація обраних технологічних процесів.

5. Прийняття рішення про створення й внесення до складу системи нових механізмів, елементів, підсистем, інформаційних технологій.

Необхідним елементом теорії є аналітичний апарат ситуаційного регулювання, що містить різні моделі, методи досліджень і реалізації функцій СР (рис. 3.6).

Головною функцією СР є ситуаційний аналіз, при якому розв'язуються такі задачі: формування класів ситуацій; віднесення поточної ситуації до одного з класів; пошук умов компенсації відхилень за заданими показниками інформаційного навантаження.

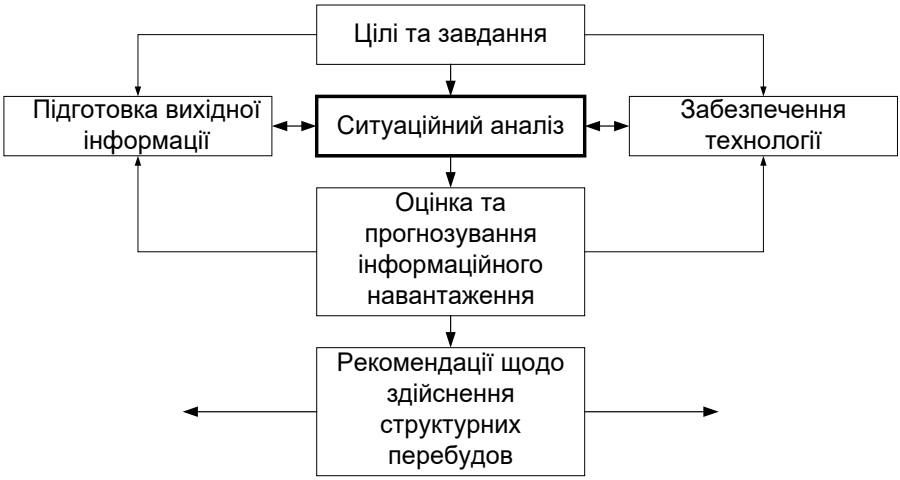

Рис. 3.6. Функції ситуаційного регулювання

Забезпечення технології — це принципи, правила, заходи, що забезпечують найефективніше сполучення елементів системи, оптимізацію їх взаємодії в часі для досягнення визначених цілей (наприклад, запобігання порушень регламенту). При цьому одним із шляхів забезпечення технології є застосування типових рішень у типових ситуаціях.

Важливим етапом є напрацювання рекомендацій з проведення структурних перебудов. Слід зазначити, що на склад апаратного та програмного забезпечення АІАС як людино-машинної системи, що будується на основі сучасних розвинутих комп'ютерних комплексів, суттєво впливає уявлення про цілеспрямовану поведінку такої системи [160].

На рис. 3.7 наведено алгоритм ситуаційного аналізу, що реалізує наведені вище функції.

При цьому на першому етапі на основі показників інформаційних потоків формується множина альтернативних виходів $Y_k = \{y_{k_i}\}, i = \overline{1,n}$, що відповідають можливим сценаріям поведінки зовнішнього середовища $w_i(t), t \in [t_0, t_k], i = \overline{1,n}$, де t_0, t_k — відповідно початковий і кінцевий моменти інтервалу прийняття рішення щодо документа. Для розв'язання цієї задачі необхідна математична модель, яка повинна містити в собі досить адекватну імітаційну модель, що дозволяє одержувати відповіді на питання типу «що буде, якщо...».

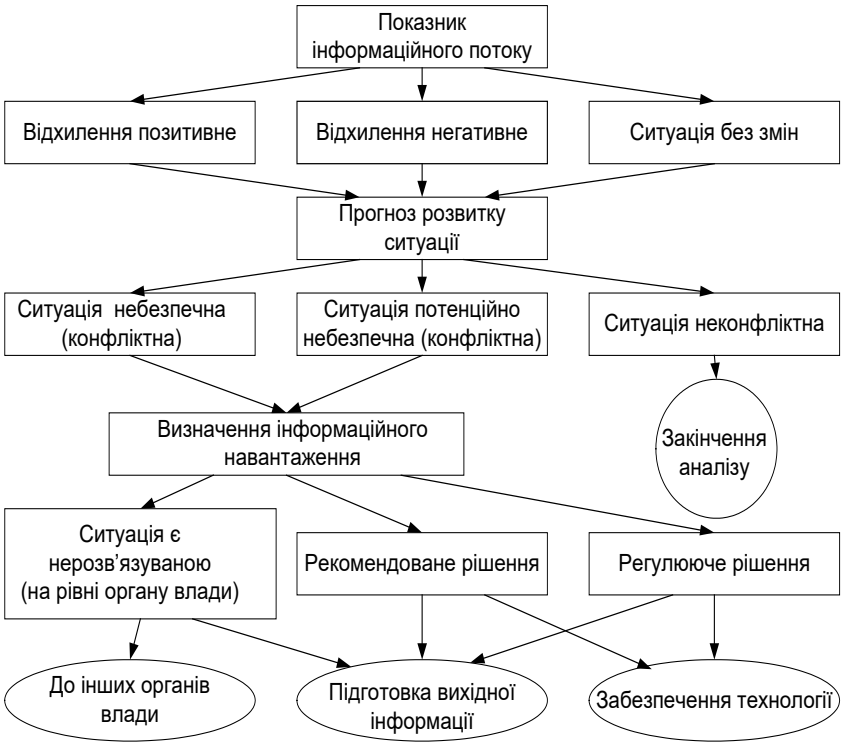

Рис. 3.7. Алгоритм ситуаційного аналізу

Крім того, будемо вважати, що цільова настанова на момент прийняття рішення t_0 є стабільною (незмінною). Це дозволяє сформулювати відповідну їй цільову функцію, що підлягає оптимізації шляхом вибору відповідних значень керованих змінних *z*. Таким чином, для кожного конкретного сценарію $w_i(t)$ на момент t_k знайдено стан z_{k_i}, що визначає екстремум цільової функції системи. У результаті буде отримана множина можливих станів системи $Z_k = [z_{k_i}], i = \overline{1,n}$.

На другому етапі вирішується завдання вибору стратегії поведінки системи $u(t_0)$, тобто в момент t_0, на основі аналізу множини можливих станів Z_k. При цьому передбачається, що на інтервалі часу $t \in [t_0, t_k]$ зміна початкового рішення $u(t_0)$ є неможливою. Наприклад, у момент t_0 приймається рішення про схвалення деякого нормативного акту. Це

рішення приймається на основі аналізу сфери дії акту (місткість ринку, ціни, податки, процентні ставки, джерела ресурсів і т.ін.). У процесі реалізації акту це рішення вже є необоротним, адже впливає на попит, ціни, ставки податків, обсяги виробництва і т.ін. Тому завдання полягає в тому, щоб у момент t_0 прийняти ефективне рішення, яке є й своєчасним.

Політика «виконавчої обов'язковості». Згідно з викладеним, вичерпна інформаційна підтримка рішень, а також забезпечення регламентованої бюрократичної роботи на базі визначених процедур і дисциплін формують основне завдання АІАС. Власне у забезпеченні прийняття ефективних рішень у визначені терміни й полягає основна функція діяльності органу влади. Тут поняття «основна функція» має, у першу чергу, подібність терміну «безвідмовність» у сенсі властивості органу влади виконувати покладені на нього функції в будь-який момент часу при заданих умовах. Водночас, ґрунтуючись на попередніх міркуваннях, вона корелюється і з поняттям інформаційної безпеки.

Таким чином, дотримуючись сформульованого В.М. Глушковим принципу «своєчасності, оптимальності і комплексності рішення», враховуючи інформаційну природу діяльності органу влади, її спрямованість передусім на «виконання документів» та велику важливість прийнятих рішень для життєдіяльності суспільства і держави в цілому, вважається за доцільне ввести поняття ***«виконавчої обов'язковості»*** органу влади. Тоді можна стверджувати, що питання ефективності АІАС (у рамках проблем, що досліджуються в даній роботі) зводиться до того, підтримує вона чи ні сформульовану в органі влади ***політику*** «виконавчої обов'язковості» (далі — ВО).

Для аналізу структури АІАС з точки зору забезпечення ВО застосуємо метод ієрархічної декомпозиції (рис. 3.8).

Особливості рівнів механізмів інформаційного забезпечення та їхньої реалізації, які дозволяють реалізувати системи підтримки політики ВО в органі влади, розглядаються на подальших сторінках. Системи підтримки політики ВО складають контроль, аудит та ін., що в принципі є достатньо дослідженими і в цій роботі не розглядаються. Політика ВО як верхній рівень ієрархії подається власними специфічними методами її формування та аналізу, які у подальшому зображені на концептуальному рівні.

Мережні методи інформаційного аналізу. Згідно з викладеним на попередніх сторінках можна припустити, що системи, подібні АІАС, мають властивості емерджентності і самоорганізації, динамічної стійкості та нелінійності взаємодії елементів. Математичний

апарат інформаційного моделювання таких систем може бути заснований на синергетичних мережних моделях (спінова модель Ізінга, нейромережна модель Хопфілда й ін.).

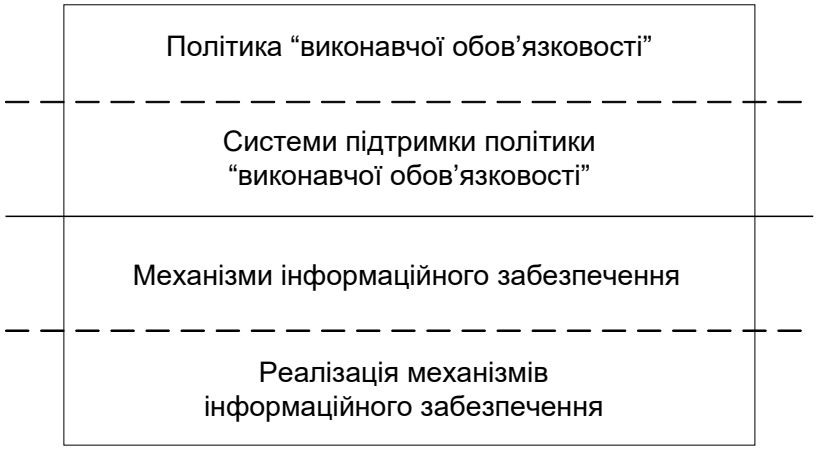

Рис. 3.8. Ієрархічна декомпозиція АІАС з точки зору забезпечення ВО

Водночас слід зазначити, що наявність в АІАС семантичної інформації потребує для перетворення даних, поданих у лінгвістичній формі, певних засобів. Зараз існує чимало теоретичних і практичних розробок з питань людино-машинних цілеспрямованих систем [161], зокрема в рамках теорії агентів і багатоагентних систем [162]. У процесах цілеполагання важливе значення мають «життєві потреби» суб’єкта дії. До таких потреб АІАС як комп’ютерної системи перш за все слід віднести потребу у ресурсах, особливо інформаційних. Введення категорії «життєві потреби» дає підставу для моделювання процесу формування головних цілей системи. При цьому досліджуються не лише ті, що спостерігаються, але й приховані властивості та відношення, інформація про які виникає не у вигляді достовірних знань, а у вигляді гіпотез. Основним методологічним прийомом в умовах, коли достовірних знань про характеристики об’єкта немає або їхнє отримання вимагає значних зусиль, є гіпотетичне моделювання [163, 164].

Застосування гіпотетичного моделювання пов’язане з процесами вибору, основу яких становлять пошукові операції. За умов значного обсягу інформації основним засобом збільшення ефективності пошуку

є використання мережних структур, зокрема нейроподібних мереж, теорія і практика яких має значний розвиток [165–167].

Так, наприклад, новою концепцією інтелектуальних систем, які самонавчаються, на основі моделювання нейрофізіологічних якостей мозку, є зростаючі пірамідальні мережі (ЗПМ). Нейроподібні мережі, що зростають, — це новий клас нейронних мереж, які являють собою динамічну структуру, що змінюється залежно від значення і часу надходження інформації на рецептори, а також попереднього стану мережі. У ній інформація про поняття, об'єкти і ситуації зовнішнього (фізичного) світу подається ансамблями збуджених нейроподібних елементів мережі і зв'язками між ними, за рахунок чого формується сукупність стійких зв'язків описуваного поняття, об'єкта чи ситуації, які забезпечують його цілісність і тотожність самому собі. Запам'ятовування описів об'єктів або ситуації супроводжується введенням у мережу нових нейроподібних елементів і зв'язків при переході якої-небудь групи рецепторів і нейроподібних елементів у стан збудження, тобто у процесі сприймання інформації і навчання мережа перебудовує свою структуру і таким чином формується внутрішній (віртуальний) світ, адекватний фізичному.

Ця концепція, яка об'єднує фізичний і віртуальний світ, має універсальний характер. Такий підхід дає нову підставу для розвитку створення інтелектуальних систем, що самонавчаються.

У зв'язку з тим, що базою моделей АІАС мають бути дві концепттуальні парадигми — інформаційної відкритості органу влади та його адаптивності, які ґрунтуються на вимогах забезпечення інформаційного обміну й інтеграції інформаційних ресурсів органів влади, визначається методологія та вирішення нової задачі побудови автоматизованих систем управління — створення комплексної компонентної моделі формалізації процесів державного управління на базі моделі інформаційних процесів, формалізмів подання процесів функціонування АІАС та інформаційних процесів, організації інформаційної взаємодії компонентів в умовах реального середовища [168].

Як відомо, концептуальне проектування за допомогою логічного апарату дозволяє формалізувати опис предметної області будь-якої складності. Найбільш значними вимогами стають мобільність цієї моделі, яка дозволяла б швидко «перебудовувати ряди» і коригувати установки в процесі прогнозування та оцінки ризику на етапі прийняття рішень.

Концептуальне проектування має базуватися на новому підході до розв'язання проблем управління — на інформаційній основі, яка враховує сучасне уявлення про інформацію як про інтелектуальний продукт — знання як ресурс суспільства [169].

«Знання — це інформація про процеси рішення, логічний вивід, закономірності, в результаті застосування якої до даних породжується нова інформація» [170, с. 62]. Характерна особливість знань полягає у тому, що вони є узагальненою інформацією, яка відображає досвід розв'язання задач. Методологія формування знань отримує розвиток у рамках різних наукових напрямків. Один з них, що розповсюджується останнім часом, є інтелектуальний аналіз даних, який передбачає технологію «виділення знань» і «видобування знань», що позначають методи знаходження залежностей між даними, які зберігаються в базах даних (Data Mining and Knowledge Discovery in Data Bases).

Одним з видів закономірностей, властивих даним, що власне й складають знання, є закономірності, що характеризують множину (класи) об'єктів. Термін «об'єкт» у нашому випадку відповідає такому елементу матеріального світу як реалізація інформаційного процесу. Об'єкт подається набором ознак.

Знання про класи об'єктів мають форму понять. У системі знань поняття відіграють роль базових елементів, з яких складаються певні логічні форми. Отже, поняття є узагальненою моделлю деякого класу об'єктів, за допомогою якої реалізуються процеси розпізнавання і генерування моделей конкретних об'єктів цього класу.

Методи виділення знань, в яких при аналізі кожного об'єкта навчаючої вибірки усі пошукові операції здійснюються в межах оточення цього об'єкта, мають назву локально-статистичних. До них відносяться й методи формування понять на основі пірамідальних мереж [171].

Отже, тенденцією у розвитку інформаційних систем, що превалює, є використання природних, властивих людині принципів моделювання середовищ, ситуацій, задач. У життєдіяльності людини велике значення мають логіко-лінгвістичні інформаційні моделі (ЛЛМ), тобто такі моделі, основними елементами яких є не числа та обчислювальні операції, а імена й логічні зв'язки. ЛЛМ адекватно описуються природно-мовними конструкціями, і це становить їхню перевагу при організації людино-машинної взаємодії [150, 164, 171, 172]. До речі, одним з перших випадків практичного використання ЛЛМ стало ситуаційне управління.

Приведеним вище вимогам також задовольняють з*ростаючі піра-мідальні мережі (ЗПМ)*, що реалізують гіпотезу про закономірності

структурування інформації при її сприйнятті та відповідні ЛЛМ. Теорія і практичне застосування ЗПМ наведені в багатьох публікаціях [164, 170, 171, 173, 174].

У пірамідальній мережі можуть бути подані ознакові описи об'єктів і семантичні відношення. Пірамідальні мережі зручні для виконання різних операцій асоціативного пошуку за загальними елементами їхніх описів. Численне застосування цих методів, зокрема для прогнозування нових хімічних сполук і матеріалів, діагностування хвороб вітчизняними та закордонними вченими та фахівцями вважаються досить ефективними.

Методологія ЗПМ призначена для розв'язання задач виділення закономірностей, класифікації, діагностики і прогнозування.

Метапроцедури аналізу на основі ЗПМ реалізовані у системі виводу і аналізу закономірностей *CONFOR*, розробленої в Інституті кібернетики ім. В.М. Глушкова НАН України, в основу якої покладений оригінальний метод індуктивного формування понять (CONcept FORmation) [174]. Вихідними даними для системи *CONFOR* є описи досліджуваного класу об'єктів, які задано наборами значень ознак.

Закономірності подаються у вигляді логічного виразу в термінах вихідних значень ознак, у наслідок чого результати обчислень системи *CONFOR* є наочними та легко інтерпретуються.

Характерними задачами для *CONFOR* є вивід закономірностей, що характеризують процеси прибуткового інвестування, розвитку регіону, класифікація економічних ситуацій тощо.

Згідно з викладеним, застосування методології ЗПМ є перспективним для використання при проведенні аналітичних досліджень в АІАС, для забезпечення класифікації ситуацій, а також для реалізації системного аналізу самої АІАС під час її проектування.

Модель інформаційно-аналітичної діяльності в органі влади. Інформаційно-аналітична діяльність в органі державної влади визначається, перш за все, його функціональними обов'язками, що задаються відповідним положенням про орган влади. Враховуючи проведений аналіз, результати якого наведені у розділі 2, орган влади має певну множину функцій $F = \{ F_i \}$, $F \neq \varnothing$.

Тут слід згадати специфіку та проблеми, які, як вказувалось, притаманні інформаційно-аналітичній діяльності в органі державної влади. Мова йде про два об'єктивних чинники. По-перше, це обмеження реального часу, протягом якого повинні бути прийняті управлінські рішення, що стає все більше критичним у сучасних умовах інтенсифікації

і прискорення управлінських процесів.

Другий чинник — це багатокритеріальність при прийнятті управлінських рішень, формальна невизначеність функцій, їх неоднозначність, постійне ускладнення функціональних завдань, пов'язане з суперечливістю, що виникає при спробі врахування інтересів усіх основних економічних суб'єктів, діяльність яких або певна складова майна перебувають у сфері впливу органу влади, що в кінцевому випадку призводить до збільшення кількості критеріїв оптимальності рішень, які приймаються.

Нарешті, орган державної влади знаходиться під постійним впливом інших ОДВ, не лише вищих, а й «сусідніх», бо, згідно з існуючим положенням, кожен орган влади має право направити звернення безпосередньо в інший орган або у вищий рівень з пропозицією надати відповідні доручення визначеним органам влади. Така практика створює непередбачувальне інформаційне середовище, яке формується на основі ймовірнісних законів, що не дозволяє планувати інформаційно-аналітичну діяльність в органі влади, оптимізувати використання висококваліфікованих фахівців і експертів та наявного парку програмно-технічних засобів.

Отже, згідно з описом (3.8), враховуючи певні групи функцій з множини F, модель інформаційно-аналітичної діяльності в органі влади можна визначити за допомогою таблиці основних напрямків цієї діяльності (табл. 3.1), у останній графі якої приведені позначення інформаційних потоків, що є визначальними для забезпечення напрямків діяльності.

Таблиця 3.1. Основні напрямки
інформаційно-аналітичної діяльності в органі влади

Напрямки			**В умовах функціонування АІАС**
№	**Назва**	**Мета**	
1	2	3	4
1.	Збір і первинне опрацювання інформації	Формування структурованих інформаційних ресурсів для інформаційно-аналітичної діяльності. Забезпечення постійного уточнення і розширення інформаційної бази для прийняття рішень	Основними джерелами є звітність суб'єктів економічної діяльності, підприємств із сфери управління ($C_{вх}$, $N'_{вх}$, $P'_{вх}$), які мають надходити засобами телекомунікацій

Продовження табл. 3.1

1	2	3	4
2.	Ведення і поповнення аналітичної інформації	Забезпечення вичерпної інформаційної підтримки прийняття рішень	Оперативні повідомлення засобів масової інформації, результати аналітичних досліджень (I', G'), що доступні завдяки Інтернету
3.	Документообіг	Забезпечення ефективності системи керування	Починається з впровадження електронної системи обліку з переходом до ведення бази даних образів документів і їх повних текстів (E, $B_{вх}$, $B_{вих}$, $O_{вх}$, $O_{вих}$)
4.	Розв'язання функціональних задач	Забезпечення виконання безпосередніх функціональних обов'язків	Впровадження різних функціональних ІАС, підсистем та задач ($B_{вх}$, $B_{вих}$, $O_{вх}$, $O_{вих}$, $C_{вх}$, $C_{вих}$)
5.	Моніторинг	Досягнення найбільш об'єктивного відображення стану справ у різних суспільних сферах	Дослідження стану зовнішнього середовища за допомогою автоматизованих засобів і технологій (G', I', $M'_{вх}$, $M'_{вих}$)
6.	Прогнозно-аналітична діяльність	Випереджаюче планування роботи органа влади	Одержання узагальненої і прогнозної інформації із застосуванням аналітичних програмних засобів (A)
7.	Моделювання	Формалізація відношень суб'єктів керування, зняття неузгодженості документів різної підпорядкованості, забезпечення узгодженості при підготовці і прийнятті рішень на різних рівнях керування в органі влади	Забезпечення єдиного поля управлінської діяльності на базі застосування програмно-інформаційного моделювання й автоматичного генерування пакетів документів і документних баз (D)
8.	Проведення соціологічних досліджень	Одержання додаткової інформації і її використання при прийнятті рішень	З використанням електронних способів інформування і широкого доступу до Інтернету ($P'_{вх}$, $N'_{вх}$)

Продовження табл. 3.1

9.	Захист інформації	Забезпечення інформаційної безпеки	Комплексне забезпечення інформаційної безпеки з застосуванням системи програмно-технічних заходів ($W'_з$, $W'_{вн}$, Z)
10.	Відкритість державного управління	Рішення питань прозорості керування державою	Залучення широких кіл громадськості до деяких видів діяльності державних установ шляхом електронних голосувань, опитувань тощо у формі «електронного урядування» та «електронної демократії» (G', I', $P'_{вх}$, $N'_{вх}$)
11.	Проведення фундаментальних досліджень	Створення інформаційних та аналітичних моделей діяльності органа влади	На базі автоматизації інформаційно-аналітичної діяльності (A, D)

3.3. Визначення та аналіз інформаційних потоків в АІАС

Моделі інформаційних потоків. Як було вище зазначено, при проведенні досліджень такої системи як АІАС має застосовуватись системний підхід з використанням інформаційного аналізу вхідних/вихідних інформаційних потоків і процесів обробки інформації. У загальному випадку цей аналіз спирається на теорію інформації, математичну теорію зв'язку та теорію масового обслуговування (теорію телетрафіку). Ці наукові напрямки є значною мірою опрацьованими та практично апробованими [157]. Водночас до цих основ слід віднести й теоретичні роботи з питань інформаційної безпеки, що значною мірою також базуються на дослідженнях з указаних наукових напрямків [175].

Таким чином, будемо вважати за можливе для розгляду питання інформаційного аналізу АІАС застосувати інтерпретацію основних положень вищезгаданих теорій і методів, ураховуючи специфіку діяльності органів влади та завдань їхньої АІАС.

Перш за все, визначимо, що інформаційні потоки в органах влади є ***потоками документів***. Тобто відправним пунктом усіх подальших ви-

кладок будемо вважати поняття «документ».

Документом (у загальному випадку) є матеріальний носій із зафіксованою на ньому інформацією, яка може бути передана в просторі та/або часі. Будемо вважати, що документ — це первинне поняття, що не має формального визначення, яке б не зводилось до використання синонімів.

Вочевидь, множина документів є ***кореспонденцією***, тобто кореспонденція — це множина повідомлень, які надходять до ОДВ, виходять з нього, або циркулюють в ньому за правилами документообігу.

Документи відповідно до тих чи інших своїх ознак можуть бути згруповані в певні підмножини. У загальному випадку такими специфічними ознаками є відповідні номер і дата видання. Зазвичай, до пари елементів {номер, дата} додають елемент «категорія», який може, наприклад, визначати вид документа («постанова», «наказ», «розпорядження» і т.ін.) або його спрямованість («вхідний», «вихідний», «внутрішній»). Трійка елементів {номер, дата, категорія} однозначно визначають будь-який документ в органі державної влади. Для загальності будемо вважати, що у випадках, коли регламентами діловодства не передбачено визначення категорії документа, він має категорію «без визначення».

Отже, документ — це будь-яке повідомлення, якому відповідно до визначених правил (зазвичай, це правила документообігу) присвоєно ідентифікатор у вигляді трійки {номер, дата, категорія}.

Ці ж правила регламентують, що кожен документ може мати лише один ідентифікатор; і жоден ідентифікатор не може бути присвоєний більше, ніж одному документу.

Дамо ще деякі визначення. Обробка кореспонденції — це процедура, яка полягає в наданні (або ненаданні) кожному з повідомлень кореспонденції статусу документа, тобто в присвоєнні (або у відмові від присвоєння) кожному повідомленню відповідного ідентифікатора у вигляді трійки {номер, дата, категорія} згідно з правилами документообігу.

Потік документів — це послідовність документів, яка сформована в результаті виконання процедури обробки кореспонденції над вхідними повідомленнями.

Для цілей даного дослідження будемо вважати, що формування потоку документів в ОДВ здійснюється спеціальним підрозділом — органом первинної обробки кореспонденції (ОПОК), яким виступає, наприклад, канцелярія.

Формально основними функціональними компонентами документообігу в органі влади, які забезпечує ОПОК, є:

- реєстрація кореспонденції (вхідні, вихідні, внутрішні);
- маршрутизація документів;
- контроль виконання документів і доручень;
- архівація документів.

Одначе функціональне наповнення поняття «документообіг», що відбувається за участю ОПОК, зазвичай значно ширше і містить такі процедури, як узгодження й затвердження загальнорозпорядчих документів, підтримка регламентів управлінських процедур, оформлення відряджень, доручень, перепусток та ін.

Але фактично до документообігу має відношення більшість підрозділів і співробітників при виконанні службових обов'язків, при цьому документ в ОДВ проходить значну кількість інстанцій (рис. 3.9), обростаючи резолюціями та підписами. Усе це формує певну специфіку документообігу в органі влади, а саме:

- множина контурів документообігу (процесів), у яких бере участь майже кожний співробітник;
- різні ролі співробітника в різних екземплярах процесу;
- нерегулярність участі в процесах;
- змінюваність процесів;
- державна важливість інформації, що накопичується в документах;
- специфічність процесів для кожного конкретного ОДВ.

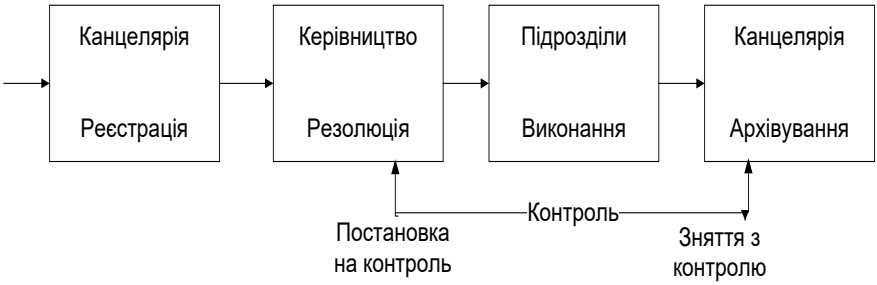

Рис. 3.9. Процес обробки вхідних документів в органі влади

Модель формування потоку документів може бути сформованою у вигляді системи масового обслуговування. Загальні риси цієї моделі такі.

По-перше, потік надходження кореспонденції є, в загальному випадку, випадковим потоком. Як наслідок, потік документів на виході також є випадковим.

По-друге, відзначимо, що обробка кореспонденції в ОПОК ведеться за відповідною дисципліною обслуговування (як правило, це дисципліна з визначеними пріоритетами). Внаслідок додержання цієї дисципліни потік документів на виході ОПОК вибудовується в послідовність, яка в подальшому може оброблюватись, переважно, за дисципліною FIFO (перший на вході — перший на обслуговуванні).

По-третє, будь-які канали, якими документи надходять з ОПОК на опрацювання до експертів, принципово мають обмеження щодо пропускної здатності, остільки «множину експертів» можна розглядати як джерело скінченної продуктивності.

По-четверте, «множина експертів» потребує визначеного часу на обробку кожного документа і може обмежувати власною продуктивністю потік документів на своєму виході.

Побудова конкретної моделі цієї системи у вигляді системи масового обслуговування може бути реалізована відомими методами. Тому ідея побудувати і модель АІАС у вигляді системи масового обслуговування видається привабливою. Однак така модель або має бути вкрай вихолощеною для того, щоб її можна було реалізувати, або виявляється занадто складною навіть на рівні формування вихідних умов.

Для наближення до розв'язання задачі сформуємо ряд вихідних положень.

Кількість документів, які може одержати ОДВ реальними каналами зв'язку будь-якого скінченного відрізку часу, є скінченною множиною. Це твердження є наслідком обмеженої пропускної здатності реальних каналів. Продуктивність системи опрацювання документів в ОДВ не перевищує продуктивності його ОПОК. Це твердження є наслідком того, що ОПОК виступає єдиним каналом для системи опрацювання документів в ОДВ. З цього отримуємо висновок: щоб уникнути втрат документів на вході ОДВ, продуктивність ОПОК має бути не нижчою, ніж продуктивність джерел вхідних документів.

Також є очевидним, що множина всіх документів, якими оперує ОДВ, є скінченною множиною. Як визначено, документом визнається повідомлення, якому поставлено у взаємно однозначну відповідність ідентифікатор — трійку елементів {номер, дата, категорія}. Це означає, що з точки зору множин множина ідентифікаторів і множина документів є еквівалентними. Тому будемо оперувати ідентифікаторами. Кожен

ідентифікатор складається з трьох елементів: номера, дати і категорії. Згідно з практикою діловодства, можна стверджувати, що множина категорій документів є скінченною множиною. Спираючись на те, що дати документів не можуть перевищувати поточну календарну дату, яка є скінченною величиною, робиться висновок, що множина дат у нашому випадку є також скінченною множиною. А це обумовлює, що множина документів, які може отримати ОДВ за одну добу, є скінченною множиною.

Таким чином, усі складові ідентифікатора документа є елементами скінчених множин. Отже ідентифікатор є також елементом скінченної множини. Оскільки між ідентифікаторами і документами існує взаємно однозначний зв'язок за визначенням, то й множина документів є скінченною множиною.

Нехай **D** — скінченна множина видів документів, D — підмножина документів певного виду з множини **D**, будь-яка інформація (повідомлення) подається у вигляді документа d, $d \subset D$.

Довільну скінченну підмножину документів певного виду D_i з множини **D** будемо називати *об'єктом O*.

Будь-яку сутність, яка здійснює відображення об'єкта D_i в документ $d_{k,j}$, будемо називати *виконанням документа*. При цьому результуючий документ $d_{k,j}$ може належати як підмножині D_i, так і деякій іншій підмножині D_k множини **D.**

Кожне виконання документа може: а) зберігатися; б) діяти. У випадку а) мова йде про збереження загального опису (процедури, алгоритму) виконання документа за допомогою ресурсів деякої системи. У цьому випадку виконання документа нічим не відрізняється від інших даних. У випадку б) мова йде про активовану програму взаємодії конкретного об'єкта з ресурсами системи, наслідком чого є визначення конкретного кінцевого документа.

Обсяг ресурсів системи, що виділяються для виконання документа, будемо називати *домен* і позначати символом Δ. Для виконання документа крім виділення домену необхідно забезпечити цей обсяг ресурсів системи особливим статусом, при якому вони будуть здійснювати перетворення даного об'єкта. Цей статус будемо визначати терміном *керування*.

Стан системи, при якому визначений її домен діє з визначеним керуванням, будемо називати *процес* і позначати символом *P*. Тобто, процес — це пара (домен, керування).

Сутність, що являє собою виконання документа у визначеному процесі, будемо називати *суб'єктом виконання S*. Тобто суб'єкт виконання — це пара (об'єкт, процес).

Вочевидь, для виконання документа суб'єкт використовує інформацію, що міститься в об'єкті *O*, тобто здійснює доступ до об'єкта *O* .

Однією з концептуальних засад АІАС є забезпечення «виконавчої обов'язковості» (ВО). При розгляді цих питань приймемо наступну, широко відому аксіому: всі питання забезпечення ВО описуються доступами суб'єктів до об'єктів. Існує безліч різних видів доступів (на запис, читання та ін). Множину можливих доступів у системі будемо позначати *R*.

Якщо розглядати множину об'єктів і послідовності доступів, то її можна подати орієнтованим графом, вершинами якого є множина об'єктів. Позначимо через $\Psi = \{\boldsymbol{G}\}$ множину можливих графів доступів. Тоді Ψ можна розглядати як інформаційний простір системи, а траєкторія в просторі Ψ відповідає функціонуванню автоматизованої системи.

У цих термінах зручно уявляти задачу забезпечення ВО в наступному загальному вигляді. В інформаційному просторі Ψ визначені можливі траєкторії Φ, у Φ виділена деяка підмножина *N* несприятливих траєкторій або ділянок таких траєкторій, яких треба уникнути. Задача забезпечення ВО полягає у тому, щоб будь-яка реальна траєкторія процесу обробки інформації в інформаційному просторі Ψ не потрапила в множину *N*. Як правило, у будь-якій конкретній автоматизованій системі можна наділити реальним змістом компоненти моделі Ψ, Φ і *N*. Наприклад, несприятливими можуть бути траєкторії, що проходять через дану множину таких станів $\Psi' \subseteq \Psi$, які призводять до обмеження доступу конкретних суб'єктів до конкретних об'єктів, що створює перешкоди для виконання регламенту обробки документів.

Таким чином, адміністратор системи, щоб траєкторії процесу обробки не вийшли в *N*, може керувати тільки зняттям обмеження на доступ у кожен момент часу. Зрозуміло, ці обмеження можуть залежати від усієї передісторії процесу. Однак, у будь-якому випадку системі доступний тільки локальний вплив. Основна складність забезпечення ВО полягає в тому, що маючи можливість використовувати набір локальних впливів на зняття обмежень на доступ у кожен момент часу, необхідно вирішувати глобальну проблему недопущення виходу будь-якої можливої траєкторії в несприятливу множину *N*.

Розглядаючи інформаційні потоки, коли об'єкт O або суб'єкт S є або джерелом, або одержувачем інформації, можна говорити про *передачу інформації*, що дозволяє реалізувати потік через канал.

З погляду забезпечення ВО канали можуть бути завантаженими (частково завантаженими) або перезавантаженими. Перезавантажені канали створюють умови обмеженості щодо доступу до інформації і тим самим можуть порушувати ВО.

Розглядаючи канали передачі інформаційних потоків, можна залучити теорію інформації для обчислення кількості інформації в потоці і пропускної здатності каналу. Якщо перезавантажений канал не можна цілком розвантажити, то частка кількості інформації в об'єкті, що недоступна по цьому каналу, служить мірою небезпеки забезпечення ВО цього каналу. В оцінках якості доступу до інформації можна використовувати граничне (порогове) значення для припустимої пропускної здатності каналів.

Величини інформаційних потоків можна визначати за допомогою теоретико-інформаційних понять.

У загальному вигляді для об'єктів X у стані s і Y у стані s' визначимо інформаційний потік, що викликає перетворення. Припустимо, що стан X і стан Y — випадкові величини зі спільним розподілом $P(x, y) = P(X = x, Y = y)$, де під $\{X = x\}$ розуміється подія; що стан об'єкта X дорівнює значенню x (аналогічно в інших випадках). Тоді можна визначити: $P(x)$, $P(y/x)$, $P(x/y)$, ентропію $H(X)$, умовну ентропію $H(X/Y)$ і середню взаємну інформацію:

$$I(X, Y) = H(X) - H(X/Y). \tag{3.9}$$

Інформаційний потік від X до Y (позначення $X \to \alpha Y$) викликає виконання деякої команди α у стані s, що переводить стан s у s', якщо $I(X, Y) > 0$. Величина $I(X, Y)$ є величиною потоку інформації від X до Y.

Для об'єктів X і Y існує інформаційний потік величини C (документів), якщо існують стани s, s' і послідовність команд α такі, що $s|\to s'(\alpha)$, $X \to \alpha Y$.

Оцінка максимального інформаційного потоку визначається пропускною здатністю каналу $X \to \alpha Y$ і дорівнює за величиною

$$C(\alpha, X, Y) = \max_{P(x)} I(X, Y). \tag{3.10}$$

Аналіз інформаційних потоків в АІАС. Базовою основою аналізу процесів обробки інформації є структури (моделі) ін формаційних потоків. Такі моделі на стадії проектування можна використовувати для класифікації АІАС з урахуванням інформаційної взаємодії основних структурних елементів органів влади, а також для проведення аналітичних досліджень у процесі функціонування системи.

Як раніше зазначалося, для аналізу інформаційних потоків, що циркулюють в органах державної влади, доцільно використовувати методологію зростаючих пірамідальних мереж (ЗПМ). При побудові пірамідальної мережі відбувається класифікація об'єктів, що має велике значення для автоматизації процесів моделювання середовищ і ситуацій. Це важливо для використання в АІАС, якщо об'єктами є інформаційні потоки, визначальні для забезпечення діяльності органа влади.

Пірамідальною мережею є ациклічний орієнтований граф, який не містить вершин, що мають одну дугу, яка заходить. Вершини, що не мають дуг, які заходять, називаються рецепторами, інші — концепторами. Рецептори відповідають значенням ***ознак об'єктів***. Концептори відповідають ***описам об'єктів***, а також перетинанням цих описів. Тобто концептори відповідають сполученням значень ознак, що визначають кон'юктивні класи об'єктів. Формування концепторів відбувається у результаті роботи алгоритму побудови пірамідальної мережі [164].

Із сполучення ознак, виділених на першому етапі — побудові мережі, на другому етапі формується логічна структура понять. Це відбувається за певними алгоритмами на основі визначених правил. Обчислення значення логічного виразу поняття дозволяє розпізнавати об'єкти. Змінним, що відповідають значенням ознак, які належать об'єкту, що розпізнається, присвоюється значення 1, іншим — 0. Одиничне значення всього виразу означає, що об'єкт входить в об'єм поняття.

Для проведення моделювання використовується режим навчання, у якому вихідними даними є об'єкти навчальної вибірки, що належать як досліджуваному класу, так і іншим класам. Об'єкти навчальної вибірки подаються ознаковими описами, тобто наборами значень ознак.

У [176] проведено моделювання та побудову ЗПМ з використанням системи *CONFOR*, де об'єктами навчальної вибірки є інформаційні потоки, визначальні для забезпечення діяльності органа влади, а набори значень ознак підготовлені на підставі усереднення проведених обстежень органів влади. За класи об'єктів прийнято: 1 — вхідні/вихідні потоки, загальні для всіх органів влади, 2 — вхідні/вихідні потоки, індивідуальні для обраного органа влади, 3 — внутрішні інформаційні потоки.

Після того, як мережу побудовано, виконується процес формування понять. Поняття — це елементи системи знань, що представляють собою узагальнену логічну ознакову модель класу об'єктів, за допомогою якої реалізуються процеси розпізнавання й генерації моделей конкретних об'єктів.

Поняття подається в мережі ансамблем спеціально виділених вершин, що відповідають найбільш істотним сполученням значень ознак. Наприклад, червоні вершини відповідають класу 1, сині — класу 2 і зелені — класу 3.

Таким чином, результатом роботи системи *CONFOR* у режимі навчання є узагальнена модель досліджуваного класу об'єктів, що містить найхарактерніші властивості цих об'єктів. Закономірність може бути подана у вигляді логічного виразу, що є більш наочним для користувача і легко інтерпретується.

Логічні вирази, що визначають різні класи об'єктів, об'єднуються в кластерні бази даних (КБД). КБД містять інформацію про групи об'єктів (кластери), специфічні для досліджуваної предметної області. На основі КБД розв'язуються задачі класифікації, діагностики і прогнозування.

Важливою особливістю методу формування понять у пірамідальних мережах є можливість введення в поняття так званих виключаючих ознак, що не належать об'єктам досліджуваного класу. У результаті сформовані поняття мають більш компактну логічну структуру, що в принципі дає можливість збільшити точність діагнозу або прогнозу. У логічних виразах виключаючі ознаки подаються змінними з запереченням.

У [176] у результаті моделювання отримані логічні вирази для трьох класів об'єктів. Отже, об'єкти класу 1 характеризуються інтенсивністю в основному 500 документів/рік, або середнім ступенем важливості інформації, або низкою оперативністю з інтенсивністю 500 документів/рік та середнім рівнем розгляду інформації, або з використанням форми взаємодії у вигляді форумів з середнім ступенем важливості інформації та середнім рівнем розгляду інформації.

Одиночні об'єкти класу 1 характеризуються інтенсивністю в 1000 документів/рік, середнім ступенем важливості інформації, середнім рівнем розгляду інформації, середньою оперативністю, опрацюванням пропозицій, щоденною періодичністю та відсутністю необхідності втручання вищого керівництва органу влади.

Об'єкти класу 2 характеризуються: використанням форми взаємодії у вигляді нарад; або неперіодичною формою появи потоку, низькою

оперативністю, використанням форми взаємодії у вигляді нарад, низьким ступенем важливості інформації та відсутністю необхідності втручання вищого керівництва органу влади; або середньою оперативністю з рівнем розгляду інформації вищим керівництвом, формою надання інформації у вигляді листування, щоденною періодичністю, формою взаємодії у вигляді нарад, середнім ступенем важливості інформації та вибірковим втручання вищого керівництва органу влади.

Одиночні об'єкти класу 2 характеризуються середнім рівнем розгляду інформації, низькою оперативністю, неперіодичним листуванням, додатковою формою взаємодії у вигляді нарад, низьким ступенем важливості інформації, відсутністю необхідності втручання вищого керівництва органу влади та інтенсивністю в 500 документів/рік.

Об'єкти класу 3 характеризуються середнім рівнем розгляду інформації, або низькою оперативністю, або формою надання інформації у вигляді звітів з середнім ступенем важливості інформації, середнім рівнем розгляду інформації, вибірковим втручання вищого керівництва органу влади, низькою оперативністю та додатковою формою взаємодії у вигляді нарад.

При цьому одиночні об'єкти класу 3 характеризуються інтенсивністю до 3000 документів/рік, листуванням з низьким ступенем важливості інформації, відсутністю необхідності втручання вищого керівництва органу влади, з рівнем розгляду інформації тільки фахівцями низького рівня, щоденною періодичністю та низькою оперативністю.

Методологія ЗПМ також може бути застосована для ситуаційного аналізу реалізації ситуаційного регулювання технологічних процесів при автоматизованій обробці інформаційних потоків. Для цього перш за все необхідно підготувати набор значень ознак типових ситуацій та провести їх класифікацію. У процесі функціонування системи має бути реалізоване діагностування ситуацій та прогнозування інформаційного навантаження від їхнього розвитку.

Принциповою відмінністю запропонованого підходу від наявних є те, що він враховує сучасні тенденції в перебудові системи державного управління і відношень суспільства і держстуктур, які мають визначальний вплив на функціонування органів влади. Але це обумовлює й потребу в проведенні додаткових досліджень, адже увесь комплекс вирішення проблем моделювання АІАС на даному етапі окреслити неможливо.

Моделі цінності інформації. Щоб забезпечити обробку інформаційних потоків (документів) з оглядом на забезпечення ВО, треба

затратити сили, засоби і ресурси, а для цього необхідно знати, до яких витрат це призведе. Вочевидь, що витрати на забезпечення ВО не повинні перевищувати можливі (встановлені). Для розв'язання цих задач зазвичай уводяться допоміжні структури — цінність інформації. Відомо декілька таких моделей. Проведемо інтерпретацію деяких з них для випадку забезпечення ВО.

Адитивна модель. Одним з видів витрат є грошові. Зрозуміло, що в грошовому виразі витрати не повинні перевищувати встановлених значень. Але не завжди можливо і потрібно давати грошову оцінку інформації. Зокрема, оцінка інформації в державних структурах (політичної інформації, військової та ін.) в грошовому виразі є незрозумілою.

Аналіз ризику. У цій моделі можливості загроз оцінюються ймовірностями відповідних подій, а втрати підраховуються як сума математичних очікувань утрат для компонентів по розподілу можливих загроз.

Порядкова шкала цінностей. Цю модель доцільно використовувати при оцінці інформації в державних структурах. Наприклад, усі об'єкти (документи) державної установи розбиваються за грифами таємності. Самі грифи таємності утворюють таку порядкову шкалу: <нетаємно> <для службового користування> <таємно> <абсолютно таємно>. Або об'єкти класифікуються за такою шкалою: <звернення громадян> <листи органів влади> <доручення Кабінету Міністрів> <запити народних депутатів> <доручення Президента>. Більш високий клас має більш високу цінність і тому вимоги щодо забезпечення його ВО є вищими.

Якщо інформація має цінність, то необхідно визначити, в якому сенсі на цю цінність необхідно орієнтуватись і які загрози ВО враховувати. Якщо, з точки зору забезпечення ВО, цінність інформації полягає в оперативності (терміновості) її використання, то можна стверджувати, що може мати місце небезпека порушення доступності інформації.

До механізмів контролю і забезпечення доступності інформації варто віднести створення системної надмірності. Такі міри відносяться до заходів з підвищення «живучості»системи.

Вимоги до систем забезпечення політики ВО. Рішення щодо забезпечення ВО є багатоальтернативним і найчастіше існування загальноприйнятого розуміння оптимальності довести не вдається. Результатом розв'язання таких задач є вибір правил розподілу і збереження інформації, а також поводження з інформацією. За відомою аналогією це можна назвати ***політикою забезпечення ВО***.

Політика забезпечення ВО (ПЗВО) — це набір норм, правил і

практичних прийомів, що регулюють керування, збереження і розподіл цінної інформації.

Дотримання цієї політики має забезпечити досягнення того компромісу між альтернативами, який вибрали керівники органу влади при затвердженні політики щодо цінної інформації для забезпечення її своєчасного використання та обробки. У той же час вибір політики забезпечення ВО — це остаточне рішення проблеми стосовно того, що «добре» і що «погано» в поводженні з цінною інформацією. Після прийняття такого рішення можна будувати систему підтримки виконання правил політики забезпечення ВО. Таким чином, побудована система обробки інформації є гарною, якщо вона надійно підтримує виконання правил політики забезпечення ВО, і, навпаки, є поганою, якщо вона ненадійно підтримує цю політику.

Як було зазначено, формалізовано система обробки інформації може перебувати в одному зі станів $S_i \in S, i = \overline{1,\ell}$, де S — множина всіх можливих станів. Враховуючи можливі негативні наслідки від того, що певні стани системи можуть вплинути на забезпечення ВО, всю множину S подамо як об'єднання чотирьох підмножин станів або зон ризику, а саме:

1) безризикова зона — область, у якій негативні наслідки не очікуються. Цій зоні відповідають стани своєчасного опрацювання документів $S_i \in S_1$;

2) зона припустимого ризику — область, у якій затримання з опрацюванням документа зберігає свою доцільність, негативні наслідки можуть мати місце, але вони менше очікуваного позитиву від прийняття рішення. Цій зоні відповідають стани $S_i \in S_2$;

3) зона критичного ризику — область, що характеризується можливістю негативних наслідків, які перевищують значення очікуваного ефекту від прийняття рішення. Критичний ризик призводить до визначення відповідального працівника (експерта) як такого, що не відповідає покладеним на нього обов'язкам, тобто це зона краху (відставки) цього працівника. Цій зоні відповідають стани системи $S_i \in S_3$;

4) зона катастрофічного ризику — область негативних наслідків, які за своїм значенням перевершують певний критичний рівень. Катастрофічний ризик призводить вже до визначення органу влади як невідповідного щодо покладених на нього обов'язків, тобто це зона краху (відставки) перш за все керівника органу влади. Їй відповідають стани системи з підмножини $S_i \in S_4$.

Зазвичай, стани системи, що входять у підмножину S_4, вже не компенсуються. У станах, що входять у підмножину S_3, необхідна, а у S_2 — можлива реалізація регулюючих рішень, таких, що у тому або іншому ступені компенсують збурювання зовнішнього середовища шляхом зміни технології опрацювання документів або навіть структури ОДВ, або переведення в режим станів S_2 чи S_1.

Кожному стану S_i на підмножинах S_2 або S_3 *n*-ї підсистеми АІАС відповідають первинні (теперішні) і вторинні (майбутні) втрати ефективності, тобто певні негативні наслідки. Отже, кожному стану S_i, ідентифікованому з однією або декількома підсистемами АІАС, відповідає вектор негативних наслідків $R_i = (r_i^1, \ldots, r_i^n, \ldots, r_i^N)$, де r_i^n — приведені до одиниці часу втрати ефективності системи у стані S_i підсистеми *n*. Для компенсації можливих негативних наслідків у кожному зі станів $S_i \in S_2$; S_3 може бути використана одна з регулюючих стратегій $\omega_\alpha \in \Omega_i$, де Ω_i — множина альтернативних стратегій з регулювання у стані S_i; $\alpha = [1, \ldots A]$ — номер стратегії.

У цих випадках при пошуках оптимальних рішень з регулювання необхідно як правило, послідовно розв'язувати дві взаємозалежні задачі:

1) вибір оптимальної стратегії регулювання ω_α, що являє собою сукупність управляючих рішень (операцій) $K_1(z) \in K$, зв'язаних між собою певною часовою послідовністю (тут α — номер стратегії; *K* — множина операцій (рішень); *l* — номер рішення);

2) вибір оптимальних значень факторів *z* для кожного рішення.

Політика забезпечення виконавчої обов'язковості. Така постановка вирішення проблем забезпечення ВО і побудови відповідної автоматизованої системи дозволяє залучити в теорію забезпечення ВО точні математичні методи. Тобто доводити, що дана система в заданих умовах підтримує політику забезпечення ВО. У цьому суть доказового підходу до використання інформації, що дозволяє говорити про «систему гарантованої ВО». Зміст «гарантованої ВО» в тому, що при дотриманні вихідних умов свідомо виконуються всі правила політики забезпечення ВО. Повний опис ПЗВО може бути достатньо об'ємним навіть у простих випадках, тому далі будемо користуватися скороченими описами. Підсумовуючи, якщо виходити з моделі забезпечення ВО, побудованої вище, відзначимо, що зміст ПЗВО дуже простий — це набір правил керування доступом до інформації.

ПЗВО за визначенням є конструктивною і може бути основою визначення деякого автомата або апарата для своєї реалізації. Водночас ПЗВО визначається неоднозначно і, природно, завжди зв'язана з практичною реалізацією системи і механізмів забезпечення ВО.

Вибір ПЗВО визначається інформаційним простором, припустимими природою процесів обробки інформації, траєкторіями в ньому і заданням несприятливої множини *N*. Коректність ПЗВО у даних конкретних умовах повинна бути, взагалі кажучи, доведена.

Побудова ПЗВО має відповідати наступним крокам: по-перше, в інформацію заноситься структура цінностей і проводиться аналіз ризику, а другим кроком визначаються правила для будь-якого процесу користування даним видом доступу до елементів інформації, що має дану оцінку цінностей. Однак реалізація цих кроків, апріорно, є складною задачею.

Пов'язаними є питання оцінки можливостей автоматизованої системи підтримувати ПЗВО. Вони також становлять складне завдання. Один з розв'язків якого може полягати у тому, щоб умови теорем, які доводять підтримку ПЗВО (включно з самою політикою), формулювати без доказу у вигляді стандарту. При цьому, як аксіому, потрібно прийняти розуміння поняття забезпечення ВО як контролю за доступом до інформації, а саме: автоматизована система забезпечує ВО, якщо вона забезпечує контроль за доступом до інформації так, що належним чином уповноважені особи або процеси, що функціонують від їхнього імені, у будь-який момент мають можливість отримати необхідну інформацію та опрацьовувати її шляхом читання, запису, створювання або її знищування.

З цієї аксіоми, інтерпретованої з відомої теорії інформаційної безпеки, можна інтерпретувати шість фундаментальних вимог до систем забезпечує ВО.

1. Необхідно мати явну і добре визначену політику забезпечення ВО як набір правил, які використовуються системою для того, щоб визначити, як забезпечити зазначеному ідентифікованому суб'єкту доступ до конкретного об'єкта.

2. Для того, щоб керувати доступом до інформації відповідно до правил ПЗВО, повинна бути передбачена можливість маркірувати кожен об'єкт міткою, що класифікує об'єкт, тобто надійно ідентифікує ступінь цінності об'єкта та режими доступу, надані тим суб'єктам, що потенційно можуть запросити доступ до об'єкта.

3. Суб'єкти індивідуально також повинні бути ідентифіковані. Ко-

жен доступ до інформації потрібно розглянути на предмет того, хто запитує доступ до інформації, на які класи об'єктів він має необхідність одержати доступ у даний час та чи є для цього необхідність.

4. Система, що гарантовано забезпечує ВО, повинна забезпечувати реєстрацію в аудиторській інформації появу подій, що мають відношення до забезпечення ВО. Аудиторська інформація повинна селективно зберігатися так, щоб з боку відповідальної за це групи можливо було відслідковувати дії, що впливають на забезпечення ВО.

5. Автоматизована система у своєму складі повинна мати апаратно-програмні механізми, що допускають незалежну оцінку для одержання достатнього рівня гарантій того, що система забезпечує виконання викладених вище вимог. Зазначені механізми стандартним чином повинні вбудовуватися в прикладні програмні засоби і проектуватися так, щоб виконати доручені задачі найоперативніше.

6. Механізми, що гарантовано реалізують зазначені базові вимоги, повинні бути постійно захищені від «взламування» і/або несанкціонованого внесення змін.

Зазвичай АІАС є розподіленою системою. У такій системі можливі два підходи до аналізу й оцінки забезпечення ВО.

1. Кожен компонент розподіленої системи є самостійною системою, що забезпечує власну ВО. Таким чином, розподілена система представляє множину взаємодіючих систем, що по-різному забезпечують ВО. У такому випадку питання гарантованого забезпечення ВО зводяться до доказу забезпеченості компонент й організації шлюзів для їхньої взаємодії. Одначе ніхто не відповідає за забезпечення ВО в системі в цілому.

2. Усі компоненти і зв'язки між ними складають єдине ціле. У цьому випадку існує деякий центр, що бере на себе зобов'язання забезпечити ВО в системі в цілому, незважаючи на невизначений периметр і змінювану конфігурацію. Тоді повинна існувати деяка політика забезпечення ВО в розподіленій системі і мережні засоби, що підтримують цю політику. Звідси отримуємо задачу синтезу з окремих компонентів єдиної системи забезпечення ВО, а також задача оцінки відповідних функцій компонент, з яких цю систему можливо синтезувати.

Аналіз і оцінка забезпечення ВО розподілених систем як єдиного цілого припускає аналіз частин, а потім побудову оцінки забезпечення ВО всієї системи в цілому. Аналіз компонентів і синтез єдиної оцінки забезпечення ВО всієї системи необхідний також при модернізації системи, при заміні старих компонентів новими, при синтезі системи з

блоків або частин, щоб мати можливість використовувати розробки різних виробників. При аналізі виникають дві проблеми: 1) як розділити систему так, щоб з аналізу й оцінки компонентів побудувати оцінку системи в цілому; 2) якими критеріями треба користуватися при аналізі компонентів і як з результатів для компонентів синтезувати загальну оцінку.

3.4. Методи визначення інформаційного навантаження в АІАС

Як зазначалося, діяльність органу влади в сучасних умовах значною мірою пов'язана з опрацюванням значного обсягу інформації, що останнім часом набуває явища масовості. Кількісна сторона процесів масового обслуговування є предметом розділу прикладної математики, який належить до теорії масового обслуговування (ТМО). У теорії масового обслуговування всі об'єкти, що розглядаються, поєднуються під загальною назвою «системи масового обслуговування». Одним із класів систем масового обслуговування є системи розподілення інформації (системи телетрафіку). Предметом теорії телетрафіку є кількісний бік процесів обслуговування потоків повідомлень у системах розподілення інформації.

У даний час методи теорії масового обслуговування використовуються для розв'язання найширшого кола задач і досить повно досліджені. Враховуючи, що основна мета теорії телетрафіку, який продовжує відігравати визначальну роль у розвитку теорії масового обслуговування, полягає в розробці методів оцінки якості функціонування систем розподілу інформації, можна стверджувати, що її можна застосувати й для розв'язання задачі вимірювання інформаційного навантаження в АІАС.

Проведемо інтерпретацію основних положень і визначень теорії телетрафіку у застосуванні для розв'язку поставленої задачі.

Як і будь-яка інша математична теорія, теорія телетрафіка оперує математичними моделями, а саме моделями систем розподілу інформації. Математична модель системи розподілу інформації містить три основні елементи — вхідний потік викликів (вимоги на обслуговування), схему системи розподілу інформації, дисципліну обслуговування потоку викликів.

Якщо спочатку на першому місці в теорії телетрафіку стояли задачі аналізу, тобто відшукання залежностей і значень величин, що харак-

теризують якість обслуговування, від характеристик і параметрів вхідного потоку викликів, схеми і дисципліни обслуговування, і які вирішувалися, як правило, за допомогою теорії ймовірностей, то зараз перед теорією телетрафіку постають складні ймовірносно-комбінаторні задачі синтезу, в яких потрібно визначити структурні параметри систем передачі (опрацювання) інформації при заданих потоках, дисципліні й якості обслуговування.

Близькими до задач аналізу і синтезу є задачі оптимізації. Одна з таких задач при проектуванні систем розподілу інформації формулюється в даний спосіб: визначити значення структурних параметрів інформаційної системи, для яких при заданих потоках, дисципліні обслуговування і вартості якісні показники функціонування системи розподілу інформації оптимальні.

При експлуатації систем розподілу інформації задача оптимізації формулюється як задача керування потоками викликів або/і структурою системи для досягнення найкращих показників якості функціонування.

Приймемо з точки зору розв'язання поставленої в АІАС задачі, що під потоком викликів як послідовності викликів, що надходять через будь-які інтервали або в будь-які моменти часу, розумітимемо потік документів, які вимагають обробки в АІАС відповідно до доручень, що їх супроводжують. Цей потік є випадковим потоком викликів.

Потік документів визначається трьома еквівалентними способами: послідовністю моментів надходжень $t_1, t_2, ..., t_n$, послідовністю проміжків часу між моментами надходжень $z_1, z_2, ..., z_n$ z_1, і послідовністю чисел $k_1, k_2, ..., k_n$, що визначають кількість документів, які надходять протягом заданих відрізків часу $[t_0, t_1), [t_0, t_2), ..., [t_0, t_n)$. При цьому під моментами надходжень розуміється момент одночасного надходження одного і більше документів.

Оскільки кожен документ має більше двох характеристик, потік документів є неоднорідним потоком. Водночас потік документів є стаціонарним неординарним потоком без післядії (неординарний пуассонівський). Тривалість обслуговування документів, що надійшли, приймається випадковою величиною з показовою функцією розподілу ймовірностей.

У ТМО важливе значення має поняття «вихід системи», що пішло від комутаційних систем, яке пов'язане перш за все з поняттям навантаження як сумарного часу обслуговування викликів. Для АІАС під ви-

ходом системи будемо розуміти умовний АРМ (державний експерт, що використовує комп'ютер), який забезпечує опрацювання документа.

Обслуговане системою за проміжок часу $[t_1, t_2)$ навантаження $y_0(t_1, t_2)$ являє собою суму часів займання всіх виходів системи (АРМів), обслуговуючих потік викликів, що надходять на її входи за розглянутий проміжок часу.

Нехай у систему, що має υ виходів, надходить потік викликів (документів). Будемо спостерігати за кожним з АРМів протягом проміжку часу $[t_1, t_2)$. Позначимо через τ_i суму відрізків часу, протягом яких *i*-й АРМ був зайнятий за час $[t_1, t_2)$. Тоді:

$$y_0(t_1, t_2) = \sum_{i=1}^{\upsilon} \tau_i. \tag{3.11}$$

За одиницю виміру інтенсивності навантаження, за аналогією з прийнятим у теорії телетрафіку, доцільно взяти ерланг (Ерл), що представляє собою навантаження за одне годино-займання. Інтенсивність обслугованого навантаження, виражена в ерлангах, кількісно дорівнює середньому числу одночасно зайнятих АРМів, що обслуговують це навантаження.

Таким чином, під навантаженням $y[t_1, t_2)$, що надходить на систему за проміжок часу $[t_1, t_2)$, розуміється таке навантаження, яке було б обслуговане системою за розглянутий проміжок часу, якби кожному викликові, що надходить, негайно (або в межах, визначених регламентом) було надано вільний АРМ для опрацювання.

За одиницю виміру інтенсивності навантаження, що надходить, також можна прийняти один ерланг.

Таке поняття ТМО, як згублене системою навантаження, що являє собою різницю між навантаженням, що надходить, і обслугованим навантаженням за розглянутий проміжок часу, для АІАС, через специфіку політики забезпечення ВО повинно мати інтенсивність, що дорівнює 0. Власне кажучи, ця вимога є одним з показників політики ВО.

Також у ТМО досліджується таке поняття, як концентрація навантаження, пов'язана із інтенсивністю навантаження в різні години доби або в ті самі години доби, але в різні дні. Для АІАС така ситуація також має місце. Поряд з випадковими коливаннями інтенсивності навантаження за годинами доби, днями тижня і місяцями року існують і періо-

дичні, відносно регулярні коливання. Ці чинники також треба враховувати при прогнозуванні навантаження.

Треба ще спиратися на той постулат ТМО, що для задовільної якості обслуговування документів у будь-який час розрахунок обсягу устаткування необхідно виконувати згідно зі значеннями інтенсивності навантаження в ту годину, коли воно є найбільшим. Ця година називається годиною найбільшого навантаження (ГНН).

Основними параметрами навантаження є: 1) число джерел навантаження — n; 2) середнє число викликів, що надходять від одного джерела навантаження в одиницю часу — c; 3) середня тривалість займання системи при обслуговуванні одного виклику — t.

За c і t необхідно розрізняти визначені категорії джерел навантаження, а саме: органи влади вищої ланки, центральні органи виконавчої влади, регіональні органи та ін. Відповідно до наявних категорій джерел навантаження визначається середнє число викликів в одиницю часу від одного суб'єкта категорії. Визначення середнього числа викликів від одного джерела відповідних категорій, що є вихідним для проектування системи, ґрунтується на результатах спостережень на діючих взаємовідношеннях органів влади. Тоді величина інтенсивності навантаження може бути розрахованою за формулою

$$y = n\, c'\, t', \tag{3.12}$$

де c' — середнє число викликів в одиницю часу від одного суб'єкта категорії; t' — середня тривалість заняття.

У теорії телетрафіку якість обслуговування викликів, що надходять, характеризується можливістю з'єднань або тривалістю чекання надання з'єднань. У цьому сенсі в АІАС слід розрізняти дві дисципліни обслуговування документів, що надходять: без утрат і з утратами.

Дисципліною обслуговування без утрат будемо називати таку, при якій документ, що надходить, забезпечується опрацюванням у момент часу, передбаченого регламентом, і з утратами, якщо опрацювання документа затримується на якийсь час, що перевищує встановлений регламентом.

З точки зору ТМО дисципліна з утратами в АІАС відноситься до дисципліни обслуговування з умовними втратами, тобто при якій виклик, що надходить на систему в момент відсутності вільних АРМів, не губиться, а обслуговується з чеканням (дисципліна обслуговування з чеканням).

Для кількісної оцінки якості обслуговування з чеканням можуть розраховуватися такі ж самі характеристики: імовірність чекання для документа, що надійшов; імовірність чекання для будь-якого документа, що надійшов, понад встановлений час; середній час чекання стосовно усіх документів, що надійшли і по відношенню тільки до затриманих документів тощо.

Важливе значення для АІАС має дисципліна обслуговування з пріоритетами, при якій документи, що надходять, поділяються на категорії, і документи більш високої категорії при обслуговуванні мають певні переваги (пріоритети) перед документами більш низької категорії.

Прикладом дисципліни обслуговування з пріоритетом може служити опрацювання документів, що надходять від вищих органів влади.

Однією з найважливіших характеристик систем є їхня ефективність. Як показник ефективності поряд з економічними (капітальними, експлуатаційними витратами) має використовуватися і такий технічний показник, як пропускна здатність. Під пропускною здатністю системи розуміється інтенсивність навантаження обслугованою системою при заданій якості обслуговування.

Пропускна здатність системи залежить від кількості АРМів, від способу (схеми) об'єднання цих АРМів, класу потоку документів, структури системи з урахуванням серверного обладнання, швидкості телекомунікаційних каналів, розподілу тривалості обслуговування і дисципліни обслуговування.

Задачі, пов'язані з вивченням процесів обслуговування автоматизованими системами потоків документів, що надходять, вимагають дослідження мікростанів системи. Досить просто скласти системи рівнянь, що описують досліджувані процеси, дозволяють марковські процеси. Однак розв'язання зазначених систем рівнянь наштовхується на великі обчислювальні труднощі.

Найбільш ефективним засобом розв'язання зазначених задач є метод статистичного моделювання. Метою моделювання є одержання статистичних оцінок імовірнісних характеристик процесів обслуговування системою потоків документів, що надходять, при заданих дисциплінах обслуговування. Ці оцінки прийнято називати статистичними характеристиками. До таких характеристик, наприклад, у системах з чеканням відносяться розподіл часу чекання початку обслуговування, середній час чекання, середня довжина черги й інші характеристики. Але закономірності формування потоків навантаження в АІАС можуть бути з'ясовані тільки шляхом постановки спостережень на діючих системах.

Одним з чинників, від якого істотно залежить навантаження у ГНН, є кількість та інтенсивність напрямків *ij* від даної АІАС$_i$ до інших АІАС$_j$ органів влади, що входять у сферу спілкування з органом влади, система якого розглядається. Якщо, наприклад, АІАС$_i$ переважно виконує доручення органів влади вищого рівня, то має місце більш інтенсивне навантаження. Тобто за інших рівних умов величини інтенсивності потоків навантаження в ГНН y_{ij}^{*} $(i, j = 1, 2,..., r)$ тим більші, чим ближче знаходяться АІАС$_j$ до «сфери тяготіння» даної АІАС$_i$.

Аналіз закономірностей формування абсолютних значень потоків навантаження звичайно виконувати досить складно, тому що взаємо відносини органів влади в часі не залишаються постійними, а АІАС розрізняються потужністю і структурним складом. Тому доцільно використовувати відношення інтенсивностей навантаження на напрямках взаємодії між АІАС до інтенсивності навантаження, що виходить від АІАС:

$$k_{ij} = y_{ij} / y_{i\ âèõ}(i, j = 1,2,...,m). \tag{3.13}$$

Ці відношення назвемо коефіцієнтами розподілу навантаження.

Очевидне виконання наступної умови:

$$\sum_{i=1}^{m} k_{ij} = \sum_{i=1}^{m} (y_{ij} / y_{âèõ\,i} = 1 \tag{3.14}$$

При відомих значеннях цих коефіцієнтів інтенсивності потоків навантаження визначаються з виразу

$$y_{ij} = k_{ij} y_{âèõ\,i}(i, j = 1,2,...,m). \tag{3.15}$$

Величина коефіцієнта розподілу k_{ij} тим більше, чим більше відношення інтенсивності вихідного від АІАС$_j$ навантаження до інтенсивності сумарної вихідної від усіх АІАС, що взаємодіють:

$$\omega_j = y_{âèõ\,j} / \sum_{j=1}^{m} y_{âèõ\,j}. \tag{3.16}$$

Таким чином труднощі прогнозування коефіцієнтів k_{ij} полягають

у тому, що їх значення залежать від цілого ряду факторів, що визначаються взаємним тяжінням $АІАС_i$ до $АІАС_j$. Кількісною оцінкою тяжіння можуть бути коефіцієнти тяжіння. При рівномірному тяжінні між усіма АІАС сфери взаємодії інтенсивність навантаження від $АІАС_i$ до $АІАС_j$ y'_{ij} $(i, j = 1, 2,..., m)$ пропорційна частці інтенсивності навантаження, що виходить від $АІАС_j$, у сумарній інтенсивності навантаження, що виходить від усіх АІАС сфери взаємодії:

$$y'_{ij} = y_{âèõ\,i}(y_{âèõ\,j} / \sum_{j=1}^{m} y_{âèõ\,j}) = y_{âèõ\,i}\omega_j. \qquad (3.17)$$

Але для діючих систем ця рівність виконуватись звичайно не буде, тому що тяжіння між різними АІАС є нерівномірним. Якщо в ліву частину цього виразу підставити фактичне значення навантаження y_{ij}, то для виконання рівності праву частину цього виразу необхідно помножити на коефіцієнт тяжіння f_{ij}. Тоді:

$$f_{ij} = \frac{y_{ij}}{y'_{ij}} = \frac{y_{ij}}{y_{âèõ\,i} y_{âèõ\,j}} \sum_{j=1}^{m} y_{âèõ\,j}. \qquad (3.18)$$

Коефіцієнт тяжіння f_{ij} $АІАС_i$ до $АІАС_j$ являє собою відношення фактичного значення інтенсивності навантаження від $АІАС_i$ до $АІАС_j$ до того значення інтенсивності навантаження, що було б між цими системами при рівномірному тяжінні в сфері взаємодії. При рівномірному тяжінні $f_{ij} = 1$ $(i, j = 1, 2,\ldots, m)$.

Значення коефіцієнтів тяжіння можна розрахувати тільки для діючих систем. Для проектованих АІАС їх значення слід прогнозувати на підставі аналізу закономірностей розподілу навантаження на діючих сферах взаємодії. Тоді для всіх АІАС у результаті прогнозу визначаються значення інтенсивностей вихідних навантажень $Y_{івих}$ $(i = 1, 2,\ldots, m)$ і матриця векторів коефіцієнтів тяжіння $\|f_{ij}\|$. Потрібно також розрахувати матрицю векторів міжсистемних потоків навантаження $\|Y_{ij}\|$.

Труднощі прогнозування матриці $\|f_{ij}\|$ полягають у складній зале-

жності зміни значень коефіцієнтів f_{ij} із зростанням кількості органів влади, що входять до сфери взаємодії. Ця залежність може бути спрощеною з використанням так званих нормованих коефіцієнтів тяжіння.

Крім коефіцієнтів f_{ij} можна застосовувати й інші коефіцієнти для врахування тяжіння між АІАС (у літературі з теорії телетрафіку вони описані). Однак, які б коефіцієнти не застосовувалися, прогнозування їхніх значень може здійснюватися тільки на основі спостережень за їхніми значеннями на діючих взаємодіях.

Використовуючи отримані характеристики, можна запроваджувати зміни правил (алгоритмів) опрацювання документів, структуру системи або інші показники функціонування системи, тобто таке керування можна віднести до керування потоками або керування технічними засобами системи.

Спосіб керування, при якому виробляється зміна розподілу потоків по напрямках, за величиною або характером розподілу викликів у потоці залежно від зміни стану системи або її окремих частин, відноситься до динамічного керування.

У випадку динамічного керування при зміні плану розподілу потоків характер потоків документів може змінюватися в будь-яких складових системи. Сама зміна плану розподілу потоків при динамічному керуванні може здійснюватися як за рахунок вибору відповідних шляхів обробки (що приводить до поділу або об'єднання потоків), так і за рахунок заборони обслуговування окремих документів.

Складання плану розподілу потоків може здійснюватися з використанням декількох способів вибору оптимальних шляхів розподілу (матричного, на графах, ігрового способу). Частина способів ґрунтується на зборі інформації шляхом безпосереднього контролю за станом елементів системи; інші способи використовують непрямі методи збору інформації шляхом аналізу статистичних даних про попередні процеси обробки.

У загальному випадку при динамічному керуванні для оцінки стану системи або її окремих частин засоби, призначені для керування системою, повинні накопичувати інформацію про стан системи протягом деякого періоду часу, усереднювати її і здійснювати керування за середнім значенням. Тривалість періоду нагромадження інформації про стан системи визначає ефективність керування. Дуже короткі періоди не дозволяють одержати досить достовірну інформацію, і керування по коротких інтервалах нагромадження інформації може виявитися неефе-

ктивним через прийняття занадто частих і поспішних рішень, що не забезпечують ефективності функціонування системи. З іншого боку, надмірно довгі інтервали спостережень роблять систему консервативною, що працює неефективно протягом тривалих періодів.

У системі можна запроваджувати централізований, зоновий і децентралізований способи керування.

При централізованому способі керування вся інформація накопичується в єдиному центрі і на її підставі приймається загальне рішення для всіх елементів системи, що і передається у відповідні ланки для його виконання.

Іншим, протилежним способом керування є децентралізоване керування, при якому окремі підсистеми приймають місцеві рішення про алгоритми опрацювань на підставі інформації від прилеглих (сусідніх) підсистем.

Зоновий спосіб керування є проміжним між зазначеними вище двома способами. При цьому способі інформація про стан системи збирається в межах частини системи (зони) і рішення, прийняті зоновим керуючим пристроєм, призначаються для їхнього використання в межах розглянутої зони.

З цього бачимо, що подібні задачі для систем з динамічним керуванням відрізняються складністю. Крім того, як і інші задачі, сформульовані для системи, вони відносяться до досить складної структури реальних інформаційних розподілених систем: потоки, які обслуговуються системою, через зміну плану розподілу потоків можуть приймати складний характер, що важко піддається аналітичному опису. У зв'язку з цим більшість задач визначення пропускної здатності АІАС або порівняння різних алгоритмів опрацювання документів при динамічному керуванні може розв'язуватись лише методом статистичного моделювання.

Підсумки до розділу

Враховуючи, що органи влади функціонують у непередбачувальному інформаційному середовищі, яке формується на основі імовірнісних законів, в умовах обмеження реального часу, протягом якого повинні бути прийняті управлінські рішення, багатокритеріальності при прийнятті управлінських рішень, можна стверджувати, що АІАС представляють новий клас систем. Тому з огляду на складність і багатогранність проблем автоматизації функцій управління в органі влади, на

інформаційний аспект його діяльності, на аналіз та оцінку підходів до моделювання АІАС при проведенні досліджень системи має застосовуватися системний підхід із використанням інформаційного аналізу вхідних/вихідних інформаційних потоків із задіянням методів моделювання і порівняльного аналізу.

Для забезпечення динамічної стійкості виконання органом влади функцій державного управління, сприяння боротьбі з інформаційною ентропією, розширення доступу до інформації в процесі прийняття рішень експертів і керівництва АІАС має включати «інформаційний регулятор», який використовується для керування в системі за рахунок керування ресурсами системи (технічними і програмними засобами), а також за рахунок керування інформаційними потоками (зміна шляхів передачі й обробки практично без обмеження обсягу потоків).

Як теорію, що має забезпечити розкриття закономірностей автоматизації функціонування органів влади, розробки принципів визначення технологічних операцій, організаційних заходів, структурних перебудов у конкретних галузевих ситуаціях в умовах послідовно-паралельного підключення різних підрозділів органу влади для розв'язання проблем, як базу формалізації та моделювання АІАС, можна застосувати теорію ситуаційного регулювання технологічних процесів в органі влади при автоматизованій обробці інформаційних потоків.

З метою забезпечення вичерпної інформаційної підтримки рішень, а також забезпечення регламентованої бюрократичної роботи на базі визначених процедур і дисциплін як основного завдання АІАС доцільне застосування поняття «виконавчої обов'язковості» та реалізація відповідної політики.

Розв'язання окремих задач, пов'язаних з керуванням у системі, може бути проілюстровано методами теорії телетрафіка як складової теорії масового обслуговування, і в деяких випадках існує можливість оцінити ефект від використання того або іншого способу керування в системі. Методологія дослідження специфіки інформаційного навантаження АІАС в стаціонарному режимі має базуватись на використанні оцінок інтенсивностей надходження потоків документів.

Враховуючи наявність у системі семантичної інформації, для вирішення проблеми структурування інформаційних потоків, що циркулюють між органами державної влади, доцільно застосувати методологію зростаючих пірамідальних мереж (ЗПМ), що базується на теорії логіко-лінгвістичних інформаційних моделей (ЛЛМ).

РОЗДІЛ 4

АРХІТЕКТУРА АІАС ЯК ОСНОВНИХ СКЛАДОВИХ ІНФРАСТРУКТУРИ ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЕРЖАВНОЇ ВЛАДИ

4.1. Архітектурні стратегії

Стратегія інформаційного менеджменту. Інформаційний підхід базується на антиентропійному розумінні переборення проблем управління. Тому в основі стратегії інформаційного менеджменту (information management) лежить концептуальна розробка всієї системи збору, обробки, зберігання і передачі інформації, застосування комп'ютерів, оргтехніки та засобів зв'язку на підприємстві, в установі, організації [169, 177].

Останнім часом набули поширення, поряд з концепцією інформаційного менеджменту, й такі напрямки, як управління документами (document management), управління знаннями (knowledge management), управління взаємодії з клієнтами (customer relationship management) та інші концепції, але всі вони базуються на інформаційному підході і для реалізації стратегії інформаційного менеджменту мають бути поєднані в єдиний комплекс.

Інформаційний менеджмент базується на ідеології керування життєвим циклом інформації (*Information Life Cycle Management*), що має циклічний характер (рис. 4.1).

Інформацією найкраще управляти, якщо використовувати підхід її циклу життя до кожного елемента, до якого звертаються, відносно інших елементів циклу життя.

Процеси менеджменту інформації відпрацьовувались при створенні систем управління окремих підприємств, як то було за недавніх часів. Але зараз вони стали визначальними й у досягненні ефективності функціонування та розвитку виробничих об'єднань, цілих регіонів, країн, і навіть об'єднань країн.

Стосовно державного управління слід зазначити, що уряд Канади, який, як вже вказувалось, є лідером впровадження в органах влади інформаційних технологій та формування електронного урядування, приділяє значну увагу перш за все питанням інформаційного менеджменту. Класифікація і реєстрація стали частиною централізованої функції керування інформацією, реалізованою у Національному архіві, що була

широко поширена усюди по урядових інституціях. При цьому фахівці з ІТ забезпечили послуги керування інформацією так, щоб ті, хто працює з нею, могли зосередитися на своїх первинних обов'язках, не витрачаючи часу на додаткові функції підтримки.

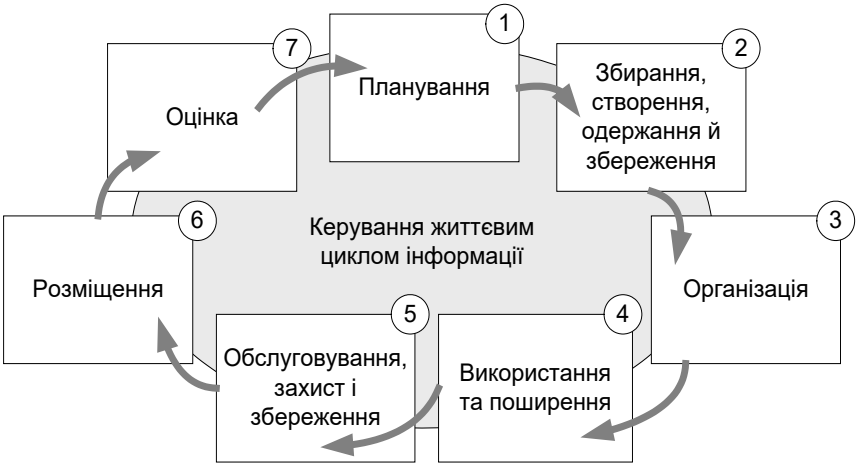

Рис. 4.1. Керування життєвим циклом інформації

Стратегія інформаційного менеджменту полягає у розробці інформаційної інфраструктури та системної концепції об'єкта управління, а також в управлінні технологією і даними. Якщо взяти для прикладу об'єкта управління звичайне підприємство, що більш апробоване, то до інформаційної інфраструктури його належать обладнання, засоби і заходи, які створюють умови для переробки інформації, що супроводжує процес виробництва, а також для зв'язку.

Так, у частині управління технологією на підприємстві необхідно проводити роботи щодо створення нових технологій, зорієнтованих на ринок, які дають продукцію, що здатна здобути своє місце в розмаїтті ринкових відносин. Тут обов'язково приймаються також рішення стосовно кадрової політики, ефективності діяльності та ін. При цьому управління даними передбачає опис і моделювання даних, розробку концепції баз даних, проектування захисту і надійності даних. У частині системної концепції підприємства виникає безліч задач, тому що інформатизація впливає і на структуру підприємства, і на характер виробництва, і на зв'язки із зовнішнім світом. При цьому впровадження на підприємстві інформаційних технологій і комунікаційних засобів має

змінити не тільки вигляд його документообігу, а й змінити саму його структуру, з тим, щоб домогтися оптимальної форми єдності окремих компонент об'єкта управління для досягнення максимальної ефективності його функціонування.

Глобальні за своєю значущістю та складністю завдання інформаційного менеджменту стоять на рівні управління державою. Поряд з проблемою аналітичної обробки масового об'єму інформації виникає необхідність геополітичного, соціального, економічного моніторингу, який підтримує процеси прийняття рішень щодо комплексних проблем з різних сфер діяльності суспільства з метою захисту національних інтересів, національної безпеки, забезпечення зростання добробуту населення та ін.

Задачі інформаційного менеджменту на рівні управління державою можна класифікувати так само, як і для підприємств, однак тут вони набувають іншого ступеня деталізації і вимагають для свого розв'язання переробки незрівнянно більшого обсягу неформалізованої інформації. При цьому урядова інформація найкраще управляється, коли кожний елемент циклу життя безпосередньо пов'язаний з діяльністю урядової установи, що управляє нею.

Водночас канадські фахівці вказують на проблеми, які виникають в сфері управління інформацією разом із розвитком технологій. Так, у зв'язку із широким поширенням персональних комп'ютерів, централізовані концепції керування почали руйнуватися. Кожен державний службовець став «інформаційним менеджером» без навчання або знань, необхідних для виконання цих нових функцій. З появою Інтернету як домінуючого засобу комунікації між людьми й організаціями усе більше інформації вироблялося в електронній формі й обсяг цієї інформації зростав по експоненті. І тут за відсутності централізованих засобів керування ставало усе важче знайти інформацію, внесену в каталоги пошукових засобів відповідно до нестандартних схем класифікації, за які ніхто не відповідає.

Цей приклад говорить про те, що впровадження на державному рівні сучасних інформаційних технологій і програмно-технічних засобів може привести до ефективного використання інформації тільки поряд з розробкою і реалізацією системної концепції організації управління інформацією. Складність розробки автоматизованих процедур управління полягає ще й в тому, що, на відміну від рівня підприємства, об'єкт управління не має чітко окреслених меж, а динаміка розвитку подій в країні і в світі не дозволяє визначити функції управління назав-

жди, чи хоч би на довготривалий час, чітко й однозначно. При цьому в системах такого класу має існувати можливість не лише автоматичної підготовки інформації про проблемну область, предмет, процес, що розглядаються, а й здійснюватися, у відповідності з досягнутим рівнем формалізації знань, інтеграції цих знань з неформальними знаннями групи осіб (фахівців, експертів, керівників), що приймають рішення. Це має відбуватися в умовах великого обсягу неформалізованої інформації та відсутності певних знань про об'єкт, неоднозначності і невизначеності вхідних даних.

Один із шляхів створення у таких умовах системи комплексного інформаційно-аналітичного забезпечення розв'язання задач, які стоять перед органами державної влади, розглянуто в [178, 179] на основі єдиної інформаційної системи спільного використання геоінформаційних систем (ГІС) і OLAP-технологій. Така система, використовуючи загальні джерела інформації з виробничої та фінансово-господарської діяльності галузі та єдину технологію інтеграції різнорідних баз даних, забезпечить наступний аналіз інформації і візуалізацію його результатів, а також дасть змогу сформувати інструментарій підтримки прийняття рішень керівництвом органу державної влади. Основним недоліком такого підходу є об'єктивні вимоги достатньо великих фінансових витрат та значного часу на впровадження та освоєння користувачами засобів, що пропонуються. Але, враховуючи стрімкий розвиток апаратних і програмних засобів обчислювальної техніки, не менш інтенсивне зростання загальної «комп'ютерної грамотності» держслужбовців, цей напрямок є досить перспективним.

Структурні особливості. Для розгляду концепції архітектури АІАС також треба враховувати можливі структури органів влади. Сфера діяльності органу влади має власну внутрішню структуру із складною системою зв'язків з такими складовими та особливостями:

а) просторово розподілена мережа об'єктів або суб'єктів діяльності галузі (заводи, фабрики, підприємства, наукові та освітні заклади, засоби транспортування і реалізації продукції);

б) функціональне розмежування діяльності об'єктів або суб'єктів галузі (здобич сировини, її переробка, транспортування, реалізація, надання послуг, проектування, наукові дослідження, будівництво об'єктів);

в) наявність або відсутність загальної організаційної структури управління діяльністю;

г) відповідність інформаційно-технічного оснащення сучасному рівню (комп'ютери і периферійні пристрої, програмні засоби, розвинені комунікаційні мережі, кваліфікований персонал).

Цим умовам відповідають більшість органів державної влади України. Враховуючи викладене, треба зазначити, що складання класифікації АІАС органів державної влади є непростим завданням. Специфіка державного апарату полягає у значній нерівномірності розподілу функціональних обов'язків між органами влади. З одного боку — це потужні міністерства з розгалуженою системою регіональних органів управління або органи з поширеною мережею об'єктів, яка існує у сфері впливу органу. З іншого — це органи влади, що виконують дуже важливі функції, але не мають ані галузі, ані регіональних органів управління. Між ними знаходиться поле проміжних конфігурацій органів державної влади.

Крім того, для забезпечення певних функцій органу влади виникає необхідність створення спеціальних ІАС, що, як правило, мають міжвідомчий характер. Тобто АІАС органу влади повинні забезпечити ще й інтеграцію у певні міжвідомчі ІАС, а також до єдиного комплексу спеціалізованих ІАС. Таким чином, для забезпечення складання уявлення про структуру АІАС доцільно розпочати з виявлення окремих складових його об'єкта управління. Аналіз існуючих галузевих структур доводить, що у загальному випадку вони складаються з таких компонент (рис. 4.2):

1) центральний апарат органу державної влади (СА);

2) регіональні та місцеві органи управління (PU_i), $i = (0, I)$;

3) підприємства та об'єкти, що входять до сфери управління (PU_j), $j = (0, J)$;

4) пересувні засоби інформування (MU_k), $k = (1, K)$.

Наведені компоненти можуть мати власні зовнішні зв'язки (*OL*). Центральний апарат органу державної влади також здійснює регуляторний вплив на суспільну систему (*RF*). Водночас центральний апарат знаходиться під постійною загрозою порушень інформаційної безпеки $W'_ç$ та $W'_{âi}$. Рівень складності галузевої структури RC_G визначається значеннями *I*, *J*, *K*.

Згідно з наведеним оглядом можливих складових органу влади, проведемо попередню загальну класифікацію органів влади з урахуванням наявності (+) або відсутності (–) конкретних структур (табл. 4.1).

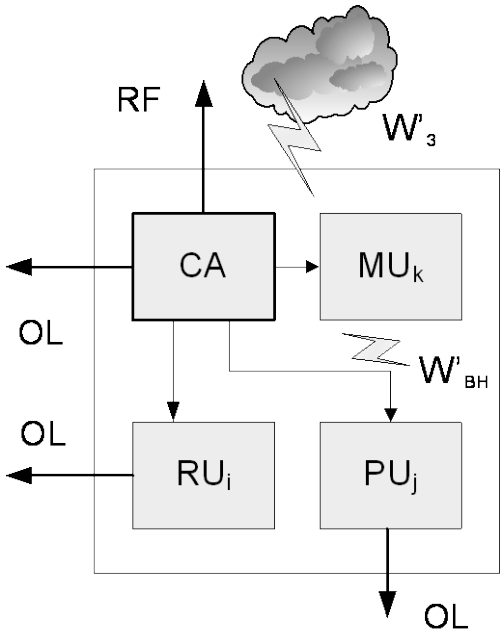

Рис. 4.2. Компоненти галузевих структур

Таблиця 4.1. Основні структури органів влади

Вид органу влади	**Наявність компонентів структури**			
	CA	RU_i	PU_j	MU_k
Органи влади вищого рівня	+	–	+/–	+
Центральні органи влади	+	+/–	+/–	+/–
Регіональні органи влади	+	+	+/–	+

Головною частиною є центральний апарат органу державної влади, який також має власну складну структуру (рис. 4.3). Структура центрального апарату визначається специфікою кожного органу влади, а структурні підрозділи, які утворюються у його складі, визначаються відповідними рішеннями вищого органу (для виконавчої влади — Кабінетом Міністрів України).

Загалом структурні підрозділи поділяються на функціональні (FD_i, $i = (1, D)$) і допоміжні (SD_j, $j = (0, S)$). Функціональні підрозділи забезпечують виконання функцій і повноважень, спрямованих на досяг-

нення основної мети діяльності центральних органів виконавчої влади. Допоміжні підрозділи виконують роботу, пов'язану із забезпеченням належних умов функціонування центрального органу виконавчої влади (його структурного підрозділу), незалежно від напряму та характеру його завдань — це кадровий, юридичний, контрольно-ревізійний, протокольний відділи, бухгалтерія та ін.

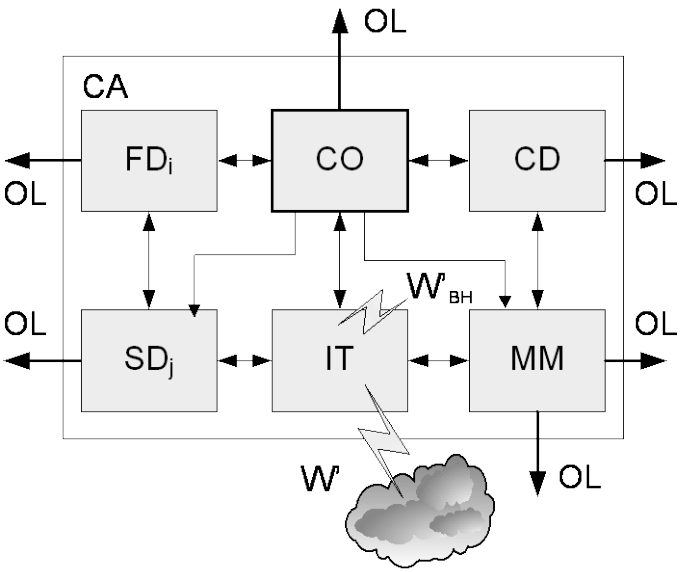

Рис. 4.3. Компоненти структури центрального апарату органу влади

Рівень складності структури центрального апарату RC_{CA} визначається значеннями *D*, *S*, які знаходяться залежно від *I*, *J*, *K*, тобто

$$\{RC_{CA}\} = F\,(I, J, K). \tag{4.1}$$

Керівництво органу влади (*CO*) має власний обслуговуючий персонал (*CD*), який здійснює організаційно-аналітичне забезпечення роботи керівника та складається з інституту радників і помічників, референтів тощо. Окремо слід виділити підрозділ інформаційних технологій (*IT*), що забезпечує супроводження засобів інформатизації та має забезпечувати заходи з захисту інформації, та сектор взаємодії з громадськістю, засобами масової інформації (*MM*). Наведені компоненти та-

кож можуть мати власні зовнішні зв'язки (*OL*).

Слід зазначити, що структура центрального апарату визначається разом із штатним розкладом на підставі функціональної компетенції органу влади. Зазвичай це відбувається інтуїтивно, ґрунтуючись на традиціях і наявних обсягах фінансування. Формалізованих методів формування структури СА не існує.

Що стосується структури інших компонент із зображених на рис. 4.2, слід зазначити, що регіональні та місцеві органи RU_i містять певну частину з підрозділів, визначених для центрального апарату, тобто є їхньою зменшеною копією. У свою чергу вони мають додаткові «виробничі» підрозділи, тобто підрозділи, призначені для виконання функцій взаємодії з населенням (наприклад, приймання та обробки податкових декларацій у місцевих державних податкових адміністраціях).

Компоненти PU_j мають стандартну виробничу структуру, яка конкретизується в залежності від специфіки діяльності. Засоби MU_k поділяються на дві категорії — транспорт для обслуговування керівництва та спеціальні засоби для забезпечення виконання керівництвом галузі функцій управління в мобільних оперативних умовах.

Стратегія інтеграції систем. Як вже неодноразово зазначалося, а також згідно з аналізом канадського досвіду, архітектура системи «електронного уряду» має бути спрямована на забезпечення міжвідомчої (корпоративної) інформаційної інфраструктури на основі загальновизнаних технологій, міжнародних рекомендацій та стандартів (Інтернет/Інтранет-технології, подання інформації у форматі XML, забезпечення необхідного рівня автентифікації користувачів, доступності й цілісності інформації, що є власністю держави). Це потребує не лише координації всіх програм у сфері інформатизації державних органів й у галузі їхньої ІБ, незалежно від їхньої відомчої приналежності, а й ***інтеграції*** відомчих АІАС до єдиної ***інтегрованої інформаційно-аналітичної системи органів влади (ІІАС)***, формування загальної проблемно-орієнтованої інформаційної інфраструктури органів влади [51, 44].

В умовах, коли керівникам будь якого рангу потрібно приймати відповідальні рішення, часто-густо за обмежений час, подати їм для ефективного оперативного аналізу великий обсяг різнопланової інформації — найважливіше завдання АІАС. Вочевидь, його в змозі вирішити лише наявність загального інформаційного простору державної влади, яке може формуватися та підтримуватися із застосуванням інтеграційного підходу.

З точки зору безпеки у зв'язку з цим слід також звернути увагу й на вимоги щодо застосування в АІАС апаратного та програмного забезпечення, основною серед яких має бути наявність ефективних централізованих засобів управління та адміністрування, що дозволяють виконувати наскрізний нагляд і контроль за функціонуванням системи в цілому й управління на всіх рівнях її ієрархії, а також забезпечують необхідну гнучкість та динамічну зміну конфігурації.

Як концептуальна схема (модель) постановки й вирішення проблеми інтеграції систем останнім часом набула поширення мережноцентрична (network-centric) парадигма [180]. При цьому в такій інтегрованій системі ймовірно доцільно слідувати принципу організації інформаційних, обчислювальних, телекомунікаційних і людських ресурсів по типу ***«матриці»***, що отримує за кордоном усе більший розвиток, коли забезпечується гнучкий, безпечний і централізований розподіл ресурсів в інтересах так званих «віртуальних організацій», створюваних під рішення виникаючих завдань у складній динамічній обстановці [181]. Матричний підхід базується на технології так званих «тонких клієнтів», у якій щораз для розв'язання конкретних задач на робочих станціях користувачів всі необхідні програми й дані або завантажуються безпосередньо з потужних мережних серверів, або їх використовують на цих серверах. Такі сервери підтримуються ***центрами обробки даних (ЦОД)***, а мережною базою є корпоративна мережа органів влади та Інтернет, який вже поступово трансформується в мережу додатків, що виконуються [182] (рис. 4.4).

Фактично мова йде про організацію так званої «хмарної обробки даних» (*Cloud computing*) як технології, в якій програмне забезпечення надається користувачеві як Інтернет-сервіс. Завдяки віртуалізації, що лежить в основі цієї технології, користувачі отримують стільки ресурсів, скільки їм треба, одержують доступ до найнадійнішої інфраструктури з необхідною продуктивністю. Відомі комерційні рішення «хмари» в Інтернеті оцінюються рівнем надійності в 99,999! Хмарні системи, як правило, й набагато краще захищені, та й до кінцевої ОС важко добратися, адже там може бути кілька рівнів віртуалізації, моніторингу і систем безпеки.

Вимоги інтеграції АІАС різних органів державного управління до єдиної системи потребують передбачення у структурі АІАС певних ***інтеграційних компонент*** **(ІК)**, що підтримують функції обміну інформацією, опрацювання керуючих сигналів і синхронізації функціонування систем [51].

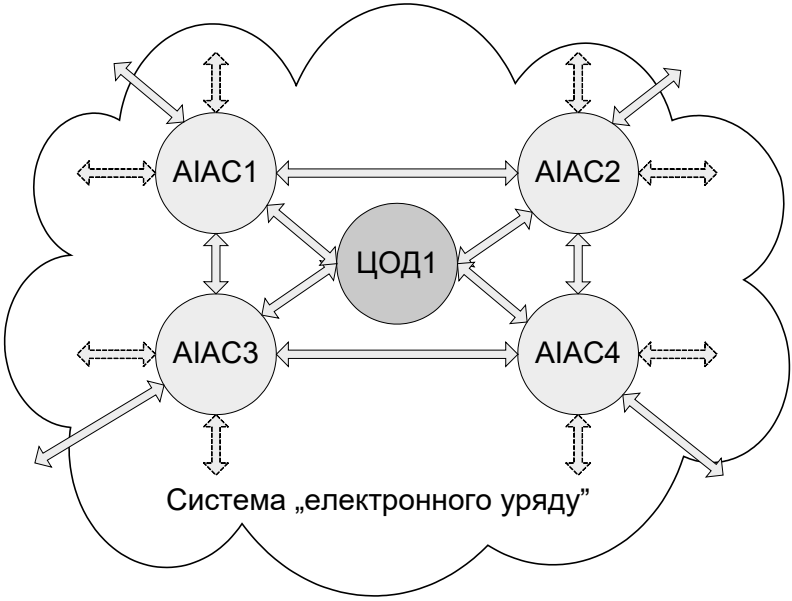

Рис. 4.4. Матрична інтеграція АІАС

Стратегія захисту інформації електронного уряду. Таємність, безпека та безвідмовність обробки інформації для *е*-уряду є найважливішими питаннями забезпечення його функціонування, тому вони становлять одну з концептуальних засад побудови АІАС. Це передбачає:

- повний захист конфіденційності та таємності урядової інформації;
- гарантії, що відповідають потребам і очікуванням клієнта;
- закінчену архітектуру безпеки, що ґрунтується на стандартах безпеки, рішеннях і методах ІМ/ІТ.

Згідно з цим загальна ІМ/ІТ інфраструктура має передбачати наявність:

- безпечного каналу, що забезпечує доступ до послуг *е*-уряду;
- виявлення вторгнення, що допоможе охороняти інфраструктуру;
- інфраструктури відкритого ключа (PKI), що забезпечує підтвердження автентичності взаємодії;
- заходи та засоби, що забезпечать безвідмовність в обслуговуванні клієнтів.

Безпечний канал — це загальна інфраструктура, що поєднує стратегічні проекти й технології, що підтримують ідеологію *е*-уряду, і формує безпечне швидкодіюче електронне навколишнє середовище органу влади з метою підтримки обслуговування клієнтів.

Використовуючи PKI, орган влади забезпечує:

- захист персональної (не класифікуємої) інформації й комунікацій, таких як внутрішні, а також взаємодію в секторах G2G, G2B, C2C;
- застосування для таємної інформації;
- гарантії конфіденційності й ідентифікації, цілісності даних і автентичності.

В основі PKI лежить використання двох ключів, комерційного наявного програмного забезпечення та відкритих стандартів.

Чому орган влади має потребу в послугах автентифікації? Це забезпечує:

- гарантії, що учасники діалогу саме ті, ким вони є за їхнім ствердженням;
- підтримку цілісності даних і конфіденційності персональної інформації;
- юридичне свідчення для невідмови від учинених дій;
- можливість розрізняти рівні встановлення дійсності для різних пропозицій обслуговування;
- безпечні та надійні електронні підписи.

Піонером і лідером у розвитку й розгортанні PKI-технології для послуг автентифікації є Канада, а її урядові послуги автентифікації для безпеки й захисту таємності є світовим прецедентом. Тому заслуговує на увагу модель автентифікації, що реалізовано в агенціях канадського уряду (рис. 4.5)[58] та яка відповідає вказаним принципам. Вона передбачає, що один або більше засобів обслуговування керування сертифікатами ключів підтримує множина провайдерів. Сертифікат (ePass) містить тільки унікальне число (MBUN) як унікальне ім'я.

Модель будується на основі згоди: клієнти вибирають, чи дійсно зв'язати множину програм з тим же самим MBUN (сертифікатом). При кожній програмі є програмно визначений ідентифікатор клієнта, зв'язаний з кожним MBUN, щоб гарантувати повторне визнання.

[58] Джерело PKI Secretariat IT Security, Chief Information Officer Branch, Treasury Board Secretariat, Government of Canada

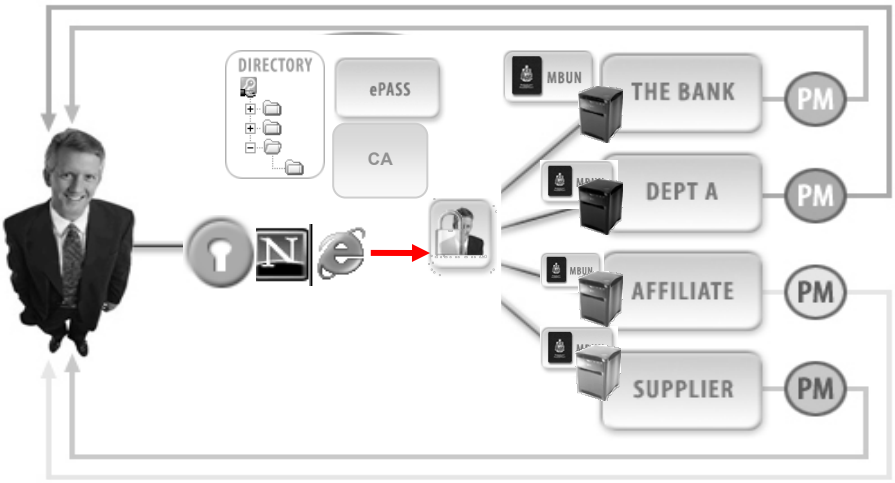

Рис. 4.5. Модель автентифікації канадського уряду

Для повноцінної роботи й збереження мінімального набору критично важливих функцій АІАС повинна мати цілком визначений запас стійкості до зовнішніх дестабілізуючих впливів середовища. Ця проблема впливає, насамперед, на підвищення вимог до інформаційної безпеки та ***живучості*** АІАС, що характеризуються високим ступенем розподілу ресурсів (обслуговуванням, програмним й апаратним забезпеченням, телекомунікаціями).

Поняття живучості (survivability) системи [183] пов'язане з її здатністю вчасно виконувати свої функції в умовах дії дестабілізуючих факторів (фізичне руйнування, часткова втрата ресурсів, відмови та збої елементів, несанкціоноване втручання в контур управління). При цьому технічна надійність, що проявляється як здатність системи працювати на заданому відрізку часу в штатній ситуації без відмов, визначає мінімальний поріг стійкості системи, за яким без наявності системи відновлення втрачених елементів і функцій може наступити катастрофа. Отже, живучість інформаційних систем має визначальне значення для інформаційної безпеки в цілому та взагалі розглядається як концепція інформаційної безпеки 21-го століття [184–187].

Узагальнюючи викладене, основні концептуальні підходи, що визначають засади архітектури АІАС, можуть бути показані на рис. 4.6.

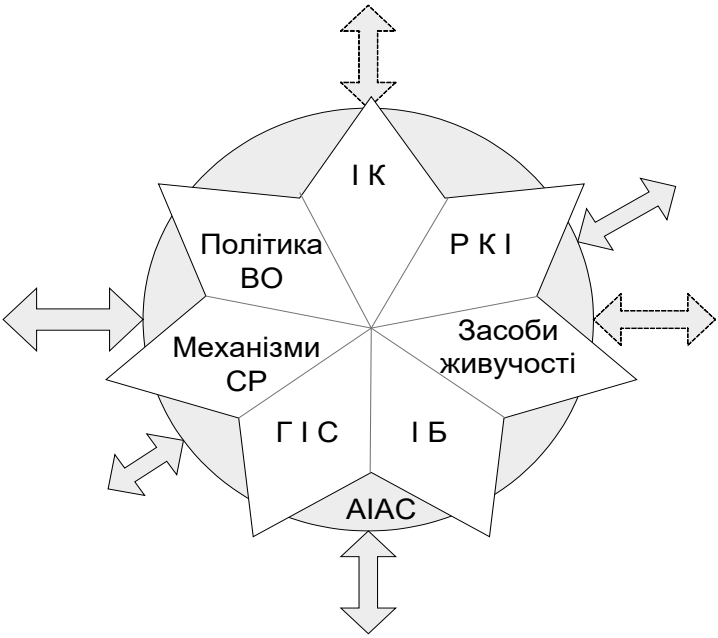

Рис. 4.6. Основні підходи до архітектури АІАС

4.2. Архітектура АІАС

Концептуальна структура АІАС. Враховуючи наперед задані умови, такі як множина функцій *F*, наявність елементів структури органу влади СА, RU_i, PU_j, MU_k, власне структуру СА, RU_i, MU_k, а також опис P_s', АІАС органу влади має створюватися як інструмент управління соціально-економічним розвитком галузі (регіону) та як система з домінуючою роллю аналітичних функцій, підтримкою стратегічного планування та розвитку. При цьому при створенні АІАС доцільно орієнтуватись не лише на конкретну організаційну структуру органу влади, а й на напрями його функціональної діяльності (з питань соціально-економічного розвитку, міжнародного життя, політичних проблем, внутрішньої політики та ін.). АІАС має розглядатися не просто як сукупність автоматизованих робочих місць, а як програмно-технічна система з інтерактивним режимом ведення інформації та надання її користувачам.

Підсумовуючи викладене, враховуючі постійні зміни складу органів державної влади та їхніх структур у результаті проведення адміністративної реформи, треба зазначити, що АІАС органу влади повинна будуватися як система з віртуальними функціональними підсистемами, що має забезпечити гнучку прив'язку до зміни організаційно-функціональної структури галузі (регіону) та до урахування особистого досвіду, поглядів і переваг керівних посадових осіб, що також змінюються, поєднуючи їх з об'єктивними методами та способами обґрунтування та підтримки прийняття рішень.

Таким чином, у загальному випадку структура АІАС розкривається такими компонентами, як система центрального апарату органу влади (CAS), системи його регіональних та місцевих органів управління (RUS_i), автоматизовані системи підвідомчих підприємств (PUS_j), а також окремі системи зв'язку та інформування пересувних засобів (MUS_k) (рис. 4.7).

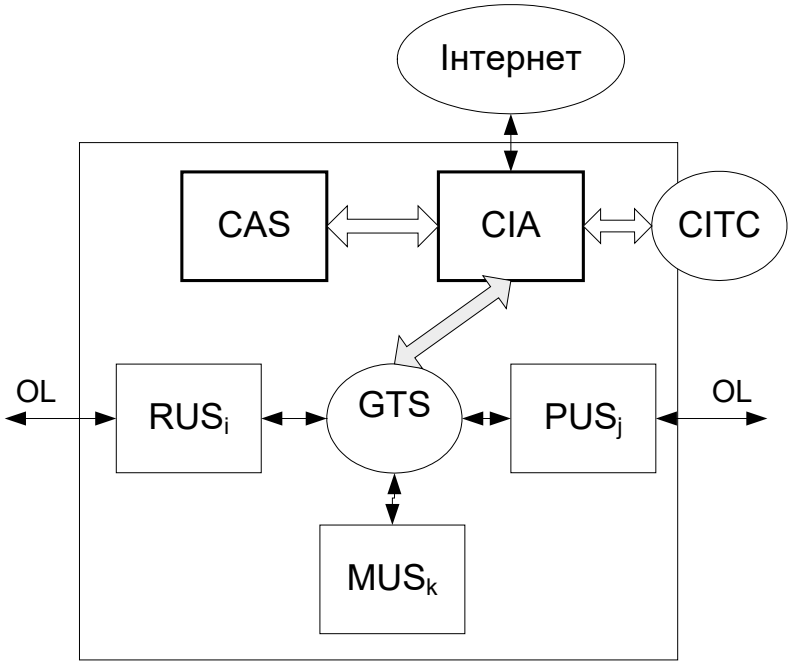

Рис. 4.7. Концептуальна структура АІАС

Враховуючи наявність автоматизованих компонент, у структурі АІАС вводяться ще дві складові. Перш за все, усі компоненти можуть бути пов'язані єдиним галузевим телекомунікаційним середовищем (GTS), яке забезпечує галузеву (корпоративну) взаємодію.

Крім того, згідно з обмеженнями штатного розкладу центрального апарату органу влади, для підтримки технології обробки інформації має бути створений окремий інформаційно-аналітичний центр (ІАЦ, CIA), у якому зосереджуються основні забезпечуючі функції, у тому числі система управління АІАС, підтримка комплексної системи захисту інформації (КСЗІ), а також комунікаційні можливості органу влади.

Діяльність ІАЦ як технологічна підтримка інформаційно-аналітичної діяльності має здійснюватися за такими напрямками: збір і ведення державних інформаційних ресурсів — оперативної, нормативної інформації та класифікаторів, проведення оперативного та ретроспективного аналізу інформації. До функцій ІАЦ може належати ведення веб-сайту органу влади (або галузевого порталу) як засобу відкритості та забезпечення електронного урядування.

Як вже зазначалось, АІАС функціонує у певному інформаційному середовищі, що складається з інформаційного простору органів влади держави та з глобального інформаційного простору. Засобами доступу до них є спеціальна інформаційно-телекомунікаційна система (СІТС), що об'єднує органи влади, та мережа Інтернет.

Серед вказаних компонентів головну роль як за обсягом перероблюваної інформації, так і за рівнем відповідальності за прийняті рішення відіграє центральний апарат органу влади. Саме в ньому зводяться усі інформаційні потоки і відбувається їхня остаточна аналітична обробка для забезпечення прийняття рішення. Ґрунтуючись на викладених даних і на досвіді створення інформаційних автоматизованих систем, структура системи центрального апарату подається як сукупність АРМів працівників різного рівня, тобто CAS = $\{ AFD_{if}, \ ASD_{js}, \ ACO_0, \ ACD_q, \ AIT_t, \ AMM_p \}$, що поєднані локальними інформаційно-обчислювальними мережами (ЛОМ) LAN_l, l = 1, 2, 3 (рис. 4.8).

Одна з мереж використовується для підтримки обміну таємною інформацією, друга — для внутрішньої Інтранет-мережі з забезпеченням вимог щодо захисту інформації, третя — для забезпечення доступу до відкритих інформаційних ресурсів, зокрема мережі Інтернет. Залежно від функцій органу владу кількість ЛОМ може бути й менше трьох.

Враховуючи, що система центрального апарату взаємодіє з усіма

трьома складовими телекомунікаційного середовища АІАС, а також наявність в інформаційно-аналітичному центрі власного комплексу АРМів, його структура визначається як

$$CIA = \{COM,\ WEB^{FE},\ WEB^{BE},\ ACC,\ AEK_r,\ AAD_d,\ AAW\}, \quad (4.2)$$

де COM — серверна структура для доступу до мережі GTS; WEB^{FE} — веб-сервер «переднього фронту»до мережі Інтернет; WEB^{BE} — веб-сервер «заднього фронту» до внутрішньої мережі Інтранет; ACC — абонентський вузол СІТС; AEK_r — АРМи експертів-аналітиків; AAD_d — АРМи адміністративного та обслуговуючого персоналу СІА; AAW — АРМи адміністрування КСЗІ.

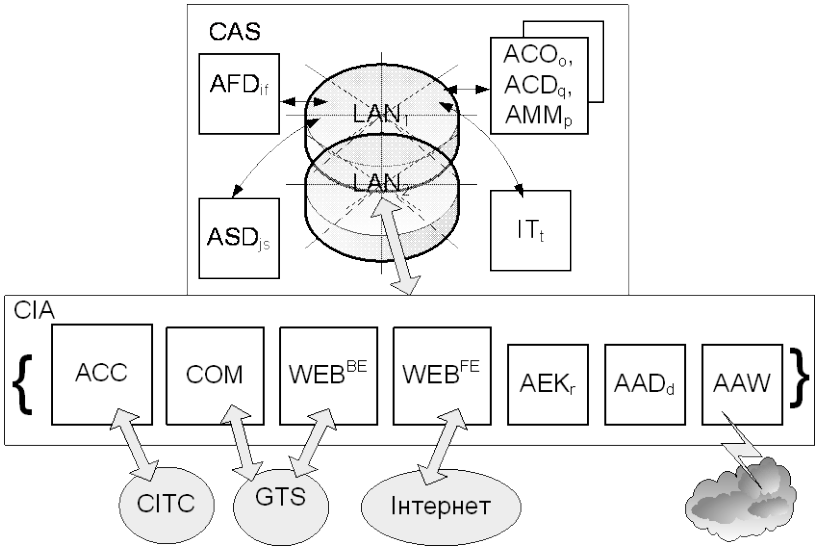

Рис. 4.8. Концептуальні структури систем центрального апарату та інформаційно-аналітичного центру АІАС

Структури систем регіональних і місцевих органів управління RUS_i фрактальні по відношенню до CAS та відрізняються зменшеною кількістю відповідних АРМів, а також рішеннями щодо серверів COM та ACC з урахуванням віддаленого доступу до GTS і СІТС.

Системи підприємств та об'єктів RUS_j, мають власні структури,

обумовлені виробничими та об'єктовими особливостями. Але до їхнього складу мають входити комунікаційні сервери COM для забезпечення доступу до мережі GTS.

Структури систем пересувних засобів інформування MUS_k містять АРМи керівника та обслуговуючого персоналу, а також засоби радіодоступу до GTS (рис. 4.9). Питання забезпечення інформаційної безпеки мають суттєве значення для пересувних засобів і повинні адмініструватись відповідним АРМом. При цьому АРМи та серверна частина мають бути реалізовані портативними засобами.

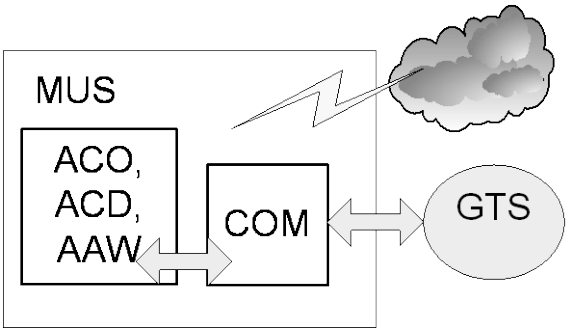

Рис. 4.9. Концептуальна структура системи пересувних засобів інформування

Визначення архітектури АІАС. Підсумовуючи викладене, слід зазначити, що архітектура АІАС визначається такими факторами:

1) характером інформаційно-аналітичної діяльності органу державної влади;

2) сучасними вимогами до відкритості урядових структур;

3) галузевою (територіальною) структурою;

4) необхідністю інтеграції АІАС до єдиної системи органів влади країни;

5) необхідністю забезпечення інформаційної безпеки АІАС і системи державної влади країни в цілому.

Обсяги та види інформаційно-аналітичної діяльності в органі влади визначаються функціональними обов'язками цього органу в системі державного апарату та пов'язаною із цим інтенсивністю інформаційного обміну, що показано у табл. 3.1.

Врахування у загальній структурі АІАС розподіленої структури відповідно до регіональних особливостей чи інфраструктури галузі зображено на рис. 4.7–4.9.

Ці дані обумовлюють присутність в АІАС необхідного компонен-

та, що матеріалізує перш за все процеси збору, перетворення, зберігання службової інформації (документів), а також процеси підготовки та прийняття рішень, контролю за їхнім виконанням (напрями 3, 1, 7 за табл. 3.1, рис. 4.3).

Цей компонент повинен мати властивості підтримувати бази даних документів (архівних і оперативних), навігаційно-пошуковий апарат, засоби перетворення форматів документів, відповідне лінгвістичне забезпечення. Засоби таких систем мають дозволяти однозначно визначити місцезнаходження, вид, доступність потрібного документа, мати стандартизований інтерфейс і забезпечувати ідентифікацію відправника шляхом обробки електронного цифрового підпису, підтвердження доставки адресату, відправки електронних документів в інші установи та можливості санкціонованого доступу до баз даних документів. Цим вимогам відповідають сучасні системи електронного документообігу (СЕД). Отже, першою базовою складовою АІАС має бути ***система електронного документообігу (ЕДО).***

Основна мета діяльності ОДВ — це виконання покладених на нього функціональних обов'язків (напрям 4 за табл. 3.1), тому суттєве місце у складі АІАС мають займати ***системи автоматизації функціональних задач (СФЗ)***.

Підтримка розв'язання функціональних задач та процесів прийняття рішень полягає у необхідності побудови моделей інформаційно-аналітичної діяльності, управління процесами аналітичних обчислень та інтеграції одержаних проміжних результатів у кінцеві показники (напрями 2, 5–8, 11 за табл. 3.1). Тому наступною складовою АІАС має бути ***система аналітичних обчислень (САО)***.

Підґрунтя для забезпечення розв'язання функціональних задач, аналітичної діяльності та електронного документообігу в АІАС утворює основна функціональна складова — ***система інформаційних ресурсів (СІР)***, яка має підтримувати структуровану й упорядковану інформацію у формі системи баз і сховищ даних різного рівня і призначення, що об'єднуються у складі розподіленої архітектури АІАС (напрями 1, 2, 10, за табл. 3.1). СІР має забезпечувати здійснення діяльності за такими напрямками, як збір та ведення державних інформаційних ресурсів — оперативної, нормативної інформації та класифікаторів, оперативний та ретроспективний аналіз інформації тощо. Головною проблемою у забезпеченні ведення СІР є вироблення єдиних правил структурування та кодування різнорідної інформації з метою її інтеграції, а також єдиних методичних підходів щодо використання й вибору

інформаційно-пошукових мов для складання запитів та індексування текстових документів.

Оперативна взаємодія систем АІАС і своєчасне та комплексне постачання необхідною інформацією має забезпечуватися наступною складовою — ***телекомунікаційним середовищем (ТС)*** (напрями 1, 5, 8, 10 за табл. 3.1, рис. 4.7–4.9). Основною вимогою до цією системи є забезпечення тривкого функціонування та спроможності зберігати свою дієздатність в умовах впливу різноманітних дестабілізуючих чинників, таких, як порушення основних каналів зв'язку та обладнання мережі, відсутність або неможливість використання резервних каналів, спроби несанкціонованого доступу до ресурсів мережі, зростання інформаційного навантаження на мережу.

Для забезпечення інформаційного обміну в рамках світового співтовариства АІАС повинна мати вихід на міжнародні і національні інформаційні системи і банки даних. Для цього в АІАС передбачається використання Інтернету, з одного боку, як засобу доступу до універсального простору інформаційних ресурсів, що являє собою всесвітня мережа, а з іншого, — як засобу «електронного уряду» для виконання оперативного обміну інформацією, звітності перед своїми громадянами через розміщення інформації про свою діяльність на веб-сторінках, взаємодії органу влади з громадянами при прийнятті законодавчих актів, на електронних референдумах, в електронних (комерційних) розрахунках тощо.

В АІАС інформаційна безпека та захист інформації набувають особливої ваги, враховуючи високий державний статус інформації, що обробляється (напрям 9 за табл. 3.1). ***Система захисту інформації (СЗІ)*** має вирішувати проблему комплексного забезпечення інформаційної безпеки АІАС, поєднання як програмно-технічних заходів, що запобігають або ускладнюють несанкціонований доступ до елементів мережі та до інформації, так і адміністративно-організаційних, спрямованих на створення належних умов безпечного функціонування та користування АІАС.

Особливого значення це має при використанні послуг Інтернету, де необхідно вирішувати питання захисту внутрішньої комп'ютерної мережі від зовнішнього втручання, використовуючи відповідні програмні та технічні засоби захисту мереж, мережні екрани.

В АІАС повинно забезпечуватись керування інформаційними взаємодіями, одночасного підключення до комунікаційних вузлів множини користувачів, захист від несанкціонованого доступу, система закон-

ного моніторингу та фільтрації інформації. При цьому має передбачатися фізичне відокремлення внутрішнього сегмента від Інтернету. Ці функції покладаються на ***систему управління АІАС (СУ)***, що реалізується в ІАЦ.

Важливою складовою частиною СУ АІАС повинна стати система централізованого керування корпоративною мережею. Загальний процес керування має розподілятися на такі основні компоненти, як керування ресурсами, збоями, конфігурацією, безпекою та обліком. Система керування мережею повинна забезпечувати централізоване адміністрування мережі, централізовану звітність про аварійні ситуації, а також реєстрацію подій у мережі.

Нарешті, ще одним завданням системи управління є реалізація функцій ситуаційного регулювання технологічного процесу опрацювання документів з використанням засобів АІАС.

У рамках інтегрованої системи органів влади (ІІАС) також передбачається створення єдиного телекомунікаційного середовища, інтегрованої системи електронного документообігу, інтегрованої системи інформаційних ресурсів, системи розподілених технологій аналітичних обчислень і системи інформаційної безпеки. Функцію спряження та забезпечення інтеграції в АІАС, як вказувалось, мають реалізувати інтеграційно-комунікаційні компоненти (ІКК), що підтримують доступ АІАС до інтегрованих ресурсів ІІАС.

Важливе місце займає також інтеграція АІАС в рамках міжвідомчих спеціалізованих систем, що забезпечують підтримку виконання важливих загальнодержавних функцій (наприклад, запобігання надзвичайним ситуаціям). До такої інтеграції залучаються лише певні органи влади (наприклад, у системі з питань надзвичайних ситуацій інтегруються 18 органів влади). Системи, що реалізують відпрацювання ***спеціалізованих міжвідомчих функцій***, позначимо $СМВ_m$, а компоненти, що реалізують спеціалізовану інтеграцію, позначимо $ІКК_m$, $m = (0,M)$.

Таким чином, вище описану архітектуру можна показати на рис. 4.10 та вважати базовою, що узагальнює всі можливі варіанти побудови систем конкретних органів влади.

В ІІАС передбачається також створення центру управління ІІАС, на який покладаються завдання управління доступом до розподіленого банку даних, обміном даними та електронним документообігом між органами влади, виконання аналітичних досліджень за міжгалузевими напрямками, управління та підтримка телекомунікаційного середовища ІІАС та ін.

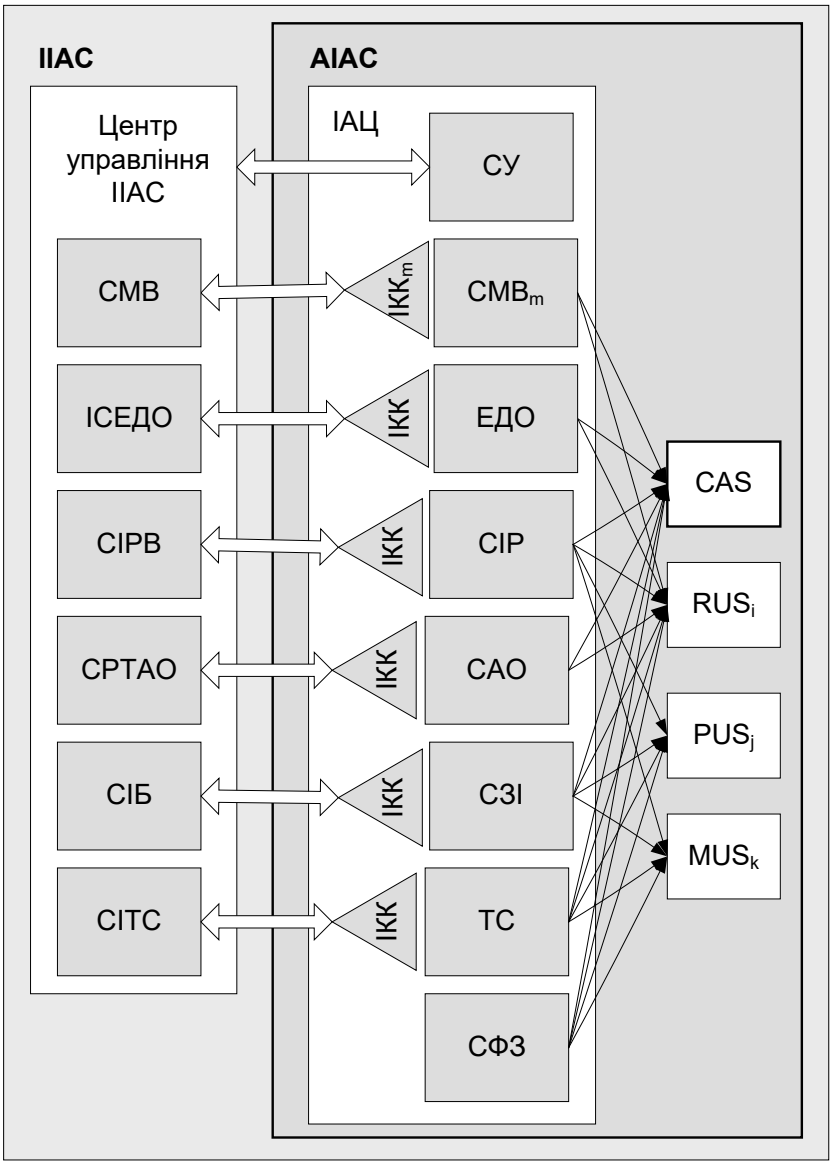

Рис. 4.10. Архітектурна схема АІАС з урахуванням взаємодії з ІІАС

Необхідно зазначити, що системи ЕДО, СІР, СФЗ, САО, СЗІ з відповідними інтеграційними компонентами, веб-сервери і ЛІОМ є тією

мінімальною сукупністю, що має бути створена у будь-якому органі влади. Інші компоненти є варіативними, їх наявність залежить від виду органу влади та масштабів галузі. Також від цього залежить і створення інформаційно-аналітичного центру.

Системи, що віднесені до постійних складових, також не можна вважати наперед заданими. Їх власна архітектура може змінюватись у широких межах. Так, наприклад, рішення щодо побудови ЛІОМ суттєво залежать від кількості абонентів мережі, а також розташування приміщень у будинку органу влади. А обсяги функціональних обов'язків органу влади, визначені його положенням, мають вирішальний вплив на структуру та кількість задач, що повинні розв'язуватись у СФЗ і САО. Тому визначення базових архітектур для кожної системи та їхніх варіативних складових є необхідним завданням.

Класифікація АІАС та архітектур. Згідно з характеристиками, отриманими в результаті аналізу інформаційних потоків із застосуванням методу ЗПМ, проведеного у третьому розділі, можна провести попередню класифікацію АІАС. Основу опису класу АІАС становлять сукупності ознакових моделей класу об'єктів, що складають ознакову модель класу АІАС. Для їх формування використовуються визначені у попередніх параграфах концептуальні структури органів влади, а також результати проведених досліджень [143, 188]. Результати виконаної класифікації з орієнтуванням на можливі структури органів влади записано в табл. 4.2. При цьому характеристики систем наведено в табл. 4.3.

Таблиця 4.2. Класифікація АІАС
з орієнтуванням на можливі структури органів влади

Клас АІАС	**Наявність елементів (систем)**				
	CAS	RUS_i	PUS_j	MUS_k	CMB
Перший	+	+	+	+	+
Другий	+	+		+	+
Третій	+	+	+	+	
Четвертий	+	+		+	
П'ятий	+		+		
Шостий	+				

Таким чином, використовуючи ці результати, можна провести остаточну декомпозицію АІАС на елементи — окремі системи, що забезпечують підтримку процесів із набору P_s' (рис. 4.11).

Таблиця 4.3. Опис класів АІАС

Клас АІАС	Опис класу
Перший	Окремі органи влади, що мають значну кількість функцій і розгалужену галузеву структуру, а також значну міжвідомчу взаємодію, що веде до високої інтенсивності інформаційного обміну, оперативності реагування та ін.
Другий	Те ж, що і клас «перший», за винятком розгалуженої галузевої виробничої структури
Третій	Те ж, що і клас «перший», за винятком міжвідомчої взаємодії
Четвертий	Органи влади, що не мають галузевої виробничої інфраструктури і сильної міжвідомчої взаємодії
П'ятий	Органи влади, орієнтовані на керування виробничою інфраструктурою
Шостий	Органи влади, що не мають галузевої структури і помітної міжвідомчої взаємодії

На рис. 4.11 зазначено інформаційні процеси з набору P'_s, а цифрами показано номери напрямів інформаційно-аналітичної діяльності за табл. 3.1, опрацювання яких забезпечується названими елементами. При цьому множина A активних елементів системи подається як {ЕДО, СІР, САО}. До множини E пасивних елементів системи варто віднести {СУ, СЗІ, ТС}. Зв'язки між елементами R реалізуються об'єктами класу 3.

Враховуючи ознакові моделі та опис класів АІАС (табл. 4.3), можна зробити висновок, що склад елементів за загальною схемою (рис. 4.11) є різним для різних класів АІАС (табл. 4.4).

Таблиця 4.4. Можливі структури АІАС

Клас АІАС	Наявність елементів				
	Центральна система			Телекомунікаційне середовище	
	ЕДО, СІР, САО, СЗІ	СМВ	ІАЦ	СІТС, Інтернет	GTS
Перший	+	+	+	+	+
Другий	+	+	+	+	+
Третій	+		+	+	+
Четвертий	+		+	+	+
П'ятий	+		+	+	+
Шостий	+			+	

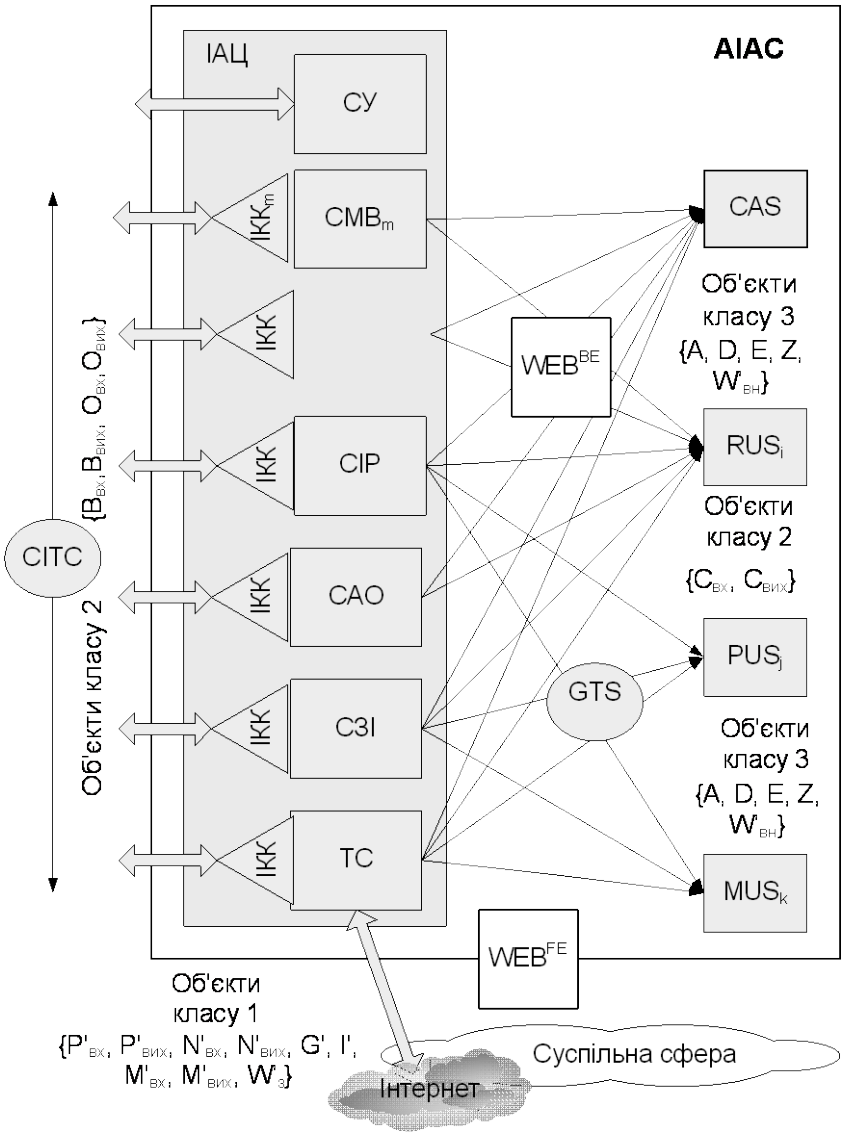

Рис. 4.11. Загальна схема елементів АІАС та їх взаємодії

Наведені в табл. 4.4 варіанти структур АІАС на перший погляд можуть здаватися майже ідентичними для усіх органів влади. Насправді кожна із складових може мати певний діапазон модифікацій.

Ці діапазони визначаються на основі інформаційного аналізу вхідних/вихідних інформаційних потоків і моделювання з метою забезпечення «виконавчої обов'язковості» та реалізації відповідної політики, дослідження специфіки інформаційного навантаження АІАС, що запропоновано у попередньому розділі.

При цьому слід враховувати, що найзагальнішим для всіх АІАС є наявність центральної системи, а утворення окремого ІАЦ — доцільним практично для всіх класів АІАС, окрім шостого.

Також телекомунікаційне середовище має утворюватись практично для кожного органу влади. Але якщо Інтернет та загальна мережа органів влади є обов'язковими складовими телекомунікаційного середовища будь-якого органу влади, то створювати власну корпоративну мережу доцільно для АІАС перших п'яти класів.

Масштаб застосування ЕДО значною мірою визначається інтенсивністю інформаційного обміну та рівнем міжвідомчої взаємодії і може мати три основні модифікації: 1) ЕДО1 — для 1-го, 2-го та 5-го класів АІАС; 2) ЕДО2 — для 3-го, 4-го класів; 3) ЕДО3 — для 6-го класу.

Модифікації СІР, САО та СЗІ визначаються масштабами галузі, наявністю виробничої інфраструктури та регіональних органів. Згідно з цим вони мають по дві основні модифікації: 1) СІР1, САО1, СЗІ1 — 1, 2, 3, 4, 5 класи; 2) СІР2, САО2, СЗІ2 — 6 клас.

Таким чином, для побудови повної інформаційної моделі АІАС і вибору модифікацій архітектури необхідно визначити у вигляді логічних виразів усі закономірності функціонування органу влади, а отриману інформацію про групи об'єктів (кластери), специфічні для досліджуваного рівня, об'єднати в кластерні бази даних (КБД). Далі на основі КБД розв'язуються задачі класифікації уточнених модифікацій складових АІАС.

Уточнення основних модифікацій здійснюється на основі набору значень ознак інформаційних потоків, що є визначальними для забезпечення напрямів діяльності конкретного органу влади. Також ці модифікації уточнюються з урахуванням результатів аналізу інформаційної взаємодії структурних підрозділів органу влади. Для цього можна застосувати методологію ЗПМ. Процес побудови ЗПМ та відповідний аналіз доцільно довести не лише до кожного підприємства (установи) галузі, а й до окремого робочого місця кожного працівника органу влади (державного експерта), що здійснює значний вплив на результати діяльності органу влади.

4.3. Оцінка ефективності архітектурних рішень

Питання оцінки ефективності запропонованих архітектурних рішень, зокрема щодо забезпечення інформаційної безпеки, на всіх стадіях життєвого циклу (розробка, створення, випробування, впровадження) системи є досить важливим, але настільки ж і складним, до того ж методологічно достатньо не опрацьованим, особливо для систем організаційного класу.

Згідно з ГОСТ 24.702-85 «Эффективность автоматизированных систем управления. Основные положения» ефективність АСУ визначають зіставленням результатів від функціонування АСУ й витрат усіх видів ресурсів, необхідних для її створення та розвитку.

Щодо систем органів влади, для них найчастіше відсутні такі кількісні критерії, як, наприклад, збільшення економічної ефективності від впровадження системи. Поширена методологія оцінки ефективності автоматизованої системи з точки зору вартісних витрат на її розробку і впровадження за критерієм вартісних вигод від впровадження більш економічної, порівняно з базовою, системи обробки даних, у випадку АІАС, в принципі, можна застосувати (якщо вдасться зібрати вихідні дані), але, ймовірно за все, очікуваний вартісний виграш буде незначним, або взагалі відсутній, або «вигаданий». Більш того, витрати на створення АІАС та підтримку її функціонування можуть бути значними і, скоріше за все, не будуть відшкодованими у грошовому виразі за доступний для огляду період.

При визначенні результатів від функціонування АСУ, згідно з ГОСТ, задають також універсальну систему узагальнених показників: оперативність (своєчасність), стійкість, якість управління й ін. Один з цих показників, що визначається організацією обслуговування користувачів і розраховується за такими основними параметрами, як ступінь відповідності відгуку інформаційної системи запитам і функціям, що реалізуються, зручності взаємодії користувача з системою, може бути оціненим лише в процесі експлуатації системи та проведення спеціальної експертизи. При цьому неможливо однозначно встановити кількісну оцінку кожного з чинників в умовах відсутності відповідних стандартів державної служби, а отже і критеріїв оцінки підвищення ефективності діяльності держслужбовців в умовах функціонування АІАС.

У наш час на заміну терміну «ефективність АСУ» прийшов більш ефектний термін «ефективність ІТ-інвестицій», для якого пропонується низка методик — традиційних фінансових (Return on Investment, Total

Cost of Ownership, Economic Value Added), імовірнісних методів (Real Options Valuation, Applied Information Economics), інструментів якісного аналізу (Balanced Scorecard, Information Economics) [189].

Фінансові методики потребують конкретних і точних даних, які по відношенню до автоматизації діяльності держслужбовців цілком підібрати майже неможливо. Перевагою імовірнісних методів є можливість оцінки ймовірності зниження ризику прийняття хибного рішення й появи нових можливостей (наприклад, прискорення опрацювання державних документів) за допомогою статистичних і математичних моделей. Тут також виникають труднощі, зокрема при оцінці впливу АІАС на якість рішення, яке залежить не лише від опрацювання документу в органі влади, але й від параметрів соціальної системи, її здатності досить точно відреагувати на державне рішення. Крім того, проекти АІАС у більшості органів влади взаємозалежні з ІТ-інноваціями в усій сфері державної влади, отже, відособлений, несистемний розрахунок ефективності таких проектів може стати безглуздим.

Що стосується оцінки іншого фактора ефективності АІАС — імовірності своєчасного, або навіть прискореного, а також якісного опрацювання документу — у цьому випадку оцінюють кількість помилок у підготовленому документі й трудомісткість їхнього виправлення. Однак для побудови таких моделей необхідно мати статистику про виникнення помилок та некоректних викладок у документах, збору якої в системі органів влади не приділяється уваги. Крім цього, при здійсненні подібного роду оцінок лишаються поза увагою інші ризики, наприклад, пов'язані з методами управління процесами опрацювання документів і прийняття рішень, що вказує на необ'єктивність оцінки з орієнтацією тільки на програмно-технічний аспект.

Перевагою якісних (евристичних) методів є реалізована в них спроба доповнити кількісні розрахунки якісними оцінками. Вони можуть допомогти оцінити всі явні та неявні чинники ефективності проектів АІАС і погодити їх із загальною стратегією розвитку органу влади. Ця група методів дозволяє фахівцям самостійно вибирати найбільш важливі для них характеристики ІТ залежно від специфіки діяльності органу влади, встановлювати між ними співвідношення, наприклад, за допомогою коефіцієнтів значущості.

Вагомим аргументом на користь застосування якісних методів є й те, що рішення про початок комплексних ІТ-проектів в органі влади значною мірою є політичним і більш підкоряється стратегічним планам

розвитку, ніж меті якнайшвидшого прискорення опрацювання документів і підвищення їхньої якості.

Основний недолік таких методів полягає в тому, що для їх ефективного застосування органу влади необхідно самостійно розробити власну детальну систему показників і впровадити її у всіх підрозділах по всьому ланцюжку опрацювання документів.

Крім того, існуючі методики, що базуються на експертних оцінках, згідно з державними рішеннями, результат багатьох з яких може проявитися через тривалий період часу — через роки, навіть десятиріччя, коли вже зміниться стан оточуючого середовища, не дозволяють отримати коректні оцінки, принаймні такі, яким можна довіряти.

Іншим негативним фактором є вплив суб'єктивної думки як на вибір системи показників, так і на експертні оцінки. Тому до фахівців, що зайняті цією справою, пред'являються особливі вимоги — вони повинні бути обізнані зі сферою ІТ, мати високий рівень знань в галузі інноваційного менеджменту і великий досвід роботи в органі влади.

Тут важливо зробити акцент ще на наступному: часто впровадження ІТ супроводжується реінжинірингом процесів діяльності. Уже давно визнано необхідність проведення в ході проектів автоматизації організаційних і культурних змін, наприклад, впровадження принципу наскрізного електронного документообігу із застосуванням електронного цифрового підпису. Тому, розраховуючи ефект від реалізації ІТ-проекту, ми визначаємо ефективність впровадження не тільки нової автоматизованої системи, але й нових принципів роботи, що далеко не те ж саме: перше передбачає автоматизацію (приводить до економії ресурсів), друге — організаційну інновацію (приводить до одержання нового знання, досвіду, нових методів). Отже, методика аналізу повинна мати властивість системності, дозволяючи виділяти із загального підвищення ефективності діяльності органу влади частину, пов'язану з реалізацією заходів конкретного ІТ-проекту як єдиного цілого, що зумовлює одержання синергетичного ефекту.

Що ж робити в цій складній ситуації? Зазвичай під ефективністю системи розуміють головну, основну характеристику якості, корисності системи, яка якісно або кількісно визначає її здатність виконувати свою основну функцію, що сприяє досягненню головної мети її застосування. Впровадження АІАС в органах влади впливає головним чином на підготовку управлінських рішень, і ефект полягає, перш за все, у своєчасності їхнього прийняття, або, як було раніше визначено, у забезпеченні виконання політики ВО. У дослідженнях щодо питань ефективності

АСУ існує вимога, що методика аналізу повинна дозволяти виділяти із загального підвищення ефективності діяльності підприємства ту частину, яка пов'язана із впровадженням нової інформаційної системи [190, 191].

Отже, показник ΔE, який визначає частку E, що вноситься засобами автоматизації в загальну ефективність E' діяльності органу влади, яка має визначатися вищим органом (наприклад, кабінетом міністрів), може стати відправною точкою (цільовою функцією) для проведення декомпозиції стратегічної мети на систему часткових показників $\boldsymbol{\Pi}$ оцінки ефективності АІАС.

При цьому, звичайно ж, важливо виходити з критерію співвідношення «ефективність–вартість», тобто враховувати матеріальні витрати Φ (капітальні й експлуатаційні) на автоматизацію (рис. 4.12).

Отже, формально показник ΔE може бути записаний у вигляді

$$\Delta E = (E' - E/\Phi)/E',$$

$$E = f(\boldsymbol{\Pi}). \qquad (4.3)$$

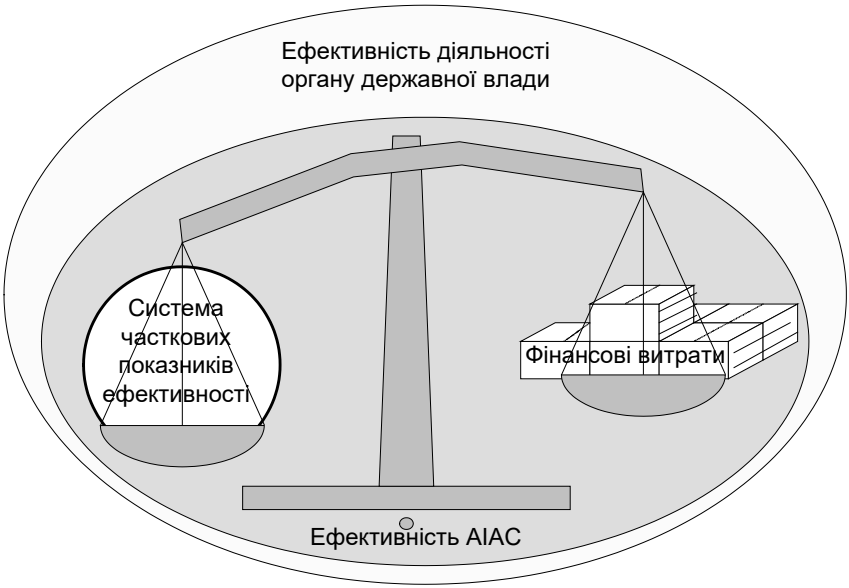

Рис. 4.12. Ефективність засобів автоматизації в загальній ефективності діяльності органу влади

До найбільш істотних часткових показників ефективності АІАС, які значною мірою впливають на реалізацію цільової функції та входять до множини ***П***, можна віднести такі: готовність, ємність, пропускну здатність, оперативність, якість рішення завдань управління, межі роботи, стійкість, експлуатаційну надійність, живучість, прихованість. Розглянемо сутність наведених показників.

Готовність АІАС — це ступінь її відповідності вирішенню завдань управління інформаційно-аналітичною діяльністю в будь-який момент часу. Кількісно цей показник оцінюється часом переведення засобів АІАС з одного ступеня готовності в інший, більш високий, що відповідає, наприклад, збільшенню інформаційного навантаження (переходу системи зі стану S_i до стану S_{i+1}), з однієї підмножини станів (зони ризику) до іншої. Час переведення АІАС до більш особливого режиму не повинен перевищувати часу переведення штату держслужбовців у готовність до ведення особливих дій (наприклад, до опрацювання термінових доручень вищих посадовців країни, зокрема у вихідні дні).

Ємність АІАС характеризує її граничні можливості при розв'язуванні завдань управління інформаційно-аналітичною діяльністю. Вона може оцінюватися різними показниками залежно від конкретних задач управління. Так, ємність АІАС з обробки інформації характеризується максимальною кількістю документів, за якими одночасно може здійснюватися прийом, пошук, обробка й видача інформації. Ємність АІАС може оцінюватися максимальною кількістю каналів одночасної взаємодії із зовнішнім середовищем (кількістю та інтенсивністю напрямків *ij* від даної АІАС$_i$ до інших АІАС$_j$ органів влади, що входять у сферу спілкування з органом влади, система якого розглядається). Вимоги до ємності АІАС в основному визначаються організаційно-штатною структурою органу влади, кількістю об'єктів зовнішнього середовища й очікуваним характером дій персоналу при розв'язанні проблемних ситуацій в особливий період.

Пропускна здатність АІАС характеризує її граничні інформаційні можливості при вирішенні завдань управління із заданою політикою виконавчої обов'язковості. Кількісно пропускна здатність АІАС може бути оцінена кількістю АРМів і серверного обладнання, способом (схемою) їх об'єднання, кількістю класів потоків документів та одночасно оброблюваних документів, швидкістю телекомунікаційних каналів, розподілом тривалості обслуговування і дисципліни обслуговування, циклом розв'язання конкретних задач за одиницю часу з певною дис-

кретністю й точністю, кількістю запусків розрахункових програм або трансакцій до бази даних за одиницю часу, пропускною здатністю каналів (які можна розраховувати, наприклад, за формулою (3.10)). При цьому беруть до уваги гіпотетичну інтенсивність навантаження $y(t_1, t_2)$, що надходить на систему за проміжок часу, та основні параметри навантаження (число джерел навантаження, середнє число викликів, що надходять від одного джерела навантаження за одиницю часу, середня тривалість заняття системи при обслуговуванні одного виклику). Доцільно також враховувати тяжіння між різними АІАС (див. (3.17), (3.18)).

Оперативність АІАС характеризує її швидкодію, тобто можливість системи реагувати на зміни оперативної обстановки. Кількісно оперативність системи може бути оцінена часовими витратами посадових осіб органу влади та технічних працівників, що обслуговують систему, при вирішенні управлінських завдань (так званий робітний час). Чим менше робітний час, тим вище швидкодія системи і тим вище її оперативність. Зменшення складових робітного часу без зниження якості вирішення завдань є одним з найважливіших напрямків щодо підвищення оперативності управління. Швидкодія системи залежить від ступеня автоматизації, рівня підготовки й злагодженості особового складу органу влади та його інформаційно-аналітичного центру.

Якість розв'язання задач управління в АІАС характеризує її можливості вирішувати поставлені завдання з необхідною повнотою, своєчасністю, вірогідністю й точністю. Кількісно цей показник оцінити найважче. Він може, наприклад, мати вираз у значеннях помилок розв'язання певної задачі і ймовірністю правильного її розв'язання, кількості несвоєчасно опрацьованих документів і хибних рішень. Для кількісної оцінки якості обслуговування можуть розраховуватися такі характеристики, як імовірність чекання для документу, що надійшов, імовірність чекання для будь-якого документа, що надійшов, понад встановлений час, середній час чекання стосовно усіх документів, що надійшли, і по відношенню тільки до затриманих документів тощо.

Межі роботи АІАС вказують на граничні значення характеристик оброблюваних і зображуваних нею об'єктів (документів) за форматами, розмірами, кольоровою гамою, периферійними засобами, що підтримуються, й ін.

Стійкість АІАС характеризується її здатністю протистояти впливу порушника безпеки й кількісно оцінюється ймовірністю функціонування при виході з ладу окремих її елементів.

Експлуатаційна надійність АІАС оцінюється ймовірністю її без-

відмовної роботи протягом певного часу, а також імовірністю її відновлення протягом заданого проміжку часу.

Живучість АІАС — властивість системи зберігати або швидко відновлювати свою функціональну здатність із вирішення завдань управління в складних умовах оперативної обстановки. Вона складається зі стійкості й експлуатаційної надійності.

До терміну «живучість» можуть належати й такі властивості АІАС, як її здатність одержувати інформацію від джерел за різними заздалегідь передбаченими варіантами, а також зберігати можливість управління підпорядкованими об'єктами в особливий період. У цілому живучість АІАС буде визначатися живучістю найуразливіших її елементів з точки зору здатності їх протистояти впливу порушника, а також ступеня резервування найбільш складних елементів АІАС у процесі її функціонування.

Прихованість АІАС — це здатність забезпечувати вирішення покладених на неї завдань при збереженні в таємниці від неавтентифікованих осіб циркулюючої в системі інформації, структури системи й місця розташування її критичних елементів.

Матеріальні витрати Φ на автоматизацію, що складаються з капітальних (асигнування на науково-дослідні та дослідно-конструкторські роботи зі створення АІАС, розробку технічних і програмних засобів, на закупівлю технічних і програмних засобів, на підготовку особового складу, на наступну модернізацію системи і її елементів) і експлуатаційних (витрати за весь термін експлуатації системи, включаючи витрати на утримання обслуговуючого персоналу, ремонт технічних засобів, придбання експлуатаційних і видаткових матеріалів), можна більшменш реально обрахувати. Вони, поряд з показниками $\boldsymbol{П}$, зазвичай виступають у вигляді техніко-економічних вимог до АІАС, значення яких задаються при розробці системи в технічному завданні на її створення.

Оцінку ефективності АІАС можна провести двома способами: на основі статистичних даних щодо реально діючої системи в умовах повсякденної діяльності органу влади (натурний експеримент) або на основі математичної моделі динаміки функціонування досліджуваної системи.

Основною перевагою першого способу є точність і об'єктивність одержуваних оцінок. Однак можливості оцінки «бойової» ефективності АІАС експериментальним шляхом досить обмежені. Натурний експеримент можливий тільки при наявності діючої системи. Тому його можна використовувати тільки на етапі модернізації АІАС. Експеримен-

тальне дослідження характеристик АІАС має такі істотні недоліки: надзвичайно висока вартість і трудомісткість проведення випробувань, неможливість створення аварійних ситуацій у системі, неможливість дослідження процесу функціонування АІАС в умовах імовірних порушень інформаційної безпеки.

Згідно з цим, основна увага при отриманні оцінок ефективності в процесі проектування АІАС приділяється дослідженню за допомогою математичного моделювання. Складність його використання полягає в тому, що в моделі необхідно коректно врахувати вплив автоматизованого управління на творчий процес опрацювання документів, підготовки й ухвалення рішення, що пов'язано із значною суб'єктивністю моделювання таких процесів.

Підсумки до розділу

Отриманні рішення та моделі АІАС дозволяють здійснити класифікацію відповідності АІАС із виділенням їхніх основних структурних елементів категоріям задач, які мають місце при обробці інформаційних потоків, для забезпечення розв'язання проблем прийняття рішень, беручи до уваги питання інформаційної безпеки, яка відрізняється врахуванням особливостей пріоритетності та дисципліни їхнього обслуговування, що дає можливість визначити особливості інформаційного навантаження.

Однією з концептуальних засад побудови АІАС в умовах функціонування *е*-уряду є безпека. На основі аналізу канадської моделі автентифікації визначено основні принципи реалізації безпечної архітектури взаємодії АІАС з населенням.

Склад компонентів архітектури для кожної АІАС визначається обсягами та видами інформаційно-аналітичної діяльності в органі влади, функціональними обов'язками цього органу в системі державного апарату та пов'язаними з цим інтенсивністю інформаційного обміну, структурними особливостями органів влади, вимогами до інтеграції АІАС, вимогами інформаційної безпеки.

Показник оцінки ефективності АІАС, що визначає частку, яку вносять засоби автоматизації в загальну ефективність діяльності органу влади, є відправною точкою (цільовою функцією) для проведення його декомпозиції на систему часткових показників $\boldsymbol{\Pi}$. При цьому важливо виходити з критерію співвідношення «ефективність–вартість».

РОЗДІЛ 5

МЕТОДОЛОГІЯ СТВОРЕННЯ ТЕХНОЛОГІЧНИХ ПІДСИСТЕМ АІАС

5.1. Сучасні інформаційні технології автоматизації інформаційно-аналітичної діяльності

За результатами наведених у попередніх розділах даних можна зробити висновок, що перш за все проектування та створення автоматизованих інформаційно-аналітичних систем органів влади є непростою задачею. Становище ускладнюється й тим, що при створенні подібної комплексної системи найчастіше треба виходити з вимог забезпечення вже існуючим окремим складовим частинам, локальним інформаційним системам у центральному апараті органу влади або на місцях в областях і районах можливості продовжувати виконувати власні функції, а також продовжувати вже розпочаті проекти створення чи модернізації локальних систем або додатків. Ураховувати вимоги інтеграції існуючих проектів у майбутню єдину систему дозволять такі принципи побудови АІАС, як єдність ближніх і дальніх цілей, проектування системи згори вниз, побудова — знизу догори. Але це потребує розробки укрупнених проектних рішень на всіх рівнях, причому таким чином, щоб отримані при цьому рішення не суперечили вимогам концепції системи та поточного і наступного проектування складових.

Ураховуючи комплексність створення в органах державної влади АІАС як систем збору, обробки, зберігання і передачі інформації, в основу методології використання ІКТ, як уже зазначалося, має бути покладена концептуальна стратегія інформаційного менеджменту, що є апробованою в досягненні ефективності діяльності окремих підприємств, їхніх об'єднань тощо, тобто в бізнес-секторі.

Також, розглядаючи архітектурні рішення, визначені у попередніх розділах, можна зробити висновок, що вони мають чимало спільного з сучасними інформаційно-аналітичними системами для управління підприємствами, де найчастіше створюються так звані корпоративні інформаційні системи — КІС (EAS — Enterprise Application Suite). Методиці створення таких систем як у нашій країні, так і за її межами присвячено безліч досліджень. Тому вважають ефективним спробувати застосувати ці результати при створенні АІАС в органах влади. Згідно з цим

доцільно провести короткий огляд рішень, що застосовуються для автоматизації бізнес-процесів на підприємствах.

Автоматизовані системи для управління підприємствами. Отже, у вказаній сфері розроблено вже чимало рішень, які базуються на автоматизації та інтеграції бізнес-операцій, об'єднаних в єдину систему. Це дозволило певним чином стандартизувати рішення на основі міжнародних рекомендацій, у результаті чого сформовано низку різних моделей процесів, які пройшли практичну апробацію.

Перш за все треба назвати системи менеджменту планування та управління (Management Planning and Control, MPC), об'ємно-календарне планування MPS (Master Planning Scheduling), а також системи, що дозволяють оптимально регулювати постачання комплектуючих у виробничий процес, контролюючи запаси на складі, які базуються на методології планування потреби в матеріалах MRP (Material Requirements Planning) [192].

Технологічним розвитком цих систем стали ERP-системи (Enterprise Resource Planning), які забезпечили автоматизацію перш за все бухгалтерського обліку і фінансів, комерційну діяльність, збут і розподіл продукції на основі інтеграції додатків, що працюють з єдиною комплексною базою даних [193]. Згідно з новими вимогами, до того, що маркетинг і планування продажу повинні бути безпосередньо пов'язаними з плануванням виробництва, зародилася нова концепція корпоративного планування і формування замовлень та оперативного управління технологічними процесами MRPII.

Зміна стратегії виробників в сторону фокусування процесу планування діяльності організації не на продукт, а на покупця, що, за задумом, має розширити можливості ділової активності, привести до збільшення продажів і ефективності бізнесу, створило нову модель керування діяльністю — планування ресурсів, синхронізоване з покупцем (CSRP — Customer Synchronization Requirements Planning). Методологія CSRP забезпечує підтримку повного життєвого циклу продукції — від її проектування з урахуванням вимог замовника до гарантійного й сервісного обслуговування після продажу.

Важливе місце при створенні систем управління займає питання інтеграції функцій, підрозділів та операцій, при цьому як інтеграційний чинник виступає якість (виробів, послуг) [194]. Використовуються такі концепції: користувачева ефективність системи (Usability), службові послуги (Outsourcing), інтеграція управління матеріалами та інформаційними потоками (Supply Chain Management), навіть створення підсис-

тем віртуальної реальності (Virtual Reality) для занурення експертів у проблемну сферу.

Залежно від ієрархії рівнів управління підприємством і інструменттами керування визначено відповідну класифікацію систем, а саме: системи стратегічного управління, системи управління ефективністю бізнесу (BPM-Business Performance Management/Corporate Perfor-mance Management), системи управління ресурсами підприємства (ERP-системи), системи управління взаємодією з клієнтами (CRM-системи), системи управлінського/бухгалтерського обліку та інші системи (Scada, CAD, CALS, PDM, PLM, CRM тощо).

Сучасні темпи розвитку бізнесу вимагають також прискорення прийняття управлінських рішень і підвищення рівня їх обґрунтованості та ефективності. З цією метою створюються спеціальні системи підтримки прийняття рішень (СППР). В умовах впровадження систем управління підприємством (наприклад, класу ERP) збільшити віддачу від них для підтримки прийняття рішень дозволяє інтеграція таких систем з геоінформаційними системами (ГІС). Геоінформаційна технологія є однією з передових інформаційних технологій, що стрімко розвивається та знаходить широке застосування. Як відомо, ГІС — це програмно-апаратний комплекс, який забезпечує збирання, відображення, обробку, аналіз і розповсюдження інформації про просторово розподілені об'єкти і явища на основі електронних карт, зв'язаних із ними баз даних і супутніх матеріалів.

Концептуально ГІС-технологія за своєю природою є універсальною й інтеграційною. Вона відображає реальний світ за допомогою інтегрованих у єдину систему й представлених у цифровому вигляді різних абстракцій — карт, наборів просторових даних (геоданих), візуальних схем робочих процесів, метаданих, моделей даних. Середовищем зберігання накопиченого знання про просторове оточення й керування цими абстракціями є база геоданих. А моделі даних відіграють роль своєрідних фільтрів, що забезпечують вибірковий доступ до узагальнених даних і їхнє ефективне використання. Можна стверджувати, що жодна інша технологія не може дати такого всеохоплюючого подання інформації як технологія ГІС. Завдяки цьому у сфері підтримки та прийняття управлінських і оперативних рішень інтеграція автоматизованих систем з ГІС породжує потужний аналітичний інструментарій опрацювання та подання інформації [194].

Застосування ГІС у цих напрямах в основному отримало розвиток і реально реалізоване в багатьох системах у світі на базі відповідних

програмних продуктів американського Інституту досліджень систем навколишнього середовища (ESRI). Універсальні можливості ArcGIS — сімейства комплементарних (що доповнюють один одного) програмних продуктів ESRI з інтеграції різних типів даних і документів — роблять його реальним і природним рішенням для побудови фундаменту інформаційної системи, що сприяє більш ефективному управлінню великими підприємствами і організаціями, стає технологічною платформою для створення корпоративних ГІС[59] (рис. 5.1).

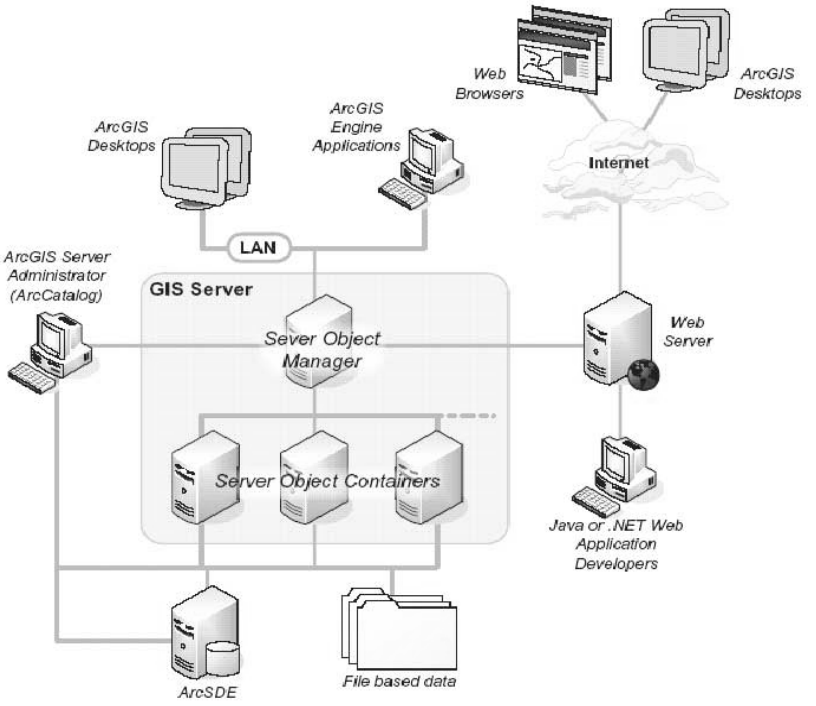

Рис. 5.1. Сімейство продуктів ArcGIS для побудови корпоративної інформаційної системи

Сформувалося також і уявлення щодо архітектури сучасних інформаційно-аналітичних систем бізнес-підприємств [195–198], до якої належать такі рівні, як збирання і первинна обробка даних; витяг, перетворення і завантаження даних; складування даних; представлення да-

[59] http://www.esri.com

них у вітринах даних; аналіз даних; веб-портал. У цілому вони будуються на базі клієнт-серверних рішень і поданні процесів у вигляді визначених інформаційних сервісів (рис. 5.2), що врешті веде до формування сервіс-орієнтованої архітектури (Service-Oriented Architecture — SOA).

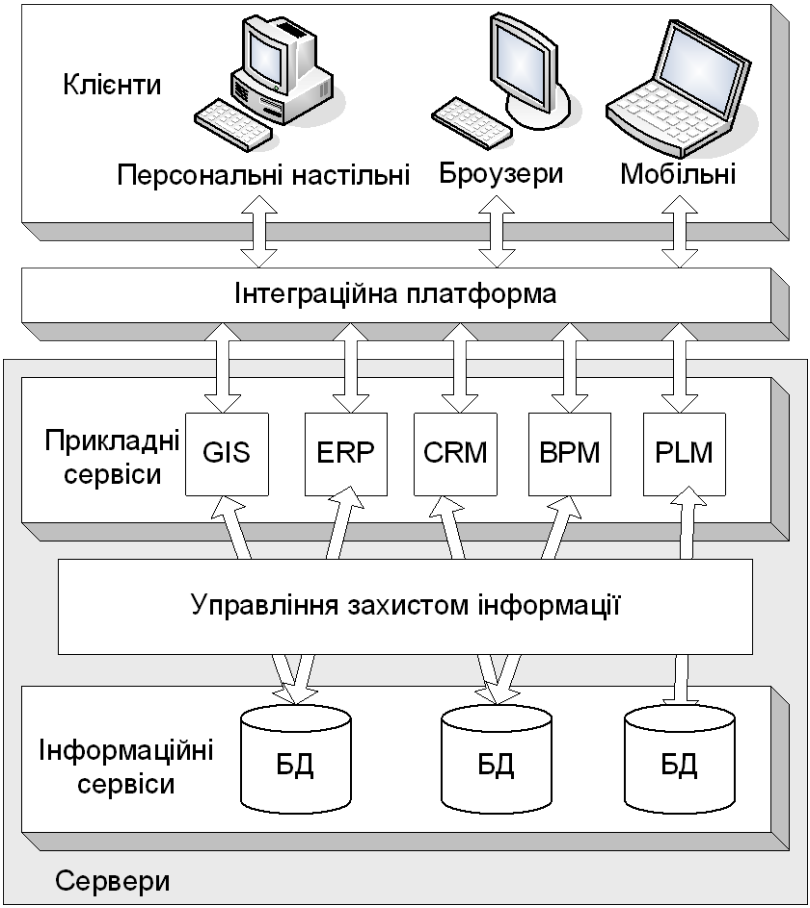

Рис. 5.2. Архітектура сучасних інформаційно-аналітичних систем бізнес-підприємств

Кожному з названих рівнів відповідають і певні технології, що підтримуються численними програмними продуктами багатьох компаній-розробників.

Усе більше значення та важливіше місце серед технологій починають займати системи захисту інформації та управління захистом (Security Management).

На рівні збору і первинної обробки даних використовуються джерела даних, які називаються транзакційними чи операційними джерелами (базами) даних, що є частиною так званих OLTP-систем (online transactional processing).

Процес витягу, перетворення і завантаження даних підтримується ETL-інструментами (Extraction, Transformation, Loading), призначеними для витягу даних з різних транзакційних джерел нижнього рівня, їхнього перетворення і консолідації, а також завантаження в цільові аналітичні бази даних — сховища даних (Data Warehouse — DW) і вітрини даних.

Застосування концепції сховища даних як предметно-орієнтованого, інтегрованого, незмінного, підтримуючого хронологію набору даних, організованому для цілей підтримки управління, розміщеному на кількох серверах БД у наш час є головним напрямом забезпечення підтримки інформаційної бази підприємства. У сфері створення засобів сховищ даних у світі існує чимало підходів і рішень — рішення компаній IBM, Oracle, Hewlett Packard, NCR, Informix Software.

Вітрини даних (data marts) призначені для проведення цільового ділового аналізу. Багатомірні вітрини організуються у вигляді багатомірних баз даних OLAP (Online Analytical Processing), де довідкова інформація подається у вигляді вимірів, а кількісна — у вигляді показників.

До сучасних засобів аналізу даних в ІАС відносяться програмні засоби, що мають назву інструментів ділового інтелектуального аналізу (Business Intelligence Tools), чи BI-інструменти.

На даний час бізнес-компанії активно починають впроваджувати різні Інтернет-технології, усе більше відчуваючи вигоду від використання цих рішень для підвищення ефективності свого бізнесу. Так, у системі mySAP, що відповідає вказаній концепції, реалізовано можливість взаємодії з клієнтом через Інтернет, а саме щодо приймання замовлення на веб-сайті (вибір продукції, розрахунок ціни, оплата, відстеження статусу й ін.). Практично всі гіганти цієї індустрії, такі як SAP[60], PeopleSoft[61], Baan[62] та інші, заявили про вихід Intranet-версій своїх програмних комплексів.

[60] http://www.mysap.com
[61] http://www.peoplesoft.com
[62] http://www.baan.com

Проведення інтелектуального аналізу даних із застосуванням програмних рішень не тільки в локальному середовищі, але й у середовищі Інтранет і Інтернет, з використанням веб-порталів, відкриває аналітикам нові можливості роботи з даними.

Найбільш популярними й такими, що добре себе зарекомендували, рішеннями для побудови порталів є WebShere Portal (IBM), SharePoint Server (Microsoft), Enterprise Portal (Jboss). Усі вони створені на основі сучасних масштабованих технологій, мають великий набір готових компонентів, і це зумовлює непросте завдання вибору базового рішення.

На сьогодні основними стандартами інтеграції на базі веб-сервісів, що застосовуються в універсальному середовищі комунікацій Інтернет, є 4 ключових стандарти:

1) публікація, пошук, використання сервісів (UDDI — Universal Description, Discovery and Integration);

2) мова опису функціоналів і інтерфейсів (WSDL — Web Services Description Language);

3) протокол доступу до об'єктів (SOAP — Simple Object Access Protocol);

4) універсальний формат даних (XML — eXtensible Markup Language, розширювана мова розмітки).

Ці стандарти підтримуються консорціумом W3C (World Wide Web Consortium), а також світовими промисловими компаніями (Microsoft, IBM). У достатній мірі зазначені вище тенденції пов'язані з розвитком концепції метамови XML. При цьому сучасний стан справ з підтримкою веб-сервісів XML характеризується лідерством компанії Microsoft[63] завдяки застосуванням платформи .Net.

Відповідаючи сучасним потребам, корпорація Microsoft також розробила «Рішення Microsoft для Інтранет» (Microsoft Solution for Intranets), що надає такі базові можливості, як забезпечення спільної роботи співробітників на базі веб-технологій, керування інформацією, організація електронного документообігу, а також проведення аудіо- і відеотрансляцій по корпоративній інформаційній мережі [199].

Як вже зазначалося, сучасні системи усе більше орієнтуються на підтримку бізнес-процесів, роблячи прозорими для користувачів рішення IT-інфраструктури. З'явилися продукти, що реалізують можливості управління бізнес-процесами та обміну повідомленнями між ними в гетерогенному середовищі. Одним із таких інтеграційних продуктів є,

[63] Джерело — «Gartner Research, October, 2002».

наприклад, Microsoft BizTalk.

В умовах використання комплексної IT-інфраструктури постає важливе питання контролю за її працездатністю та проходженням інформації, тобто керування інфраструктурою. Для вирішення цієї проблеми використали продукти локального застосування — такі як LAN-console, що забезпечує реєстрацію усіх дій, які відбуваються на робочій станції, також комплексні інструменти: TIGER — інтеграційна платформа управління, що базується на автоматичній проекції бізнес-функцій підприємства на його IT-інфраструктуру; Lancelot — система, що в режимі реального часу забезпечує збирання контрольної інформації з усіх елементів інфраструктури; Sybilla — система аналізу контрольних даних та передбачення з використанням нейронних мереж і фрактального аналізу; нарешті такі комплексні продукти, як, наприклад, Microsoft Solutions for Management.

Вирішення питань інформаційної безпеки в корпоративних автоматизованих системах з кожним роком набуває все більшої актуальності і знаходить, відповідно, більш ефективні технологічні рішення як у вигляді технічних засобів, програмної реалізації, так і у побудові комплексних систем захисту.

Цьому, перш за все, сприяє сформована модель побудови корпоративної системи захисту інформації, що заснована на адаптації Загальних Критеріїв (ISO 15408) та відповідає міжнародному стандарту ISO/IEC 15408 «Інформаційна технологія – методи захисту – критерії оцінки інформаційної безпеки», стандарту ISO/IEC 17799 «Керування інформаційною безпекою», а також спеціальним нормативним документам щодо забезпечення інформаційної безпеки, прийнятими в Україні, які враховують тенденції розвитку світової нормативної бази з питань захисту інформації.

З іншого боку, чимало світових брендів пропонують готові рішення для забезпечення корпоративної інформаційної безпеки. Так, наприклад, Microsoft пропонує міжмережний екран з інтегрованими сервісами ISA Server 2006, що дозволяє захистити IT-середовище підприємства від загроз, які надходять через Інтернет, одночасно забезпечуючи користувачам швидкий і безпечний віддалений доступ до додатків і даних. При цьому ISA Server 2006 забезпечує інтегровану безпеку, ефективне керування й швидкий, безпечний доступ до всіх типів мереж.

При створенні ІАС підприємства використовуються програмні рішення як різних фірм-виробників (змішані рішення), так і одного виробника (платформні рішення). Вочевидь, «коробкові» рішення приво-

дять до «клаптевої» автоматизації, ускладнюючи впровадження надалі інтегрованої системи. Тому перевага усе більше віддається комплексним платформним рішенням. Серед постачальників виділяються такі лідери, як Microsoft (рис. 5.3)[64], SAS, Oracle, SAP, PeopleSoft, Info Builders, Hyperion. Вирішальний критерій, що виділяє цих виробників, — наявність власної СКБД.

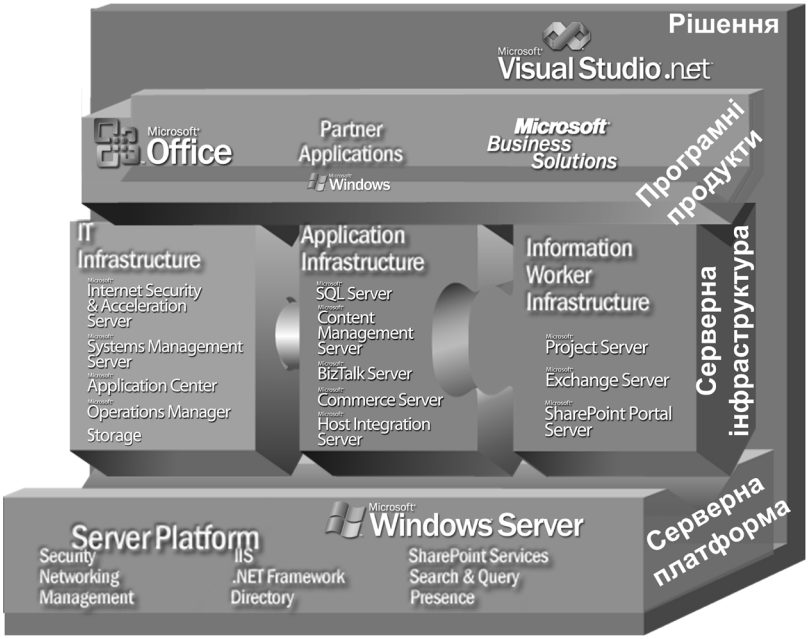

Рис. 5.3. Інтегрована платформа Microsoft

Останнім часом на ринку з'явилися та успішно працюють і вітчизняні постачальники комплексних рішень — «Парус:Предприятие», «1С:Предприятие», «ИТ-Предприятие», «Галактика», «Миратех», «Компас-Украина» та ін.

Питання вибору західної або вітчизняної системи враховує основні фактори, що істотно впливають на рішення — вартість програмного забезпечення і час його впровадження. Ці показники у західних постачальників зазвичай є вищими. Крім того, треба враховувати, що впровадження й освоєння великих західних систем пов'язане, насамперед, з

[64] Джерело — російське представництво Microsoft, Москва.

особливостями закладеної у них бізнес-логіки, орієнтованої на європейську бізнес-культуру, що не завжди прийнятно на наших підприємствах.

На сьогодні практично визначено і стратегічні цілі проектів інформаційних систем у бізнес-секторі, і тактичні плани їх впровадження. Так, у [200] наведено перелік етапів, які мають бути виконані для забезпечення ефективного впровадження: передпроектне обстеження з аудитом компанії та визначенням цілей і задач проекту, моделювання бізнесу з оцінкою повернення інвестицій, навчання фахівців групи впровадження, а також інші широко відомі етапи, аж до введення системи в промислову експлуатацію та післяпроектного обстеження і промислового аудиту.

Визначено й ключові фактори успіху, які пов'язані із ступенем комплексності рішень (рис. 5.4).

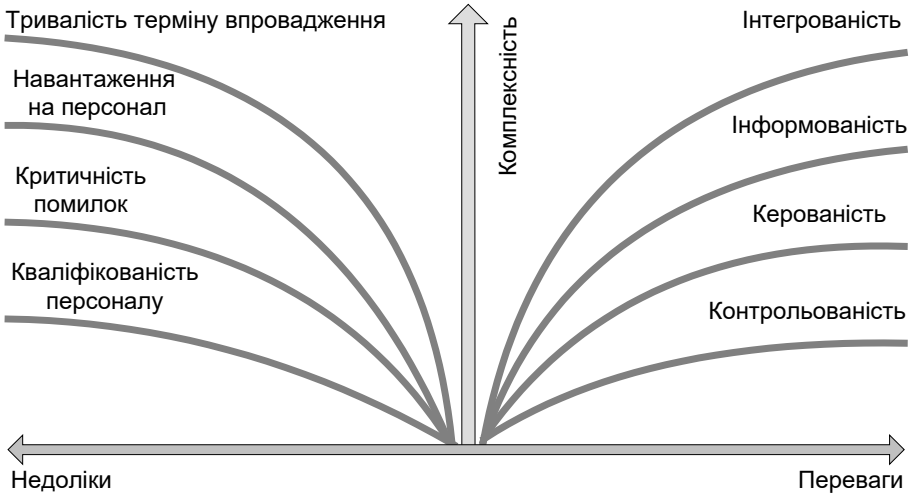

Рис. 5.4. Фактори, які пов'язані із ступенем комплексності рішень

Вони полягають у зростанні інтегрованості, коли всі підрозділи на підприємстві зв'язані одне з одним і при цьому не виникає необхідності багаторазового введення одних і тих же даних або звірення результатів, у збільшенні інформованості, коли всі необхідні дані для прийняття рішень доступні з єдиного сховища даних, у керованості підприємства завдяки формалізації бізнес-процесів, а також у забезпеченні широких можливостей для контролю за діяльністю персоналу, запобігання неса-

нкціонованих дій з їхнього боку, нарешті забезпечення належного рівня безпеки. На жаль, зворотний бік медалі має й низку негативних чинників, рівень яких також збільшується із зростанням ступеня комплексності. Впровадження комплексної системи автоматизації підприємства передбачає тривалий термін виконання робіт, що пов'язане із вимогами ретельної підготовки й пророблення рішень. При цьому зростає навантаження на персонал, адже в такій системі з'являється можливість обробляти більшу кількість трансакцій силами існуючого або навіть меншого за кількістю персоналу. Це вимагає наявності спеціально підготовленого та навченого персоналу, адже управляти підприємством і її бізнес-процесами при наявності системи комплексної автоматизації під силу тільки кваліфікованим фахівцям. В умовах колективної роботи зростає й критичність помилок, навіть однієї помилки. Користувачам системи доведеться усвідомити, що кожна їхня дія повинна бути ретельно продуманою з огляду на її вплив на інші етапи одного бізнес-процесу.

Таким чином, у сьогоднішніх умовах, враховуючи, що будь-який бізнес, щоб стати успішним, має навчитися швидко реагувати на постійну зміну ринкової ситуації, співробітники найбільш ефективних компаній використовують інструменти, які необхідні їм для систематизації і спільного використання інформації у рамках усієї організації, а також для одержання швидкого доступу до динамічно обновлюваної інформації.

Результатом цього є підвищення продуктивності праці і прискорення прийняття рішень. Створення веб-порталів, «універсальних установ» (one-stop shops), центрів телефонного обслуговування (call centers) прямо пов'язане з сучасними організаційними змінами в управлінні підприємствами [201]. При цьому ще раз треба звернути увагу на зміну стратегії виробників убік планування діяльності організації з оглядом, у першу чергу, на клієнта.

Методологічні підходи до використання інформаційних технологій в АІАС. Ураховуючи, що в сучасних умовах *е*-уряду державне управління зорієнтоване на клієнтське обслуговування громадян, орган влади певним чином можна уподібнити підприємству зі специфічними «бізнес-процесами» з обслуговування клієнтів. Як і на підприємствах, використання інформаційних технологій державними службами забезпечує комплексні послуги і допомагає краще розуміти своїх «клієнтів». При цьому можна зробити висновок, що певні техно-

логії автоматизованого управління підприємством можуть бути застосовані і в АІАС органу влади [202].

Таким чином, наведені в попередніх розділах чинники, зокрема вплив на органи влади множини інформаційних відношень, інтенсивність їхньої взаємодії, яка постійно зазнає змін у бік збільшення, а також стала тенденція до інтеграції інформаційно-аналітичних систем органів влади в єдину систему, характеризують вимогу створення в органах влади АІАС як комплексних корпоративних систем на базі апробованих рішень та інформаційно-телекомунікаційних платформ.

З методологічної точки зору такий підхід є досить доцільним. Цілком очевидно, що в сучасних ринкових умовах і в умовах відкритості сукупність правових, економічних, фінансових зв'язків поєднує підприємства та органи влади в єдине соціальне поле. При цьому відбувається суттєвий структурний вплив на органи влади, які зазнають значної перебудови у бік подальшої формалізації поточних, рутинних операцій та автоматизації експертних операцій. Підприємства, які значно гостріше, ніж органи влади, відчувають зниження ефективності своєї діяльності, розпочали подібний етап перебудови значно раніше. Тому досвід розробки і використання автоматизованих інформаційних систем на підприємствах має бути базою для методології створення АІАС в органах влади.

Отже, методологічні підходи до використання інформаційних технологій в органах влади мають базуватись перш за все на підтримці парадигм відкритості та адаптивного органу влади, а також на використанні досвіду, набутому при створенні та розвитку методології автоматизації управління підприємствами. Отже, складовими загальної методології мають бути такі чинники:

а) забезпечення підтримки автоматизованих процесів єдиною інтегрованою системою;

б) об'єднання додатків з інформаційними ресурсами;

в) рішення на базі відкритих стандартів;

г) надання онлайнових послуг;

д) автоматизація («електронізація») документообігу;

е) забезпечення спільної роботи над документами на базі Інтернет-технології з використанням внутрішнього («корпоративного») веб-порталу;

є) віртуалізація робочого середовища експерта (держслужбовця);

ж) застосування безпечної архітектури;

з) використання інтелектуальних карток.

Головним же методологічним підходом має бути вимога формування ефективної архітектури системи на основі міжнародного досвіду шляхом об'єднання всіх підходів (рис. 5.5)[65].

Рис. 5.5. Етапи формування ефективної архітектури системи

З урахуванням викладеного визначимо основні напрямки побудови АІАС за наступним переліком стереотипних функцій інформаційно-аналітичної обробки даних.

1. Оперативний аналіз інформації — оперативне інформування, фактологічне інформування, контент-аналіз для побудови інформаційних вибірок та отримання довідкових матеріалів шляхом інформаційного пошуку за індексами документів, KWIC- та KWOC-показниками або поглибленого інформаційного пошуку в повнотекстових базах, використання класифікаторів, довідників і словників, доступ до інформаційних ресурсів спільного користування.

2. Ретроспективний аналіз інформації — статистичний аналіз, картографія, добування закономірностей (прихованих чи неявних) з великих масивів дослідних даних (Data mining, Knowledge discovery).

[65] Gartner, Meta, Giga, MIT.

3. Системно-аналітична діяльність — моніторинг, аналіз та прогнозування, моделювання об'єктів і процесів, ділові ігри, експертний аналіз, організація опитування населення та оцінювання громадської думки.

4. Планування — довгострокове (зі значною часткою прогнозування і передбачення), середньострокове, оперативне.

5. Повсякденна внутрішня діяльність — бухгалтерський облік, матеріально-технічне забезпечення, господарче управління, управління кадрами, правове забезпечення, діловодство та документообіг, підтримка редакційно-видавничої діяльності.

Перший напрям в органах влади зараз найбільш розвинений та вже має певну технологічну інфраструктуру. Одначе рівень оперативного інформування значно залежить від накопичених в ОДВ інформаційних ресурсів, насамперед загальнодержавного користування. Тому у цьому напрямку йдеться про перехід від OLTP-баз даних до інформаційних сховищ, де можуть застосовуватися методи аналітичної обробки даних, наприклад, OLAP-методи, власні інформаційні вітрини (Data mart) та єдине інформаційне сховище (Data warehouse). Особливо це стосується БД міжвідомчих систем, наприклад, для складання та виконання Держбюджету країни. Також за цим напрямком більшої уваги слід приділяти контент-аналізу та фактологічному інформуванню.

Технології першого напрямку є інструментом репрезентативних вибірок інформації для інтелектуальної аналітичної діяльності за другим, третім та четвертим напрямками. Кількість задач в органах влади, що потребують таких методів, є чималою і вже існують позитивні приклади використання методів системного аналізу та математичного моделювання об'єктів і процесів в органах влади.

Що стосується п'ятого напрямку, то тут задачі менш складні і чимало вже робиться, наприклад у бухгалтерському обліку (на основі «1С:Бухгалтерія», MS Excel), в управлінні кадрами (з використанням СКБД загального користування), а також у веденні електронних картотек документів на основі готових рішень постачальників.

І на останок слід звернути увагу на особливості створення й впровадження АІАС в органах влади. Впровадження системи автоматизації управління призводить до серйозних перетворень в організації, тому воно є складним і хворобливим процесом.

Одним із найважливіших етапів проекту впровадження АІАС є повне й достовірне обстеження органу влади у всіх аспектах діяльності, його оцінка з погляду на те, чи можливо взагалі впроваджувати у ньому яку-

небудь систему. Адже впровадження АІАС вимагає суттєвого перегляду внутрішньої логіки роботи держслужбовців, перебудови існуючої системи опрацювання документальної інформації, пристосування нормативної бази до роботи в нових умовах. У випадку поганої організації «бізнес-процесів» в органі влади подальша автоматизація спричинить тільки погіршення ситуації.

Звичайно, можна автоматизувати все «як є». Але, зазвичай, у результаті обстеження виявляються причини необґрунтованих затримок в опрацюванні документів, а також протиріч та дублювань в організаційній структурі, усунення яких дозволяє істотно скоротити час виконання бізнес-процесів та збільшити якість інформації для підтримки прийняття рішень.

Широковідомим є тезис, що не можна автоматизувати те, чого немає (або не слід автоматизувати безладдя). Відсутність чіткого управління (менеджменту) в органі влади не дозволяє коректно поставити задачі його автоматизації. Звичайно, це в першу чергу філософські й психологічні аспекти, адже більшість керівників управляють своїми підрозділами тільки спираючись на особистий досвід, інтуїцію й власні уявлення, а також досить неструктуровані дані про стан питань, що розглядаються. Необхідно пам'ятати про співвідношення «80/20»: система автоматизації — це на 80 % менеджмент і тільки на 20 % — технології. Тому для успішного впровадження АІАС необхідно максимально формалізувати всі ті контури управління, які планується автоматизувати.

Крім того, автоматизовані системи для органів влади не існують у вигляді коробкових рішень, а їхнє впровадження здійснюється поетапно і є дуже трудомістким, оскільки потрібно виконувати настроювання множини неочевидних параметрів, проводити «реінжиніринг» і навчання користувачів. Із-за того, що цикл впровадження може займати кілька років (а іноді й більше), рішення та обладнання системи за цей час морально застарівають, не встигаючи за розвитком технологій.

Говорячи про створення АІАС, варто розрізняти розроблювачів системних рішень і консалтингові компанії, які безпосередньо впроваджують систему, надають консультаційні послуги й займаються технічним супроводом. Тому виникає ще одне питання — зупинитися на розроблювачі або консультанті? Перевага безпосередньої роботи з розроблювачем полягає в тому, що облік специфічних бізнес-процесів і їхнього «відтворення» в АІАС реалізуються набагато швидше, ніж при роботі з консалтинговими компаніями, які, наприклад, не є власниками вихідного програмного коду.

Отже, у подальших параграфах наведено основні вимоги та методологія застосування інформаційних технологій в АІАС, базою для визначення яких є запропоновані методологічні підходи, а також результати, розглянуті на попередніх сторінках. Розширений опис застосування сучасних ІКТ в АІАС наведено в [129].

5.2. Основні вимоги до інформаційного забезпечення та систем зберігання даних в АІАС

Інформаційні потреби органів влади ґрунтуються на необхідності інформаційної підтримки їхнього функціонування та аналітичної діяльності, а також організації взаємодії АІАС органу влади з іншими ІАС. Тобто інформаційне забезпечення АІАС призначене виконувати три основні функції:

1) забезпечення функціональних та аналітичних задач АІАС необхідними даними;

2) забезпечення фахівців — користувачів АІАС довідковою інформацією;

3) формування спільних інформаційних ресурсів органів влади, зокрема для інформування населення.

Водночас, згідно з наведеним описом слід зазначити, що інформаційне забезпечення АІАС суттєво залежить від стану створення та організації використання в державі *інформаційних ресурсів*.

Проблеми формування і використання національних інформаційних ресурсів. Принципове поняття ***інформаційні ресурси*** визначають як документовану інформацію, що зберігається в різних інформаційних системах (комп'ютерних базах і банках даних, бібліотеках, архівах, інформаційних сховищах і т.ін.). При цьому під документованою розуміється інформація, зафіксована на матеріальному носії з реквізитами, що дозволяють її ідентифікувати[66].

Певні інформаційні ресурси в державі набувають статусу ***національних***. Це, у першу чергу, інформаційні ресурси, які містять інформацію з різноманітних аспектів діяльності органів державної влади і місцевого самоврядування, а також юридичних осіб і громадян, що відповідають визначеним вимогам до структури й утримання і зареєстровані у відповідності з регламентованою процедурою. Наприклад, найбільш

[66] Ринок друкованої, теле- і радіопродукції, а також діяльність державних і інших засобів масової інформації не є предметом даного дослідження.

розвинутою в країні є сфера національних ресурсів науково-технічної інформації [203, 204].

Серед комплексу заходів, що мають забезпечити розвиток національних інформаційних ресурсів, а саме: удосконалення нормативно-правової й методичної бази формування, обліку, використання і захисту інформаційних ресурсів, розвиток інфраструктури інформаційних ресурсів передбачає формування ***сист еми інформаційних ресурсів органів держ авної влади (СІРВ)*** як вагомої складової сучасної інформаційної інфраструктури [205, 206].

Формування СІРВ має неабияке значення в першу чергу для забезпечення функціонування АІАС, а також для забезпечення інтеграції цих систем в ІІАС, у якій інформаційні ресурси органів державної влади є найважливішими інтеграційними компонентами.

Водночас слід зазначити, що СІРВ є важливішою складовою й системи «електронного уряду», яка забезпечує наявність електронних інформаційних ресурсів для підтримки всіх процесів, що мають місце в повсякденній діяльності органів державної влади у взаємодії з населенням.

Отже, основні вимоги до формування й використання національних інформаційних ресурсів (НІР) суттєво впливають також на розвиток СІРВ. Крім того, формування системи управління НІР для України на даному етапі її розвитку є стратегічним напрямом і потребує від органів державної влади вирішення проблем, що виникають, з єдиних методологічних позицій.

Аналіз стану інформаційних ресурсів країни визначає множину проблем, які у своїй більшості є загальними й для сфери формування і використання інформаційних ресурсів в органах влади. Серед чинників, що системно впливають на цей комплекс проблем, слід відзначити такі:

а) переважно галузевий (відомчий) принцип інформатизації, що призводить до формування інформаційних ресурсів, орієнтованих, як правило, на задоволення потреб обмеженого кола користувачів;

б) відсутність у державних органах та організаціях спеціалізації на ведення масового інформаційного обслуговування користувачів;

в) неузгодженість і несумісність форматів даних, які зберігаються в різних інформаційних системах, несумісність регламентів і технологій їхнього відновлення, використання різних класифікацій і інших лінгвістичних засобів, що призводить до неоднозначності і суперечливості інформаційних ресурсів різних відомств, неможливості їхнього спільного використання і взаємодії при вирішенні міжгалузевих задач;

г) відсутність єдиних правових норм, які регулюють доступ до державних інформаційних ресурсів, регламентують порядок передачі і використання інформації про діяльність органів державної влади, підприємств і організацій у відкритих мережах і відповідають вимогам інформаційної безпеки.

Ці та інші проблеми в сфері формування і використання НІР, аналіз їхніх причин свідчать про необхідність зміни пріоритетів у державній політиці в цьому напрямку. Забезпечення формування умов виробництва, збереження, поширення і комплексного використання усіх видів інформаційних ресурсів, вільного доступу до них з боку громадян і організацій будь-якої форми власності, в остаточному підсумку підвищення ефективності діяльності підприємств і організацій, органів державної влади і місцевого самоврядування — в цьому власне має полягати суть державної політики в сфері НІР. Вона також повинна враховувати можливості міжнародного співробітництва у сфері інформаційних технологій, продуктів і послуг, реальні можливості вітчизняної інформаційної індустрії.

Комплекс заходів для забезпечення розвитку НІР доцільно здійснювати шляхом реалізації державної програми формування Системи національних інформаційних ресурсів (СНІР). Розпорядженням Кабінету Міністрів України від 5 травня 2003 р. № 259 затверджена «Концепція формування системи національних електронних інформаційних ресурсів», згідно з якою до основних напрямків створення СНІР відносяться й створення інформаційних ресурсів органів державної влади.

Слід зазначити, що взагалі основою для формування СНІР як системи мають бути АІАС. Для цього потрібне вирішення складних організаційно-технічних питань, пов'язаних із забезпеченням скоординованого формування та ведення державних інформаційних ресурсів органами влади. Це стосується, в першу чергу, тих органів державної влади, що мають у своєму розпорядженні розвинуті територіально розподіле-ні інфраструктури, орієнтовані на збір інформації по всій території України.

Для забезпечення формування, використання і захисту інформаційних ресурсів державного сектора та їх застосування в інтересах держави та суспільства в цілому потрібно провести управління державними інформаційними ресурсами, обов'язковість реєстрації державних інформаційних ресурсів у національному реєстрі інформаційних ресурсів (НРІР) як комплексу взаємопов'язаних заходів органів державної влади, установ та організацій [207].

Необхідно також встановити офіційний порядок обліку державних інформаційних ресурсів, організувати звітність державних організацій про їх використання перед органами державної влади. Облік і контроль використання інформаційних ресурсів повинні базуватися на офіційно встановленому переліку показників.

Інфраструктура СНІР містить у собі такі компоненти (рис. 5.6), як організаційні структури, що забезпечують поточну підтримку і розвиток функцій збору, опрацювання, збереження, поширення, обміну, пошуку і передачі інформації, а також структури, що забезпечують інформаційну взаємодію виробників і споживачів інформаційних ресурсів, продуктів і послуг, реалізацію доступу до інформаційних ресурсів і продуктів, спираючись на сучасні інформаційні технології, програмно-технічні комплекси, лінгвістичні засоби і правові норми регулювання інформаційних відносин.

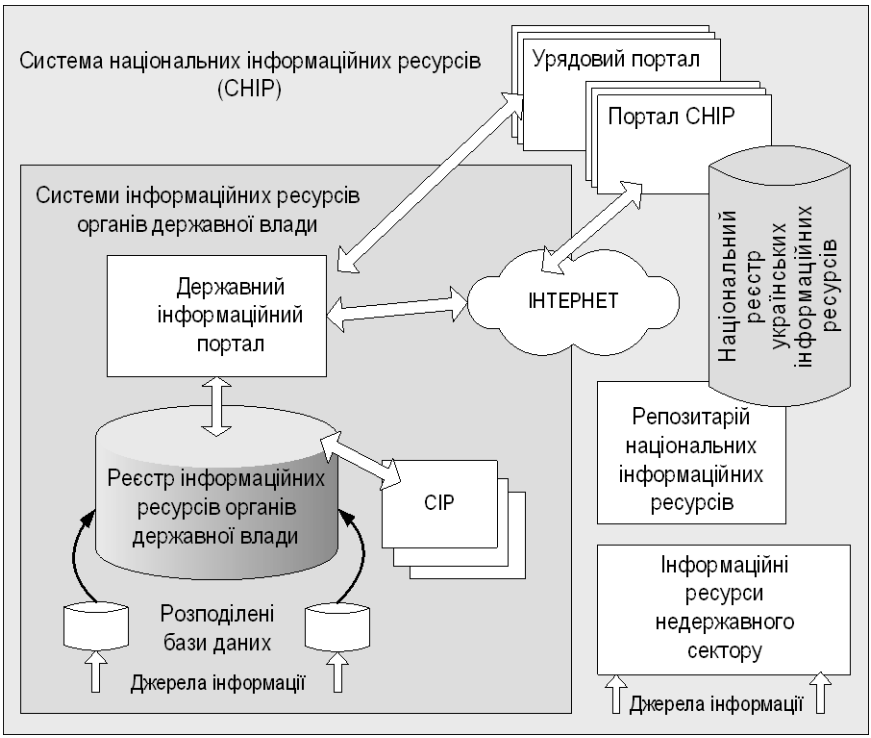

Рис. 5.6. Інфраструктура системи національних інформаційних ресурсів

Інформаційно-аналітичні центри органів державної влади, інші інформаційні служби міністерств і відомств разом з інформаційними службами державних адміністрацій міст і районів, соціальної, індивідуально-побутової і правової сфери (наука, освіта, культура, засоби масової інформації, охорона здоров'я, соціальне забезпечення і т.ін.) мають складати організаційне і технологічне ядро інфраструктури СНІР.

Пріоритетами в застосуванні повинні користуватися технології Інтернет/Інтранет, а також технології, які ґрунтуються на ідеології інформаційних сховищ, технології створення інформаційних ресурсів на сучасних носіях інформації, розвинуті системи графічних і текстових редакторів, ГІС-технології.

Складовою частиною національної безпеки України є інформаційна безпека. Забезпечення інформаційної безпеки національних інформаційних ресурсів є обов'язковою умовою при включенні їх до СНІР. Склад основних заходів повинен відповідати вимогам щодо забезпечення захисту інформації на кожному з етапів її виробництва, обробки і збереження, визначених законодавством і підзаконними нормативними актами компетентних органів державної влади.

Структура системи інформаційних ресурсів органу державної влади. Створення систем інформаційних ресурсів (СІР) АІАС і СІРВ в цілому має відбуватись з орієнтацією на інтеграцію в складну інформаційну структуру (див. рис. 5.6), центральною ланкою якої є Єдиний урядовий веб-портал. При цьому, як це видно з рисунку, СІР органів влади є складовими СІРВ, яка в свою чергу є складовою СНІР.

СІРВ передбачає наявність таких структурних компонент, як державного інформаційного порталу; реєстру інформаційних ресурсів органів державної влади (РДІР); різних джерел інформації, а також функціональних вузлів СІР ОДВ [205].

Функціональні вузли СІРВ в органах влади (рис. 5.7), перш за все, мають відповідати положенням, наведеним у попередньому параграфі. Крім цього, вони забезпечують формування інформації про власні ресурси для включення до РДІР.

Як передбачалося вище, головною складовою СІР має бути інтегрований банк даних (ІБД) як ядро сховища даних, що має містити локальні бази даних, у яких розташована необхідна для функціонування ОДВ інформація. Інформаційний ресурс СІР формується переважно за рахунок неструктурованих даних, у тому числі завдяки вибору інформації з мережі Інтернет. При цьому взаємозв'язок інформаційних еле-

ментів системи здійснюється за допомогою телекомунікаційних засобів обміну, формуючи таким чином розподілений банк даних СІРВ.

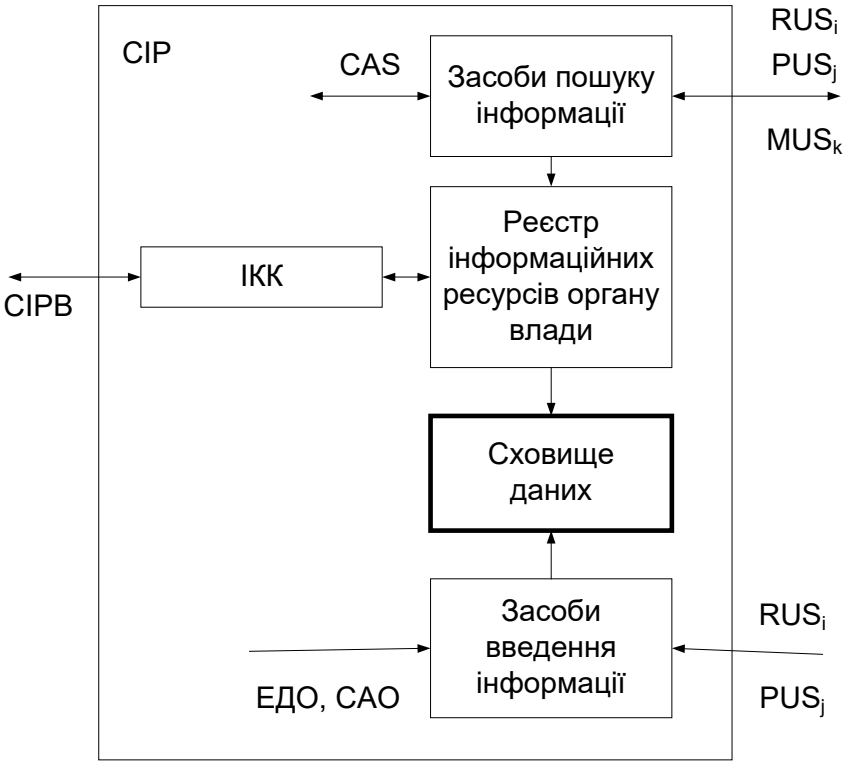

Рис. 5.7. Загальна структура СІР

До складу інформаційного забезпечення також має входити уніфікований набір первинних документів; системи класифікації та кодування; нормативно-довідкова інформація; проблемно-орієнтована база даних; технічна, нормативно-методична та інструктивна документація.

Враховуючи значну кількість інформаційних потоків, що опрацьовуються органом влади, технологія збору та накопичення інформації в СІР ОДВ має передбачати її одноразове введення, формалізацію передачі при інформаційному обміні між структурними компонентами (рис. 5.8), а також необхідну й допустиму, з урахуванням рівня доступу, інтеграцію як у межах усієї СІРВ, так і в межах окремих функціональних ланок.

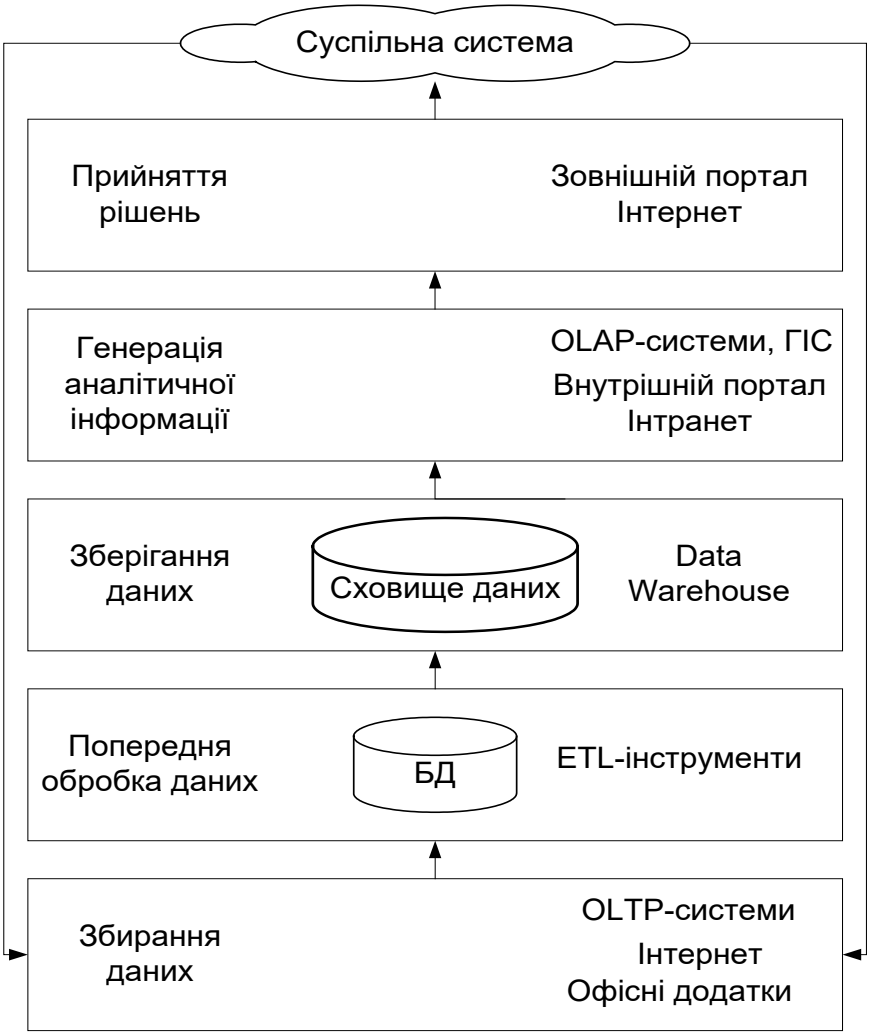

Рис. 5.8. Загальна схема проходження інформації в АІАС

Дублювання інформації в інформаційних фондах компонентів системи здійснюється як технологічний засіб наближення інформації до її безпосереднього користувача. Інформаційною основою необхідної інтеграції даних у межах СІРВ повинні стати типові елементи лексичного та лінгвістичного забезпечення, які використовуються в її різних структурних компонентах.

База даних апарату управління (центральний рівень) повинна забезпечуватись інструментом санкціонованого дозволу на запуск транзакцій, що виконують записи тільки до бази даних центрального рівня АІАС. Відновлення несуперечливості бази даних у підпорядкованих вузлах (підрозділах, організаціях) корпоративної мережі АІАС ініціюється по закінченню кожної з цих трансакцій, посилкою підтверджень у напрямку, зворотному до напрямку проходження звітів.

У базах даних нижчих рівнів повинні зберігатися фрагменти бази даних центрального рівня. Крім горизонтальної фрагментації, передбачається вертикальна, внаслідок чого підмножина об'єктів регіонального та місцевого вузлів повинна містити тільки оперативну інформацію, тобто поточні значення атрибутів. Історія змін значень атрибутів повинна зберігатися тільки в базі даних центрального рівня системи.

Засоби пошуку документів у документальних базах даних (ДБД) СІР мають дозволяти виконувати пошук за довільними комбінаціям відомих значень таких ознак, як загальні ознаки документа; особливі ознаки документів одного типу (в межах типу документа); ключові слова та їхні комбінації. Технологія інформаційного пошуку має включати програмні засоби пошуку в Інтернеті та програмні засоби пошуку в базах даних СІРВ з використанням реєстру даних. У системі інформаційного пошуку СІР ОДВ також необхідно передбачити використання обмеженої природної мови.

Засоби пошуку мають забезпечувати взаємозв'язок ДБД із реляційними БД і в основному орієнтуватися на роботу зі структурованими текстовими даними і мультимедійною інформацією та даними, що надходять в оперативному режимі. У зв'язку із значним прогресом у технологіях сканування та розпізнавання текстів, у ДБД мають зберігатись усілякі відсканованої копії документів із забезпеченням їх зручного пошуку [208].

Основними функціями системи пошуку інформації є такі, як отримання даних від серверів даних розподіленої мережі; індексація отриманих даних; зберігання та поновлення даних індексації; обробка запитів користувачів.

Наступним підходом має бути застосування технології об'єднання додатків з інформаційними ресурсами на базі ETL-інструментів та цільових аналітичних баз даних — сховищ даних для підвищення оперативності і якості роботи державних службовців, забезпечення надання їм доступу до інформації у будь-який час і в будь-якому місці.

Сховище даних СІР ОДВ у відповідності із призначенням і внутрішньою організацією має включати до свого складу такі компоненти:

а) структуровані фактографічні дані;

б) документальні дані неформалізованих та частково формалізованих документів, що призначені для зберігання, накопичення, формування та отримання текстових і графічних документів, які не можуть бути структуровані у вигляді таблиць, а також даних, фіксованих на паперових носіях у вигляді таблиць, формулярів та карток;

в) набуті та зафіксовані певними документами знання з метою їхнього використання при здійсненні аналізу;

г) єдину в СІР базу метаданих, що призначена для ефективного пошуку та ідентифікації необхідних даних.

Для реалізації в АІАС найбільш підходять дві основні ідеї, які лежать в основі концепції сховища даних, а саме: 1) інтеграція роз'єднаних деталізованих даних у єдиному сховищі; 2) поділ наборів даних і додатків, що використовується для оперативної обробки і застосовується для вирішення задач аналізу.

Це положення ґрунтується на визначенні інформаційного сховища як спеціальним чином організованої бази даних, вміст якої має такі властивості: предметна орієнтація; інтегрованість даних; інваріантість у часі; незнищуваність (стабільність інформації); мінімізація надмірності інформації. До того ж, на відміну від БД, у традиційних OLTP-системах, де дані підібрані відповідно до конкретних додатків, інформація в DW орієнтована на задачі підтримки прийняття рішень.

Для органів влади інтегрованість даних, яка означає подання даних користувачу у вигляді єдиного інформаційного простору, має неабияке значення. При використанні інформаційного сховища дані, що надходять з різних джерел, де вони можуть мати різні імена, атрибути, одиниці виміру і способи кодування, після завантаження в DW очищуються від індивідуальних ознак, тобто немов приводяться до загального знаменника.

У процесах прийняття рішень з високою відповідальністю інваріантість у часі є також важливою характеристикою. На відміну від OLTP-систем, де достовірність даних гарантована тільки в момент читання, оскільки вже в наступну мить вони можуть змінитися в результаті чергової трансакції, в DW дані зберігають свою істинність у будь-який момент процесу читання.

Незнищуваність, або стабільність інформації, є також важливим показником з огляду на специфіку діяльності органів влади. Якщо у

OLTP-системах, які історично призначалися для ефективної обробки структур даних у відносно невеликій кількості чітко визначених транзакцій, записи можуть регулярно додаватися, видалятися і редагуватися, а також які погано підходять для систем підтримки прийняття рішень, то в DW-системах, згідно з вимогою тимчасової інваріантості, існує така специфіка проектування структури бази даних, що один раз завантажені дані теоретично ніколи не змінюються. Стосовно них можливі тільки дві операції: початкове завантаження і читання (доступ).

У сховищі даних варто виділити оперативні й аналітичні складові. Для оперативної обробки потрібні свіжі дані за кілька останніх місяців, у той же час для проведення достовірного аналізу і прогнозування в сховищі даних потрібно мати інформацію про діяльність організації і стан галузі протягом декількох років. Тому обсяг аналітичних БД як мінімум на порядок більше обсягу оперативних.

В АІАС практично можуть використовуватись рішення усіх провідних світових виробників, що добре описані у різних виданнях. До таких рішень, перш за все, слід віднести рішення IBM A Data Warehouse Plus, що забезпечується інтегрованим набором програмних продуктів і сервісів, заснованих на єдиній архітектурі і сімействі СКБД DB2; рішення компанії Oracle, що ґрунтується на різноманітному асортименті продуктів самої компанії і діяльності партнерів у рамках програми Warehouse Technology Initiative; роботи HP, що виконуються в рамках програми OpenWarehouse на основі Unix-платформи і програмного продукту Intel-ligent Warehouse; рішення компанії NCR на архітектурі Enterprise Information Factory і використанні СКБД Teradata; рішення компанії Informix Software на її продукті On-Line Dinamic Parallel Server тощо.

СІР має забезпечувати конфіденційність, цілісність і доступність інформації. З цією метою при обміні інформаційними повідомленнями в СІР спочатку необхідно використати засоби електронного документообігу (ЕДО), що передбачають застосування шифрування та електронного підпису. Ці засоби дозволять чітко та однозначно ідентифікувати відправника повідомлення та гарантувати незмінність повідомлення під час його доставки.

Для забезпечення надійного централізованого зберігання інформаційних ресурсів найбільш важливих служб ОДВ — документообіг, поштова система, аналітика — призначена підсистема зберігання даних. Підсистема повинна також забезпечувати доступність інформації, що зберігається, як для користувачів, так і для програмних застосувань.

Підсистема зберігання даних має інтегруватись в інфраструктуру АІАС та тісно взаємодіяти з підсистемою резервного копіювання даних (рис. 5.9). Архітектура керування непрямо залежить від архітектури підсистеми зберігання даних. Важливим аспектом підсистеми зберігання даних є її керованість у всій організації. Тобто між архітектурою підсистеми зберігання даних та архітектурою керування встановлюється серйозна залежність — це надає фахівцям, що працюють з підсистемою зберігання даних, можливість керувати своїми рішеннями.

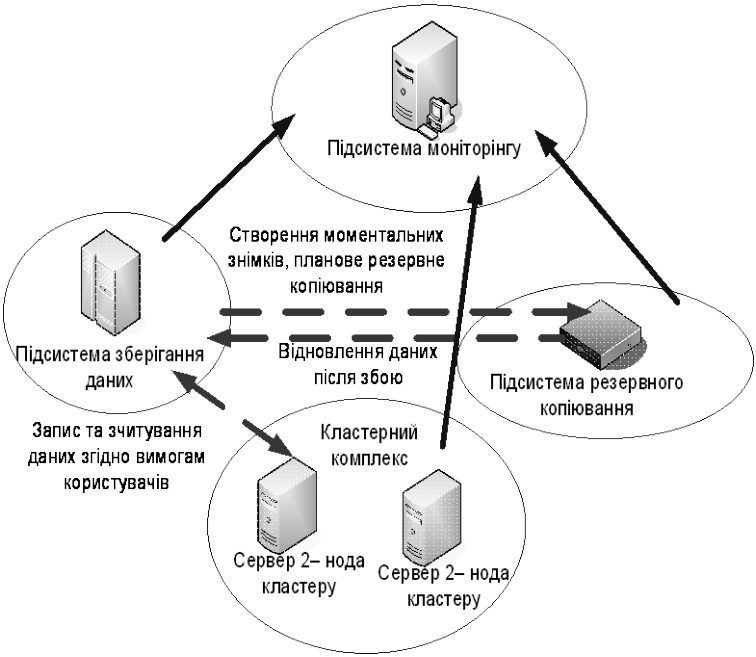

Рис. 5.9. Функціональна схема підсистеми зберігання даних

Для досягнення безпеки необхідно також передбачити створення комплексної системи захисту інформації (КСЗІ) СІР, яка задовольнятиме таким вимогам, як розробка комплексу нормативних документів у розрізі забезпечення безпеки СІР, забезпечення централізованого керування безпекою для впровадження єдиної політики безпеки, забезпечення вищого за середнього рівня захищеності окремих доменів/підмереж СІР, можливість підтримувати багаторівневість захисту, забезпечувати можливість локалізації виявлених загроз і механізмів відклю-

чення пошкоджених/атакованих підсистем від решти СІР, підтримувати функції забезпечення конфіденційності, цілісності, доступності та спостережності [209].

Технології інтеграції інформаційних ресурсів АІАС. В органах державної влади накопичується та обробляється дуже великий обсяг інформації, значна частина якої може використовуватись як загальнодоступна. Проблема полягає в тому, що зберігається вона, в основному, в паперовому вигляді, як файли операційної системи та в локальних базах даних, часто — на застарілій техніці.

Досить суттєвим чинником є також те, що ці бази даних різнорідні, містять різноманітну інформацію — тексти, реляційні таблиці, графіки, об'єкти мультимедіа. Вагоме місце займають бази даних з розробленими під них у різні роки спеціалізованими інформаційно-довідковими та інформаційно-пошуковими системами. Вони успішно експлуатуються, але для загального використання потребують створення зовнішніх інформаційних надбудов.

Вирішуючи питання організації даних в органах державної влади, потрібно враховувати, що, природно, ефективно зберігати і зручно управляти можна лише структурованою інформацією. Але, за оцінками деяких дослідників, на сьогодні майже 65 % наявної інформації є первісно не структурованою. До такої інформації належать листи, договори, газетні та журнальні статті, фотографії та інші подібні документи. Характерно, що саме з ними мають справу службовці органів державної влади.

Таким чином, інформаційна підтримка АІАС сама собою являє складну систему. Базовий рівень системи містять так звані компоненти (інструментальні програмні системи, стандарти подання й обміну даними, коди і кодифікатори та ін.), що утворюють середовище для розробки функціональних підсистем.

Перший (вхідний) блок системи — підсистема архівного банку даних (АБД) — накопичує дані про сферу діяльності ОДВ, систематизує і перетворює їх у внутрішні інформаційні стандарти. Результатом роботи АБД є незалежні та документовані файли даних про різні сфери діяльності й регіони, які цікавлять орган влади. Модель інформаційного фонду АБД будується в контексті моделі предметної області.

Масиви даних, що сформувалися в АБД, надходять у наступний блок системи — інтегрований банк даних (ІБД). Основне призначення ІБД полягає в підтриманні даних у зв'язаному стані на основі складнішої моделі, що враховує як предметну область системи, так і функціо-

нальні вимоги, які виникають в різних ситуаціях використання даних для вирішення поточних завдань.

Результатом роботи ІБД є комплексна база даних (результати моніторингу, аналітичних досліджень і розрахунків, інформація ЗМІ, тематичні карти та ін.), що підтримується в актуальному стані для «живлення» наступного блоку — підсистеми проблемно-орієнтованих додатків (ПОД).

У широкому аспекті ПОД можна уявити у вигляді сукупності спеціально підібраних (під конкретне завдання) тематичних даних, раніше отриманих знань і прикладних програм, що реалізують засоби й моделі аналітичних досліджень. Ці компоненти інтегровані у вигляді інформаційно-технологічного комплексу для отримання нової інформації, необхідної в процесі вибору варіантів прийняття рішень.

Під час розв'язання прикладних задач підсистема ПОД повинна надати користувачу можливість використати:

- первинні дані спостережень про явища і об'єкти (фактографічні дані);
- результати обробки й узагальнення матеріалів у ході аналітичних досліджень у вигляді текстових описів, графіків і т.ін. (текстові дані);
- тематичні карти, географічно прив'язані результати моделювання ситуацій (просторові дані).

Найбільш актуальні для ПОД аспекти підготовки даних — це єдність засобів ідентифікації об'єктів (даних, моделей тощо) та подання їх у вхідних по відношенню до підсистеми документах. Уніфікованість об'єктів у ПОД може підтримуватися спеціально розробленими або вибраними з існуючих кодами, кодифікаторами і класифікаторами для даних, що стосуються різних аспектів задач. Але найефективнішим може виявитися застосування геоприв'язки даних. Принцип зберігання даних на основі просторового каталогу можна використати для повної інвентаризації сховища документів згідно з типами документів, їхньої належності до певного виду діяльності, конкретної організації або підприємства. А за відомим місцеположенням організацій і підприємств можна проводити пошук та аналіз відповідних документів.

Взаємодія перерахованих елементів ПОД і бази даних здійснюється за інформаційно-програмними стандартами, а саме:

а) стандартами інформаційного інтерфейсу для підтримання обміну даними між базовим і аналітичним модулями, відображення та аналізу отриманих результатів;

б) стандартами програмного інтерфейсу для здійснення ініціювання аналітичних модулів у підсистемі та організації їхнього виклику з базового фрагменту.

Ґрунтуючись на цих твердженнях, для комплексного інформаційно-аналітичного забезпечення вирішення завдань, які стоять перед органами державної влади, найкраще створити єдину інформаційну систему, яка буде використовувати загальні джерела інформації, єдину технологію інтеграції різнорідних баз даних, наступний аналіз інформації й візуалізацію його результатів.

Таким чином, СІР ОДВ має уявляти собою інтегроване інформаційне середовище, яке повинно служити базовою основою системи інформаційних ресурсів АІАС.

Треба при цьому брати до уваги, що СІР ОДВ має розглядатися як комплекс взаємно узгоджених і взаємодіючих корпоративних і проблемно-орієнтованих інформаційних середовищ галузі, а саме центрального апарату органу державної влади; сфери виробництва і виробничої інфраструктури галузі (підприємств та організацій, наприклад, сільського господарства, промисловості, енергетики, зв'язку, транспорту, будівництва і т.ін.); соціальної сфери галузі (наука, освіта, культура, засоби масової інформації, охорона здоров'я, профспілки, зайнятість, житлово-комунальні служби та ін.).

Крім того, при організації єдиної СІР ОДВ необхідно враховувати, що в умовах реформування господарства країни така структура може складатися із значної кількості об'єктів, які раніше були роз'єднані або входили в інші структури. У результаті рівень технічного оснащення, набір програмного забезпечення та, як наслідок, формати зберігання й обміну даними в багатьох випадках відрізняються, що викликає проблеми при використанні інформації в центральному апараті для координації діяльності галузі. До того ж, навіть для розв'язання однакових задач в рамках одного об'єкту можуть використовуватись програмні продукти різних розробників або власні розробки, що часто призводить до численних проблем при формуванні інформаційного поля галузі. Даний чинник є досить суттєвим для СІР ОДВ, тому що в процесі її функціонування відбувається активне звернення до різнорідних баз даних або до звітів, що були згенеровані спеціалізованими прикладними програмами.

У цілому СІР ОДВ може бути охарактеризована у функціональному, структурному, трансформаційному і методичному аспектах.

Функціональний аспект СІР ОДВ віддзеркалює її роль у вирішенні завдань органу державної влади. Виділяються такі функції СІР ОДВ:

а) моніторинг (постійний, періодичний, оперативний, запізнілий, прогнозуючий);

б) зберігання (збір, сортування, розміщення, відновлення, пошук і видача інформації);

в) обробка (логічне перетворення інформації);

г) розподіл інформації (вибірковість доставки інформації в системі органів державної влади по рівнях ієрархії керування).

Структурний аспект СІР ОДВ відображає форми і структури збереження й перетворення інформації в органі державної влади і містить класифікацію інформації, інформаційну мову, документацію, структуру інформаційних масивів, мову спілкування з інформаційною системою, а також методичні та інструктивні матеріали, систему підготовки кадрів і захисту інформації (рис. 5.10).

Рис. 5.10. Основні компоненти СІР

Трансформаційний аспект визначає перетворення інформації в процесах управління державою на різних рівнях та етапах просування інформації від входу до виходу.

Основу методичного аспекту СІР ОДВ становлять такі принципи, як методологічна єдність, інформаційна сумісність (використання єдиної системи форм документів, класифікаторів, кодів і шифрів для всіх функціональних підсистем), типізація блоків інформаційного забезпечення, уніфікація обміну інформацією, інтеграція обробки інформації з одноразовим введенням інформації в систему і багаторазовим її використанням, гнучкість структури СІР ОДВ.

Серед компонент СІР ОДВ важливе значення для забезпечення інтеграції інформаційних ресурсів відіграє система класифікації та кодування інформації, яка використовується для формалізації інформації, що переміщується інформаційними потоками в межах інформаційного простору органу державної влади.

Основною метою розвитку систем класифікації інформаційних ресурсів є удосконалення засобів представлення всіх видів інформації для можливості ефективного використання інформаційних ресурсів при вирішенні задач державного управління, для можливості регулювання їхнього розвитку та, у кінцевому підсумку, інтеграції інформаційних ресурсів у європейський та світовий інформаційний простір, гармонізації їх із цим простором.

Обов'язковою умовою внесення інформації до складу інформаційних ресурсів є її документованість. У даний час документування інформації, як правило, здійснюється в порядку, встановленому центральними та регіональними органами державної влади, їхніми структурними підрозділами, відповідальними за організацію діловодства, стандартизацію документів та їхніх масивів, збереження та захист даних.

Інформація, необхідна для забезпечення процесів державного управління, взагалі класифікується залежно від галузі, виду економічної діяльності, від суб'єкта цієї діяльності та його цілей. За основу найбільш крупної класифікації інформаційних ресурсів можуть використовуватись класифікатори міжнародного рівня International Standart Industrial Classification of all Economic Activites — (ISIC), а також галузевий класифікатор видів економічної діяльності в рамках ЄС — Nomenclature General des Activites Economique dans les Communites (NACE) та їх національні аналоги (ОКПД, ОКЗ, ОКС, ОКОФ, ОКОНХ тощо).

Однією з площин є класифікація залежно від сфери створення, виникнення та застосування інформаційного продукту, від рівня та сектора економічної системи. Тут можна виділити наступні класи:

а) загальносистемна інформація;

б) правова, офіційна інформація;

в) наукова, довідкова, науково-технічна (стандарти, форми, метрологічна) інформація;

г) організаційна внутрішньосистемна (ділова, виробнича, рекламна, маркетингова) інформація залежно від галузевої та функціональної характеристики підприємств та інших первинних структур економічної діяльності;

д) управлінська, тобто службова інформація органу державної влади (облікова, звітна, обов'язкова статистична, фінансова, податкова, інвестиційна та ін.).

Можливою реалізацією вищого рівня класифікації інформаційних ресурсів органів державної влади за функціональними напрямками діяльності може бути класифікація інформації відповідно до напрямків діяльності Урядових комітетів Кабінету Міністрів України.

У СІР ОДВ можна виділити два рівні (рис. 5.11):

1) предметні та проблемно-орієнтовані бази даних із відповідними інформаційно-пошуковими й інформаційно-довідковими системами (нижній рівень);

2) реєстр інформаційних ресурсів, який являє собою систему метаданих локальних (предметних) БД із системою його створення, використання та захисту (верхній рівень).

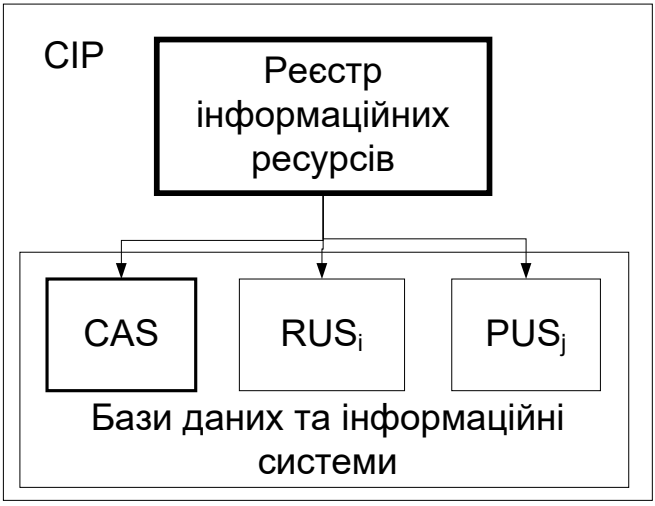

Рис. 5.11. Два рівні СІР

Реєстр інформаційних ресурсів — ще один важливий засіб інтеграції інформаційних ресурсів. Основою його створення є ідеологія систем метаданих, тобто відповідного словника-довідника інформаційних ресурсів. У цьому випадку доступ користувачів до інформаційних ресурсів органів влади відбувається через єдиний реєстр (рис. 5.12).

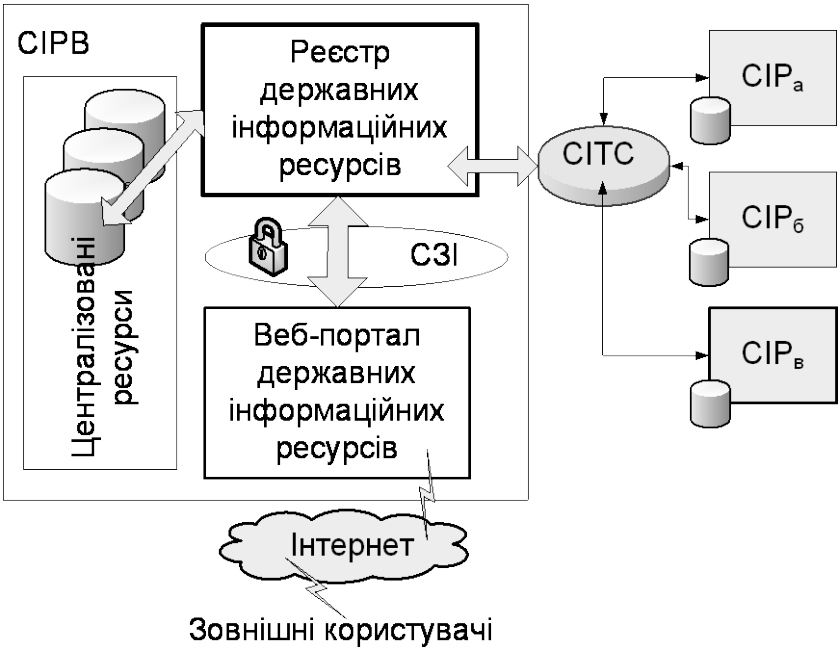

Рис. 5.12. Доступ користувачів до розподіленої БД СІРВ

При розробці концепції реєстру варто звернути особливу увагу на такі його функції, як фіксацію прав власності, володіння та використання інформаційних ресурсів, доцільність реєстрації в реєстрі обмежень з доступу та обґрунтування цих обмежень з урахуванням чинного законодавства, надання реєстру фактично значення правової системи. Критичність цього ресурсу висуває підвищені вимоги до його інформаційної безпеки.

Необхідно також узяти до уваги, що облік та реєстрація інформаційних ресурсів повинні охопити всі рівні їхнього формування, функціонування та управління — від центрального апарату до рівня підприємств [205, 206].

Найбільш відповідальним і складним, де проблеми інтеграції стоять особливо гостро, є нижній рівень СІР ОДВ — регіональних об'єктів. Адже, як відзначалося, тут має місце значне різноманіття подання інформації, на ньому найчастіше особливо тісно переплітаються суперечливі інтереси, неоднозначно вирішуються проблеми власності, доступу. При цьому відіграють певну роль не відрегульовані механізми міжвідомчої інформаційної взаємодії, безліч міжгалузевих завдань, що не мають поки що необхідного законодавчого оформлення.

З метою забезпечення інтеграції інформації для реалізації аналітичних підходів в управлінні в мережних організаціях у світі має місце також підхід формування так званої віртуальної промислової корпорації (ВПК) і розробки для управління ВПК програмного забезпечення на принципах New Business Intelligence (NBI).

Одним із шляхів інтеграції, зокрема, є й спільне використання технологій OLAP і геоінформаційних систем (ГІС) [210]. Таке поєднання завдяки інтеграційним перевагам цих технологій дозволяє забезпечити керівників підрозділів необхідною інформацією з виробничої та фінансово-господарської діяльності галузі для прийняття управлінських рішень на основі оперативного доступу до просторово розподілених баз даних різноманітних інформаційних систем підприємств галузі, а також сформувати інструментарій підтримки прийняття рішень керів-ництвом органу державної влади.

Розглянемо принципи інформаційної взаємодії структурних елементів АІАС на прикладі УІАС НС. Ця система створювалась на основі принципів інтеграції функціональних, інформаційних і програмно-технічних засобів окремих функціонально-структурних елементів (ФСЕ).

Інформаційний ресурс УІАС НС як засіб відображення актуального стану її предметної області в цілому являє собою розподілену БД. При цьому кожний ФСЕ містить у своєї локальній БД інформацію, необхідну й достатню для вирішення завдань, що стоять перед ним по інформаційному забезпеченню керівництва відповідних органів виконавчої влади (по повноті, складу та з урахуванням вимог щодо розмежування доступу) на своєму рівні. Предметна область УІАС НС визначається як логічне поєднання предметних областей діяльності міністерств, відомств і держадміністрацій стосовно НС (згідно з напрямками їхньої роботи).

Принцип інформаційної підтримки процесів прийняття рішень щодо НС полягає у виконані таких вимог:

а) БД кожного ФСЕ повинна відображати рішення і директиви, прийняті (вироблені) відповідним йому рівнем управління;

б) результати відпрацювання рішень і директив відповідного рівня управління фіксуються в БД як відомості, що одержані та/або реалізовані внаслідок виконання відповідних управлінських рішень і вони є вхідними (вихідними) даними для відпрацювання відповідним ФСЕ;

в) оцінка результатів виконання рішень і директив здійснюється з урахуванням відомостей, що накопичені в БД відповідного ФСЕ, як результат виконання відповідної інформаційно-статистичної задачі, або моделювання.

г) функціонально-аналітичне забезпечення має базуватися на сучасних математичних і програмних засобах побудови забезпечуючих підсистем підтримки прийняття рішень і засобах геоінформування.

Використання ГІС-технологій при організації та інтеграції даних в АІАС. Геоінформаційні ресурси — це один із важливіших видів ресурсів країни, без якого неможливе ефективне використання інформації та управління державою [211–214]. Рівень геоінформаційного забезпечення підприємств та органів влади стає важливим критерієм могутності держави, суттєвим засобом вироблення її внутрішньої та зовнішньої стратегії. Тому розвинені країни приділяють особливу увагу проблемам впровадження геоінформаційних технологій у повсякденну діяльність підприємств та управлінських структур. У світовій практиці розвиток геоінформаційних технологій прямує вгору, і ця тенденція, без сумніву, збережеться на ближчі десятиріччя. Згідно з цим, інформаційно-аналітичну підтримку діяльності органів державної влади вже важко уявити без застосування ГІС.

Це підтверджується й тим фактом, що якісно новий рівень подання інформації, створюючи нові ефективні засоби для співробітництва урядових інституцій, підприємницького сектора і населення, а також безпосередньо між урядовими агенціями надає комбінація доступу до Інтернету і картографічної інформації [213].

Використання Інтернет і ГІС, зокрема для забезпечення більш ефективного електронного уряду, надає безліч переваг. Адже просторові дані мають значно інший контекст і значення, чим подані в текстовому або табличному форматі; вони дозволяють набагато зручніше виконувати інформаційні запити, а також забезпечувати процеси інформування. З розвитком Інтернет-технологій підтримки мап використання ГІС стає ще більш простим і повсюдним.

Для подібної підтримки E-Government, що перетворюється вже в G-Government (геоелектронний уряд), є певні підстави. Перш за все, це широке застосування ГІС у різних сферах діяльності. ГІС-технології вже використовуються на декотрих сайтах органів влади, наприклад, Міністерства з надзвичайних ситуацій, Київської обласної держадміністрації, Львівської міської ради та ін.

Крім того, слід зазначити, що шляхи інтеграції ІАС органів державної влади також пов'язані із застосуванням ГІС. Аналіз Національної програми інформатизації України, завданнями якої передбачається ст.-ворення ІАС ОДВ, свідчить, що не лише велика кількість проектів має виконуватись із застосуванням геоінформаційних технологій, а й достатня кількість проектів взагалі базується саме на застосуванні ГІС [215].

Мабуть, найважливішою властивістю ГІС з тих переваг, які вже розглядалися раніше, є їхня здатність до інтегрування даних, отриманих з різних джерел, та забезпечення взаємодії з іншими інформаційними системами і технологіями.

Один з шляхів інтеграції пов'язаний з геоприв'язкою інформації. Це мотивується, по-перше, тим, що за деякими оцінками 70–80 % усієї інформації, яка використовується в організаціях, вже є просторово прив'язаною або є картами, схемами, кресленнями (у тому числі й електронними). Можливість їх перегляду за допомогою спеціальних засобів значно підвищує ефективність роботи. До того ж, знання географічного місцеположення потрібних документів дозволяє проводити пошук за меншим набором документів. Нарешті, існування розвинених засобів ГІС дає змогу вивчати масиви документів на основі просторової прив'язки, характерної практично для всіх документів, що зберігаються. Географія часто-густо є фактично єдиним об'єднуючим фактором серед множини завдань, що вирішуються установою, а, отже, і єдиним фактором, на базі якого може бути об'єднана і підготовлена для спільного аналізу вся різнорідна інформація. Тому ГІС у багатьох випадках уже використовується як базова інформаційна технологія для управління підприємствами та організаціями.

Окремі документи, що зберігаються в системі, повинні бути закодовані для їхньої прив'язки до ширших понять. Більша частина цього процесу може бути частково автоматизованою шляхом використання профілюючого програмного забезпечення, основаного на використанні деревоподібних мереж. Тут може знадобитися адаптивний процес, в якому масив документів з географічною прив'язкою використовується як навчальний набір для періодичного поновлення методики пошуку.

Якщо повернутись до типової схеми обробки інформації в органах влади, то слід зазначити, що переваги застосування ГІС уже відчуваються, починаючи з перших двох етапів — збирання, попередньої обробки даних і забезпечення їхнього зберігання — відбувається накопичення даних із різних джерел, що надходять у різних форматах, а також етапу генерації аналітичної інформації, коли забезпечуються інтеграція даних та аналіз, інтерпретація, подання тематичної інформації в зручній і наочній формах. Що стосується наступного етапу, коли має за безпечуватись надання інформаційних та інших адміністративних послуг, вид подання інформації набуває великої ваги. Адже інформація призначена для сприйняття пересічними громадянами та підприємцями, здебільшого необізнаними особливостями інформаційно-комп'ютерних технологій.

Враховуючи ці обставини, потрібно забезпечити «прозорий» доступ користувачів до всієї наявної інформації. З цих причин зростає увага до питань керування даними всього комплексу об'єктів і явищ (адміністративно-територіальний устрій, комунікації, гідрометеорологія, екологія, надзвичайні ситуації, забруднення і т.ін.) як взаємопов'язаного й інтегрованого процесу їхньої обробки. Згідно з цим, загальна централізована схема поєднання інформаційних ресурсів і систем просторових даних має містити окрему підсистему дата-центру (рис. 5.13).

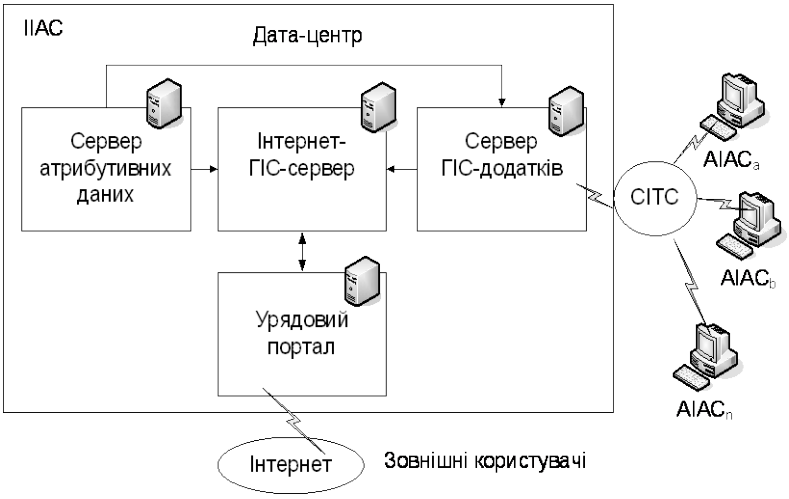

Рис. 5.13. Підсистема інформаційних ресурсів і систем просторових даних інтегрованої системи органів влади

Найбільш відповідальним етапом підготовки даних є створення фонду картографічних матеріалів зі сфери керування органу влади. Основною інформаційною одиницею топографічної основи повинні бути аркуші карт масштабу 1:1000000 (дрібномасштабні), 1:100000 (великомасштабні), 1:25000 (детальні). Тематичні карти, необхідні для вирішення аналітичних завдань, повинні бути прив'язані до єдиної топографічної основи.

Перспективою подальших досліджень має бути визначення базової сукупності картографічних матеріалів для різних видів органів влади, що має централізовано створюватись та зберігатись, а також комплексу функціональних задач для реалізації геоінформаційного обслуговування в системі електронного уряду.

5.3. Забезпечення електронного документообігу в органі державної влади

Основні засади електронного документообігу в органі влади. Як вже було визначено, єдиний шлях до вирішення проблем автоматизації документообігу полягає у застосуванні сучасних систем електронного документообігу (Electronic Document Management Systems — EDMS), які забезпечують достовірність, контроль та автоматизацію діловодства.

Основним призначенням системи ЕДО в органі влади є опрацювання 3-го та 6-го напрямків інформаційно-аналітичної діяльності в умовах функціонування АІАС (табл. 3.1), але фактично через цю систему так чи інше проходять й потоки за майже усіма іншими напрямками.

Під терміном «електронний документ» у контексті застосувань в органі влади як різновиду документу, інформація в якому зафіксована у вигляді електронних даних, звичайно мається на увазі текстовий файл (документ MS Word або іншого текстового редактора), електронна таблиця MS Excel, графічний файл, кілька взаємозалежних файлів різних форматів тощо.

Впровадження ЕДО у першу чергу сприяє підвищенню продуктивності праці та скороченню часу опрацювання одного документа за рахунок єдиних засобів керування життєвим циклом і маршрутизацією документів, адміністрування документообігу, єдиних механізмів зберігання документів та розмежування прав доступу до них, загальних за-

собів пошуку документів, навігації й доступу до документів, єдиних засобів розробки й настроювання прикладних додатків.

Тому для органів влади встановлення системи електронного діловодства і документообігу (СЕД/СЕДД) є найважливішим питанням, враховуючи також, що, як вказувалося, орган влади забезпечує за рік обробку значної кількості документів.

Зважаючи на плутанину в термінології, що поки ще існує в царині ЕДО, необхідно визначитися в поняттях. Будемо розрізняти два класи систем. До першого відносяться системи керування електронними картотеками (архівами). Їхніми основними функціями є реєстрація нових документів, збереження, пошук і їхній витяг з метою передачі в додатки, що вміють з ними працювати.

До другого класу відносяться системи електронного документообігу. На них покладають функції керування документами на шляху проходження від одного користувача (посадової особи) до іншого (див. рис. 4.1) з можливістю контролю за їхнім переміщенням, з фіксацією всіх змін і супровідних резолюцій. Враховуючи значну важливість систем другого класу, такі системи мають бути складовими АІАС. Впровадження такої системи ЕДО в органі влади на основі застосування сучасних програмно-технічних засобів забезпечує комплексне вирішення проблеми управління документообігом і контролю виконання доручень (рис. 5.14).

Під рухом документів в ЕДО розуміють не їхнє фізичне переміщення (тому що вони найчастіше залишаються на сервері), а передачу прав на їхнє використання з повідомленням конкретних користувачів і контролем за їхнім виконанням.

Важливою особливістю впровадження систем ЕДО в органі влади, чого важко або неможливо досягти при традиційному документообігу, є організація надійного і захищеного збереження документів, а також роботи з ними із реалізацією санкціонованого доступу до документів, відслідковування зроблених у них змін, контролювання всіх версій документів тощо.

У цілому система ЕДО ОДВ має забезпечувати:

а) відповідність системи та діловодних процесів, що нею автоматизуються, не тільки відомчим, а й державним стандартам України (ДСТУ) та нормативним документам;

б) можливість внесення оперативних змін до системи згідно зі змінами чинного законодавства України без втрати працездатності;

в) відповідність вимогам щодо захисту інформації та забезпечення конфіденційного документообігу, наявність засобів криптографічного захисту документів та електронного підпису;

г) одночасну підтримку традиційного паперового документообігу та електронного;

д) впорядковане архівне зберігання всіх версій документів із вбудованими засобами їхнього повнотекстового пошуку;

е) можливість колективної роботи виконавців з одним або декількома об'єктами обробки;

є) відкриту архітектуру, сумісність з сучасними корпоративними СКБД, офісними програмними системами, засобами електронної пошти та факсимільного зв'язку;

ж) інтеграцію з інформаційно-аналітичною системою вищого рівня (наприклад, Секретаріату Кабінету Міністрів України);

з) модульну побудову системи та можливість швидкої її реконфігурації при зміні організаційно-штатної структури установи;

і) використання сучасних веб-технологій для розподіленої обробки документів.

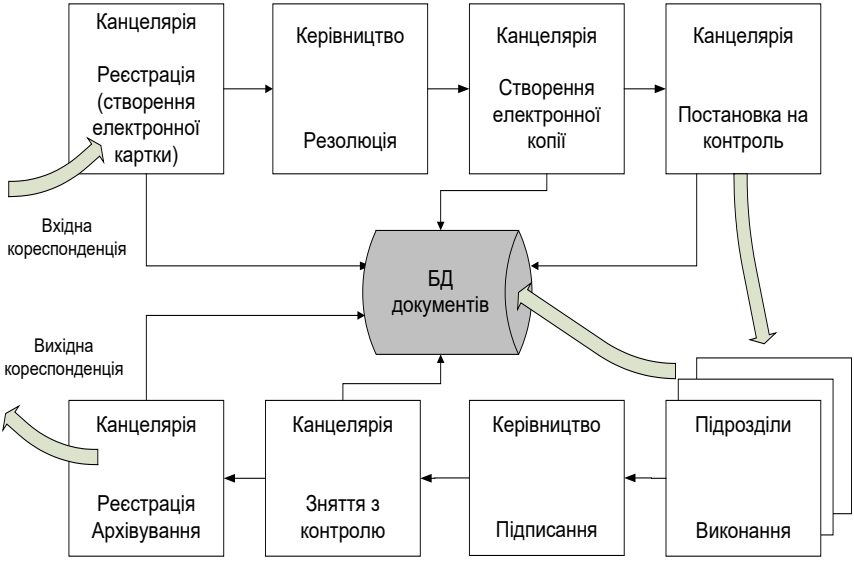

Рис. 5.14. Типова схема обробки вхідних документів в АІАС із застосуванням електронного документообігу

Система ЕДО АІАС — це класична складна система, яка потребує спеціальних підходів під час розробки, впровадження та експлуатації, тому вона повинна створюватися одночасно із створенням АІАС і згідно держстандартів щодо інформаційних технологій, функціонуючих в Україні. Враховуючи, що ще тривалий час буде існувати паралельно електронний та традиційний — паперовий документообіги, один з підходів має базуватися на методології композитного документообігу, яка полягає у декомпозиції задачі на сукупність активностей у вигляді описаних процесів, що створюють систему взаємодіючих елементів [216].

Важливим є питання забезпечення інтеграції системних програмних платформ ЕДО на стандартних підходах і протоколах додаткових засобів захисту інформації корпоративних мереж, що прийняті уповноваженим органом України з технічного захисту інформації.

Згідно з існуючою практикою, як правило, будь-які документи зовнішнього документообігу за допомогою спеціальних засобів мають перетворюватися у внутрішній формат подання даних. Те ж саме виконується при необхідності перетворення внутрішнього формату у зовнішній формат документообігу (рис. 5.15).

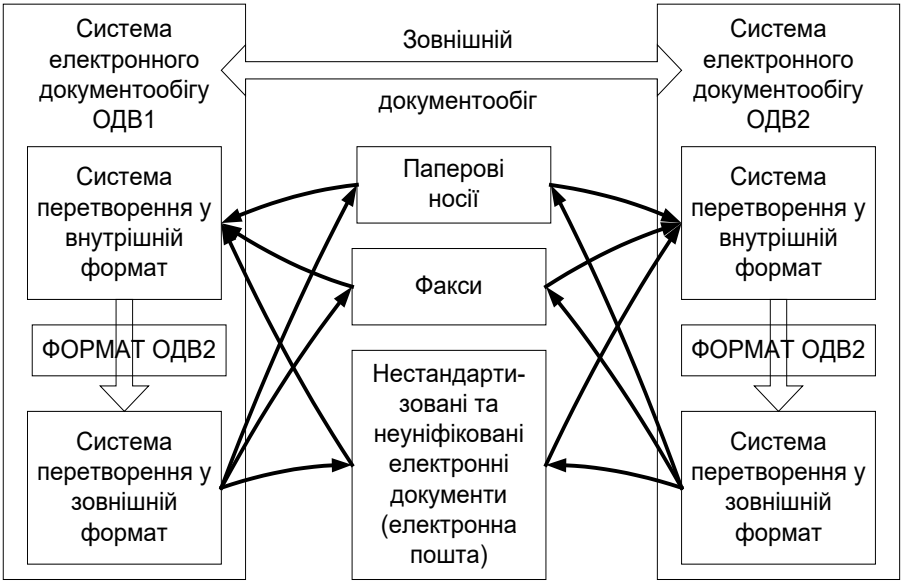

Рис. 5.15. Властивості документообігу між різними ОДВ

Така організація документообігу є традиційною для України. Причини цього — відсутність стандартизації та уніфікації як внутрішнього подання даних у різних СЕД, так і формату інформаційного обміну між різними системами. Крім того, для інформаційних обмінів необхідне узгодження протоколів і комунікаційної інфраструктури, надання юридичної сили електронним документам тощо.

Впровадження системи ЕДО, починаючи від традиційного паперового діловодства і до автоматизованого електронного документообігу з міжвідомчою інтеграцією, має проходити певні етапи (рис. 5.16), якими передбачається виконання значного комплексу робіт з розробки інфраструктури документальних даних і системи підтримки електронного документообігу, а саме:

1) створити інфраструктуру маршрутизації документів у підрозділах органу влади;

2) забезпечити єдину систему формалізації процесів опрацювання документів;

3) впровадити систему автоматизації бізнес-процесів (WorkFlow);

4) впровадити засоби пошуку, формування звітів і витягу знань та ін.

Для забезпечення прискорення обробки паперових документів і створення певної бази для переходу до ЕДО доцільним є запровадження технології штрих-кодування документів (рис. 5.17).

Ще одним важливим питанням є впровадження єдиного стандарту електронних документів для забезпечення сумісності файлів, створених в офісних пакетах різних виробників. Спеціальний підрозділ Єврокомісії з обміну даними між адміністраціями (IDA) запропонував прийняти за міжнародний стандарт офісних документів формат, що використовується у вільно поширюваному офісному пакеті OpenOffice.org. Розробляється також єдиний файловий формат офісних документів на базі мови XML.

Архітектура підсистеми ЕДО ІАС ДКЗІ побудована на основі концепції «відкритих систем». Підсистема ЕДО являє собою територіально-розподілену комп'ютерну систему. Розподілений характер визначає відповідні характеристики та вимоги до підсистеми — орієнтацію на «клієнт/серверні» технології обробки і доступу до інформації, використання комунікаційних каналів і відповідних протоколів обміну. У зв'язку із цим за базове прикладне програмне забезпечення для автоматизації ЕДО та контролю виконання вибрано «Систему управління потоками робіт та організації конфіденційного документообігу ОПТІМА-СТАНДАРТ».

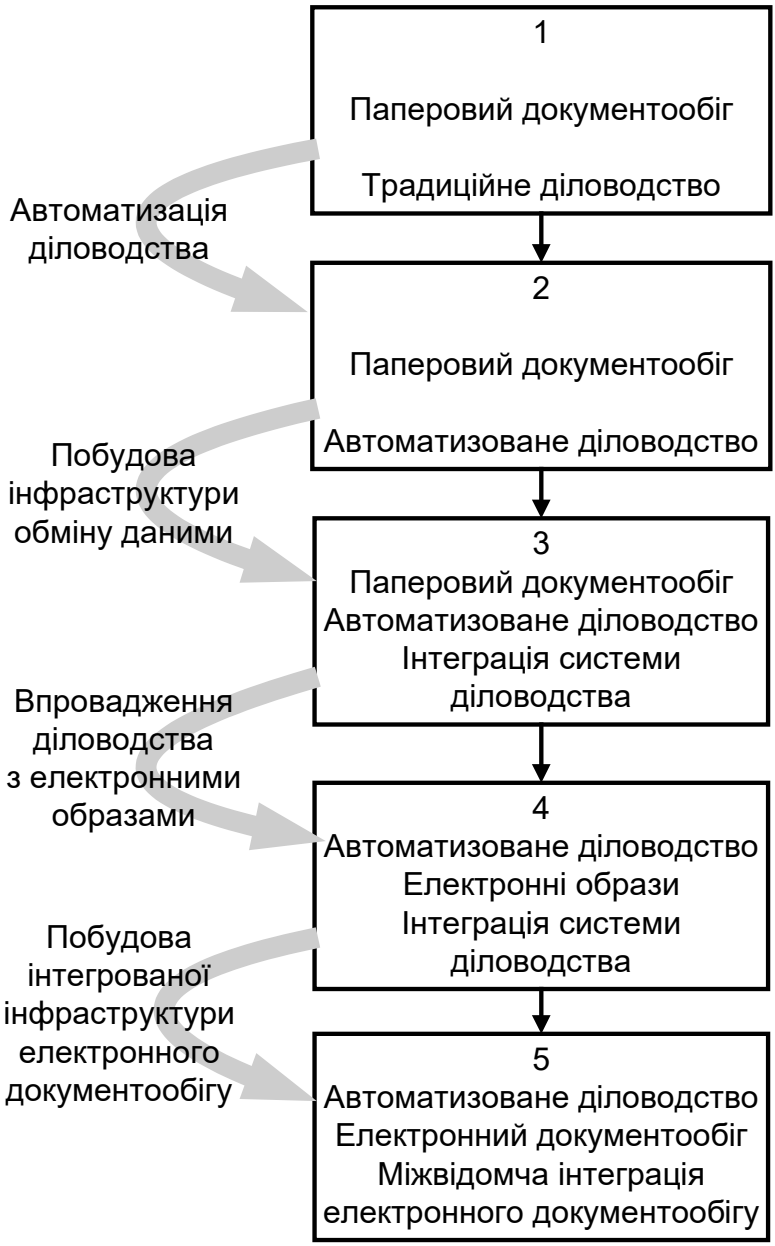

Рис. 5.16. Основні етапи впровадження електронного документообігу в ОДВ

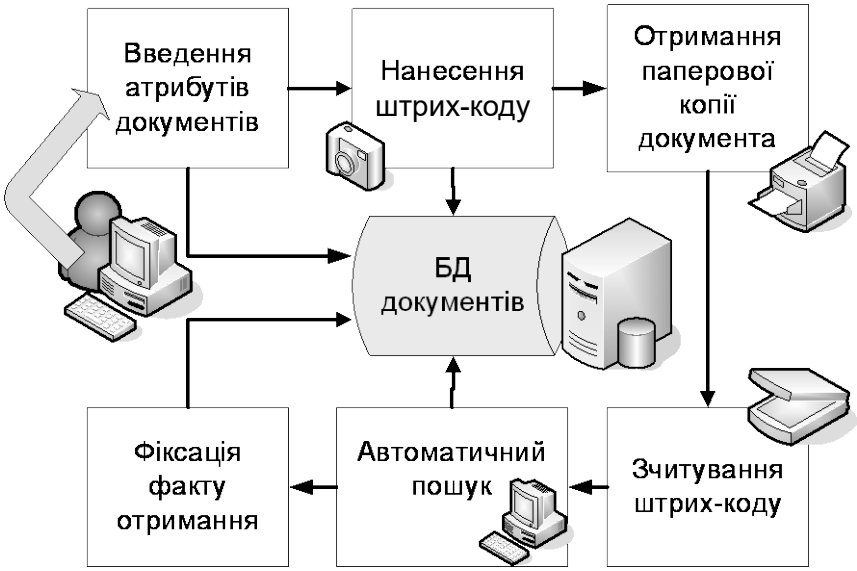

Рис. 5.17. Використання технології штрихкодування в системі ЕДО

Як приклад розглянемо рішення щодо побудови ЕДО ІАС ДКЗІ. СЕДО передбачена як складна організаційна структура, що взаємодіє з іншими процесами управління в державі та спрямована на досягнення цілей забезпечення інформаційно-аналітичної діяльності. При цьому застосовано наступні підходи:

1) в організаційному аспекті — забезпечення контролю цілісності документів, реєстрації документів відповідно до регламенту роботи; зведення до мінімуму змін у системі, що стосуються зв'язків із зовнішніми структурними підрозділами та установами в разі зміни організаційної структури ІАС ДКЗІ; забезпечення багатоваріантності зв'язків із зовнішніми у відношенні до ІАС ДКЗІ структурними підрозділами та установами з метою збереження працездатності системи у випадку втрати зв'язку з будь-яким зовнішнім структурним підрозділом;

2) в інформаційному аспекті — інтеграція даних, що підтримуються та використовуються структурними підрозділами та установами при їх взаємодії; можливість виконувати основні функції в локальному режимі функціонування системи; відповідність існуючим інформаційним технологіям, які розробляються і функціонують у ДКЗІ;

3) в алгоритмічному аспекті — відповідність алгоритмів функціонування системи вимогам міжнародних стандартів і рекомендацій щодо

побудови та використання інтерфейсів користувача, мережних засобів, систем управління базами даних і знань тощо;

4) у технічному аспекті — забезпечення взаємозамінності та резервування технічних засобів системи з метою досягнення потрібної надійності її функціонування; забезпечення розширення програмно-технічних засобів без змін програмного й інформаційного забезпечення, доповнення та оновлення функцій і складу системи без порушення її функціонування;

5) у технологічному аспекті — забезпечення побудови діловодних процесів у рамках сучасної концепції WorkFlow таким чином, що управління та планування здійснюється відносно процесів (потоків робіт) взаємодії ІАС ДКЗІ з ОДВ, в яких створюються, оброблюються та з яких надходять документи; забезпечення можливості легкого та швидкого переналагоджування процесів відносно змін технологій обробки чи потреб кінцевих користувачів без суттєвого зниження продуктивності та надійності системи в цілому.

АРМи СЕДО мають дружній інтерфейс (рис. 5.18), розвинуті засоби допомоги та навчання, не потребують від рядового користувача спеціальної фахової підготовки та надають можливість отримати всілякі довідки, звіти та результати аналізу документів (рис. 5.19, 5.20).

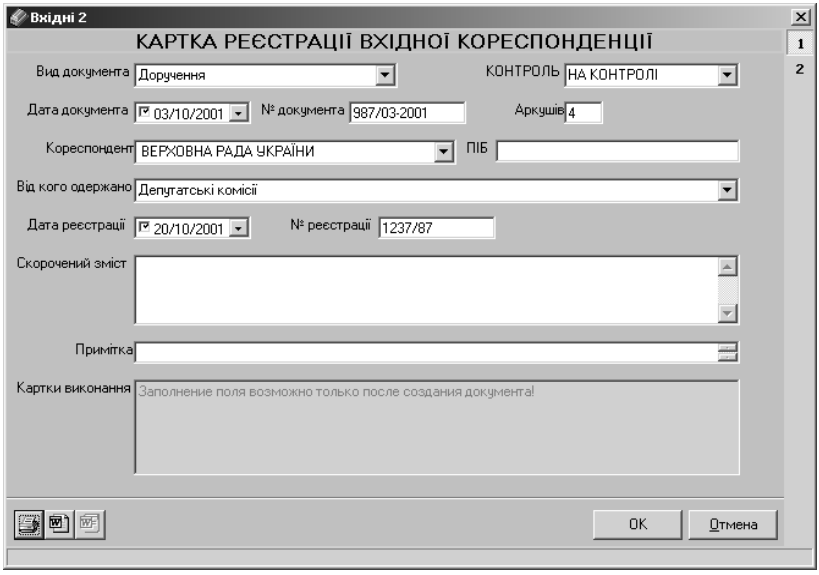

Рис. 5.18. Інтерфейс реєстрації вхідної кореспонденції

ДЕРЖАВНИЙ КОМІТЕТ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ УКРАЇНИ

Відділ обліку і контролю документів

01001, м. Київ, вул. Хрещатик, 22, тел. 229 95 02

Форма ЗГ01-ДКЗ

АНАЛІЗ
заяв та скарг, що надійшли в Управління справами ДЕРЖКОМЗВ'ЯЗКУ УКРАЇНИ
на роботу місцевого телефонного зв'язку
за період з 23.10.2001 по 23.10.2001 ВКЛЮЧНО

№ п/п	Назва виробників об'єднань та підприємств зв'язку	Незад. якість роботи тел. з.	Встановлення телефону	Перестановка телефону	Залиш. телеф. на самост. лінії	Перейменування телефону	Винос телеф. у коридор	Довідки про МСТЗ	Довідки про тарифи	Підкл. попеp. оформл. телеф.	Заміна номеру телефона	Прискорене введ. в дію АТС	Вирішення кабелю	Видача платіжних довідок	Кабелювання будинку	Встановлення таксофону	Ремонт телеф. апарату	Придбання телеф. апарату	Телефонізація села	Встановлення парал. апарату	Придбання телеф. довідника	Різне	ВСЬОГО
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Всього:

23.10.2001р.

Рис. 5.19. Форма звіту щодо аналізу заяв і скарг, що надійшли, на роботу місцевого телефонного зв’язку

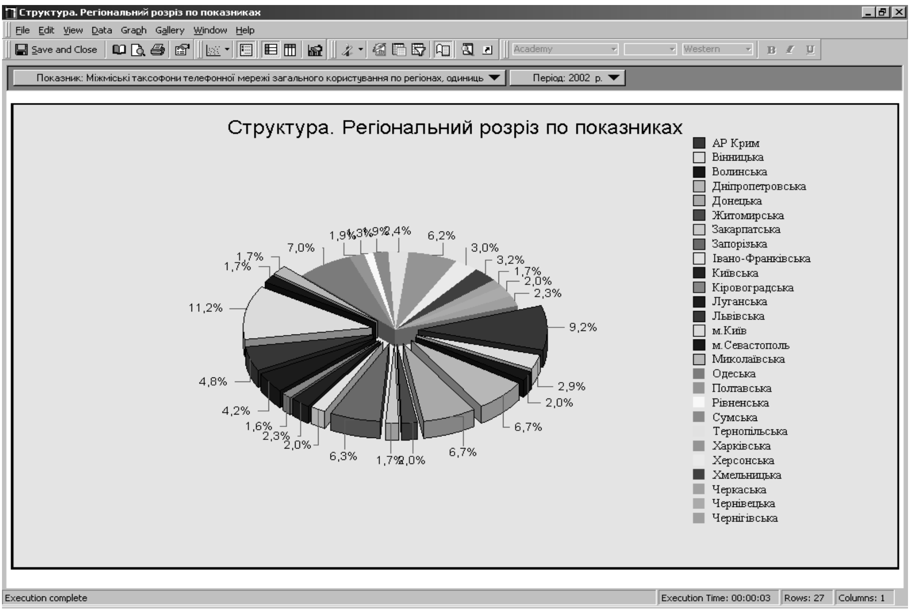

Рис. 5.20. Сторінка звіту щодо регіональної структури розвитку міжміської таксофонної телефонної мережі загального користування

Ще один приклад — реалізація підсистеми автоматизації документообігу в ІАС НКРЗ. Ця підсистема призначена для автоматизації процесів документообігу й контролю виконавчої дисципліни. Підсистема охоплює та спрямовує діяльність співробітників, яка пов'язана з реєстрацією, обробкою, підготовкою, узгодженням, зберіганням і обліком документів, контролем виконавчої дисципліни, а також передачі в архів як самого документа, так і його електронного образу.

Підсистема будується на основі архітектури клієнт-сервер, окремим сервером бази даних (централізоване сховище даних) і клієнтськими робочими місцями на базі веб-браузера (рис. 5.21).

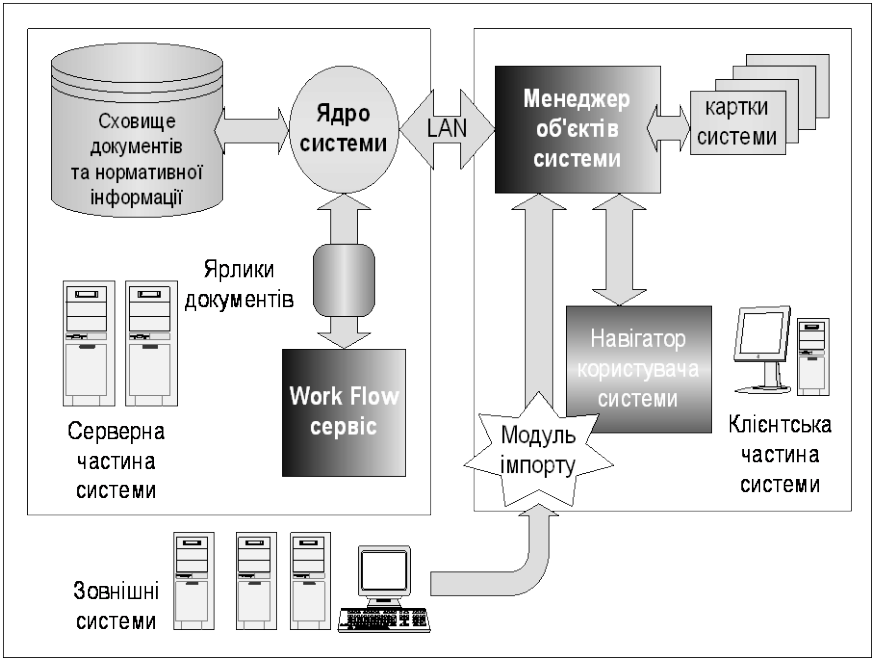

Рис. 5.21. Функціональна схема клієнтської та серверної частин підсистеми автоматизації документообігу ІАС НКРЗ

Підсистема управління документами спроектована та створена для роботи з документами та бізнес-процесами в установі, а також має механізми інтеграції з іншими інформаційними системами.

Використання електронного цифрового підпису. Розвиток електронного документообігу в органах влади має сприяти, зокрема, спрощенню подання звітності, реєстрації суб'єктів підприємницької діяльності, митного оформлення товарів тощо. Тому важливим питанням є використання електронного цифрового підпису (ЕЦП) для виконання органами влади заходів забезпечення трансакцій з автентифікацією користувача. За наявності необхідних елементів інфраструктури ЕЦП стає можливим реально запровадити ЕДО, тому що, згідно з законом, саме накладанням електронного підпису завершується створення електронного документа, а перевірка цілісності електронного документа проводиться шляхом перевірки ЕЦП.

Широке застосування ЕДО з забезпеченням ЕЦП у нашій державі регламентується низкою нормативно-правових актів, прийнятих Кабінетом Міністрів України упродовж 2004 року на виконання Законів України «Про електронний цифровий підпис» і «Про електронні документи та електронний документообіг».

У цілому ця сукупність актів фактично встановлює не лише порядок застосування ЕЦП та електронних документів юридичними та фізичними особами, а також визначає організаційну інфраструктуру та її суб'єкти, функціонування яких є необхідним за технологією використання ЕЦП (рис. 5.22, 5.23). Зокрема визначено статус таких суб'єктів, їхні права, обов'язки та вимоги щодо надання ними відповідних послуг.

Згідно з законом, застосування ЕЦП в Україні базується на інфраструктурі відкритих ключів (PKI). Основними елементами інфраструктури ЕЦП є центри сертифікації ключів (ЦСК). ЦСК, акредитований в установленому порядку, є акредитованим центром сертифікації ключів (АЦСК), який має право обслуговувати виключно посилені сертифікати ключів. Правила посиленої сертифікації затверджені наказом Департаменту спеціальних телекомунікаційних систем і захисту інформації (ДСТСЗІ) від 13.01.05 № 3. Саме посилені сертифікати мають застосовуватись в органах влади.

Для їхньої підтримки передбачається створення засвідчувальних центрів органів влади як елементів загальної інфраструктури ЕЦП. Засвідчувальний центр здійснює засвідчення чинності відкритого ключа процедурою формування сертифіката відкритого ключа та надає послуги ЕЦП цьому органу влади і підпорядкованим йому підприємствам, установам та організаціям.

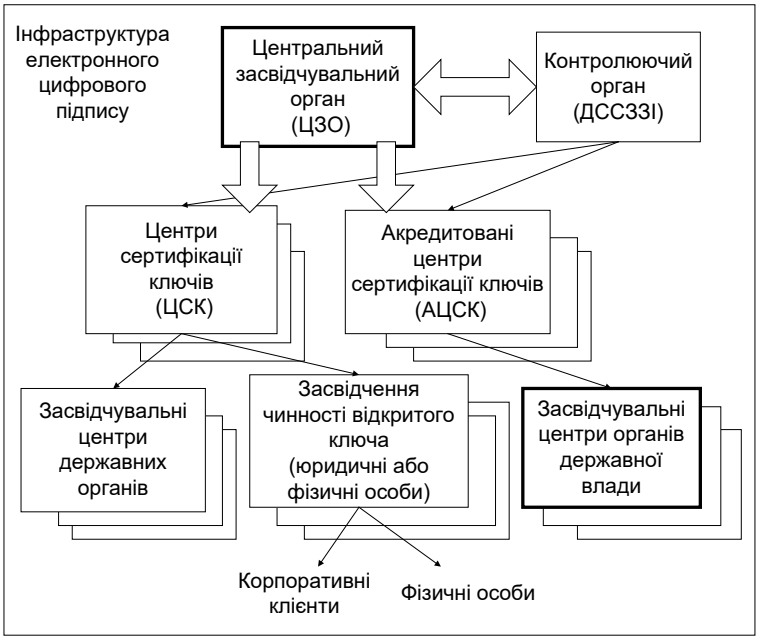

Рис. 5.22. Інфраструктурна схема загальнодержавної системи ЦЕП

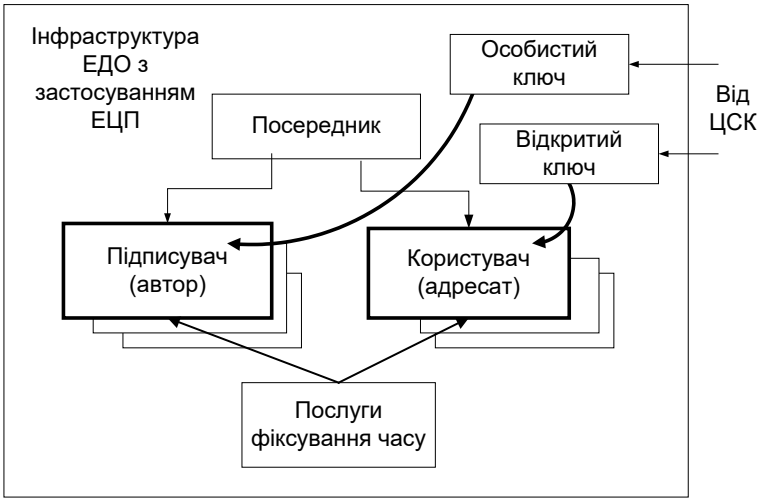

Рис. 5.23. Інфраструктурна схема системи ЕДО

Відповідно до закону акредитацію центрів сертифікації ключів провадить центральний засвідчувальний орган (ЦЗО), тому ЦЗО визначається як головний елемент системи ЕЦП. Відповідними директивними документами визначено структуру ЦЗО та його взаємовідносини в системі ЕЦП (рис. 5.24) [217].

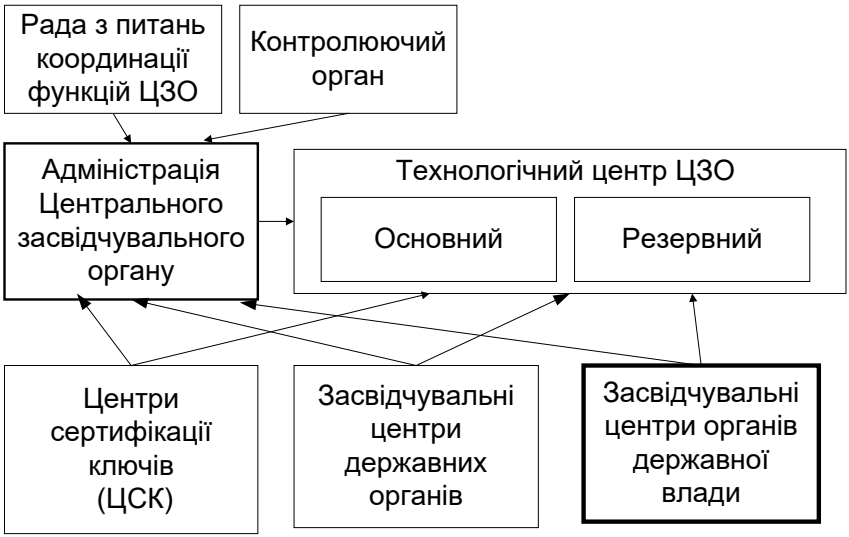

Рис. 5.24. Структура ЦЗО та взаємовідносини в системі ЕЦП

Враховуючи надзвичайну важливість надійності функціонування системи ЕЦП, в інфраструктуру законом введено такий елемент, як контролюючий орган. Він перевіряє дотримання вимог закону центральним засвідчувальним органом та центрами сертифікації ключів. За визначенням функції контролюючого органу покладаються на спеціально уповноважений центральний орган виконавчої влади у сфері криптографічного захисту інформації.

Одним з важливих аспектів ЕДО є засвідчення наявності електронного документа (електронних даних) на певний момент часу. Згідно із затвердженим порядком засвідчення наявності електронного документа (електронних даних) на певний момент часу є послугою фіксування часу, яка здійснюється шляхом додавання до документа або логічного поєднання з ним позначки часу. Ці послуги надаються ЦСК або АЦСК на договірних засадах.

5.4. Підтримка функціональної діяльності та аналітичної роботи в АІАС

З основних напрямів діяльності органу влади (табл. 3.1) значна частина, що має підтримуватися АІАС, належить до розв'язання функціональних задач та аналітичної діяльності, що між собою, власне кажучи, тісно переплетені.

Для забезпечення вирішення зазначених проблем потрібні спеціальні засоби, що створюються на засадах новітніх інформаційних технологій з використанням понятійно-інформаційної моделі предметної області, яка постійно оновлюється й уточнюється, із залученням соціопсихологічних методів для урахування впливу людського фактора. Власне вони й формують аналітичну складову інформаційних систем.

Аналітична підтримка прийняття рішень. Передусім, кожна система інформаційно-аналітичного забезпечення ОДВ повинна забезпечувати функціонування певної системи підтримки прийняття рішень (СППР), яка є центральною ланкою і забезпечує взаємодію керівництва органу влади, секретаріату і функціональних та інших підрозділів у процесі підготовки прийняття рішень (рис. 5.25).

Аналітична складова розробляється з метою виконання наступних функцій:

а) вчасного надання фахівцю необхідної інформації, яка має бути актуальною за часом, місцем і обсягом;

б) забезпечення процесу підготовки інтегрованих даних фахівців нижчого рівня для напрацювання рішень фахівцями вищого рівня;

в) підтримки процесу розробки комплексних, збалансованих за цілями і можливостями довгострокових стратегічних програм та рішень;

г) моніторингу окремих управлінських процесів та управлінської діяльності в цілому з метою виявлення і локалізації проблем, позитивних і негативних тенденцій, визначення їхніх причин шляхом забезпечення багатоатрибутного просторово-часового аналізу;

д) прогнозування результатів від реалізації прийнятих рішень.

Аналітична складова утворюється як сукупність алгоритмів аналізу інформації, методик аналітичних досліджень, напрацьованих схем для розв'язання конкретних прикладних задач. Для її розробки обов'язково необхідно залучати спеціалістів з даної галузі, які спроможні сформулювати задачі аналітичного характеру та мають досвід їхнього розв'язання.

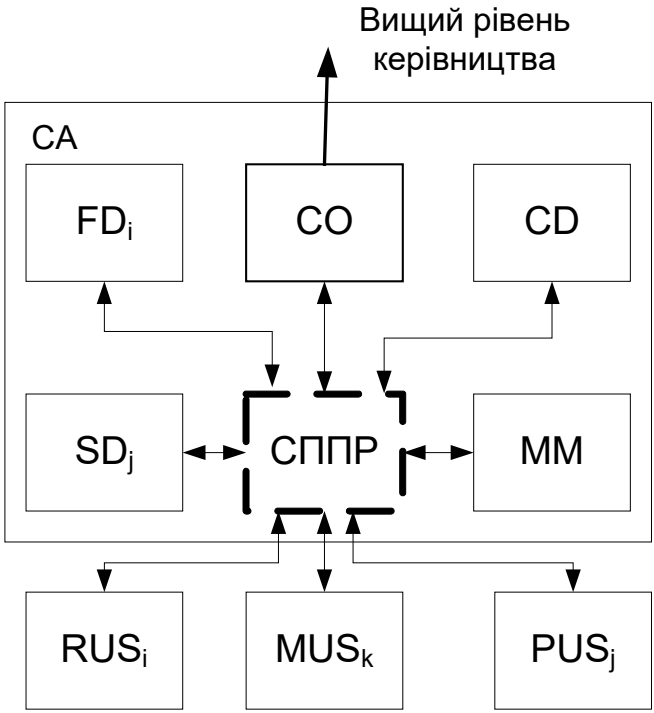

Рис. 5.25. Місце СППР у системі інформаційно-аналітичного забезпечення органу влади

Так, наприклад, річний бюджет є ключовим елементом виконання практично всіх стратегічних задач державної організації. Тому одним з методологічних підходів у цій царині має бути забезпечення підтримки усього бюджетного циклу органу влади (а також планування, затвердження, реалізацію, облік грошових витрат і надходжень, засоби фінансової аналітики (FAT — Financial Analytical Tools), реалізацію електронних платежів (EPS — Electronic Payment System) тощо) єдиною інтегрованою системою, яка може базуватися на технології ERP.

Як приклад реалізації функціональних комплексів програм візьмемо до розгляду основні характеристики щодо призначення, виконуваних функцій, вхідної та вихідної інформації КП «Експерт» АСЕК.

Основні функції цього КП зводяться до автоматизованої обробки заяв, що надходять до ДСЕК, накопичення, перегляду, коригування та відбору даних по заявах і контролю оплати дозвільних документів

суб'єктами зовнішньоекономічної діяльності. Функціональна схема підсистеми «Експерт» наведена на рис. 5.26.

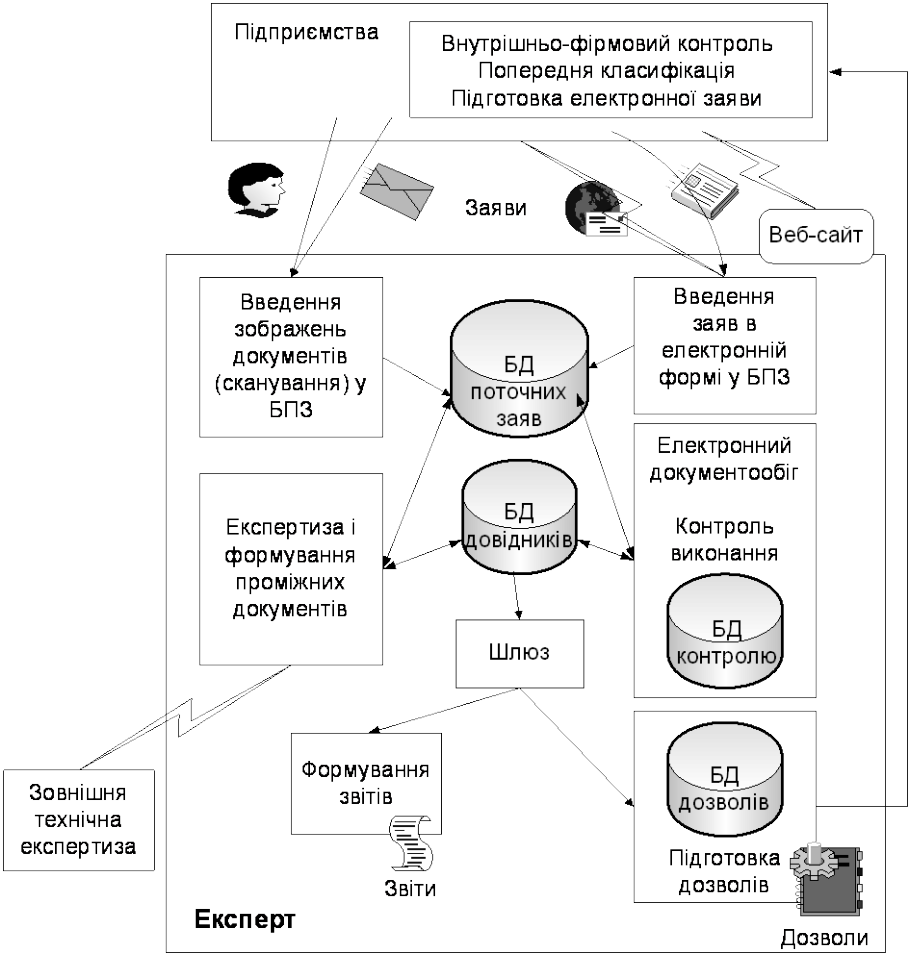

Рис. 5.26. Функціональна схема підсистеми «Експерт»

Технологічні процедури підсистеми «Експерт» полягають у наповненні секретної БД; друкуванні дозволів; веденні довідників; адмініструванні (надання прав користувачу на виконання дій у системі по перегляду чи зміні даних, а також на виконання окремих специфічних функцій).

Вхідними даними КП «Експерт» є заявки підприємств; запити користувача на формування вихідних даних. При роботі також використовується значна кількість довідників (словників) — країн; континентів; напрямів передач; одиниць виміру; характеру міжнародних передач; умов поставки; категорій ООН; митниць України; керівництва; особливих умов заяв; походження товарів; типів міжнародних передач; форм власності; типів подій; об'єктів; посад; ролей; експертів; типів товарів; угод; підприємств; валют; видів дозволів; видів товарів; кінцевих документів та ін.

Вихідними даними комплексу є дозвільні документи; відмови; запити; звіти за встановленими користувачем параметрами.

Інформаційне забезпечення аналітичної стадії підготовки рішень. Автоматизація функціональної діяльності та прийняття рішень в ОДВ, що має базуватися на аналітичному забезпеченні, має масштабуватися на відповідні рівні структурних елементів і включати програмну підтримку для забезпечення взаємодії органу влади з необхідними інформаційними джерелами, ведення аналітичної обробки даних з єдиного інтегрованого банку даних.

Методи проведення аналітичних досліджень в органах влади можуть бути досить різноманітними — якісними та кількісними, формально-логічними та кібернетичними, функціональними та інформаційними. Але головним принципом вибору методу аналітичного дослідження повинна бути комплексність, коли обмеження одного методу компенсуються перевагами іншого. За формою аналітична діяльність може бути закритою й відкритою — залежно від мети досліджень і призначення результатів. При цьому треба враховувати, що по мірі просування аналітичної інформації знизу нагору ступінь її конфіденційності може зростати, що пов'язано, з одного боку, з ростом узагальнюючого характеру інформації, а з другого — з інтересом розвідувального характеру інших країн та структур.

Вочевидь, надійність і коректність аналітичної складової суттєво залежать від інформаційного середовища АІАС і безпосередньо від якості галузевих та загальнодержавних інформаційних ресурсів, які використовуються при її розробці і функціонуванні.

Крім того, створення аналітичної складової в АІАС слід розглядати і як проблему розподілу функцій. Тому при проектуванні АІАС необхідно визначитися щодо важливості таких критеріїв аналітичної складової:

а) мінімізації загальної вартості її розробки та підтримки;

б) забезпечення її захищеності та конфіденційного характеру рішень, що приймаються;

в) забезпечення швидкої, ефективної та безпомилкової роботи в режимі діалогу з її ресурсами завдяки зменшенню складності організації та використання ресурсів;

г) зниження вартості її програмного забезпечення;

д) забезпечення її розвитку, розширення та гнучкості.

Ефективна інформаційна робота аналітичних служб істотно пов'язана з тим, що інформація, яка надходить, має використовуватися для оптимізації рішень, що приймаються, і розглядатися як важливий ресурс цього процесу. При цьому забезпечувати узгодженість і несуперечність цілей, що ставляться на всіх рівнях управління, контролювати їхнє додержання та приймати рішення щодо забезпечення їхнього досягнення має скоординована система показників та затверджених методик їх розрахунку як аналітичної бази.

Для забезпечення складання прогнозних розробок з використанням ітераційних підходів, теоретико-ігрових моделей тощо потрібне коло фахівців, що володіють відповідною методологією та здатні застосовувати її до аналізу ситуації, що змінюється. Зокрема для цього у системі державних органів необхідна розвинена структура відповідних консультативно-аналітичних організацій.

Цінність аналітичної складової полягає у тих знаннях, які становлять найбільш важливий досвід органу влади, його інтелектуальний капітал, і з часом вона зростає. Знання, які генеруються аналітичною складовою і інтегруються в базу знань, є знаннями-зразками, що реалізують конкретні методи, методики, технології дій, залежно від розвитку проблемних ситуацій у предметній сфері (рис. 5.27).

Узагальнення досвіду створення та використання різних ІАС свідчить, що найбільш ефективним підходом для розробки АІАС з аналітичною складовою є підхід, оснований на використанні продуктивних знань, тобто таких, які дозволяють отримати якісно нові споживчі властивості АІАС у цілому. Виявлення продуктивних знань можливе при спеціальному функціонально-фізичному аналізі діючої АІАС чи тієї, яка тільки проектується, при спільній роботі фахівців-користувачів АІАС і її розробників.

Для використання проблемно-орієнтованих алгоритмів роботи з різними видами продуктивних знань необхідно сформувати відповідні бази продуктивних знань. Формалізація, яка застосовується при формуванні баз продуктивних знань, дозволяє ефективно маніпулювати цими

знаннями, а їх поєднання не з об'єктом, де вони впроваджуються, а з функціями, які наявні в тезаурусі функцій і властивостей, робить цей підхід до проектування АІАС та її складових достатньо універсальним, що може використовуватися при розробці АІАС у будь-якому органі влади [218].

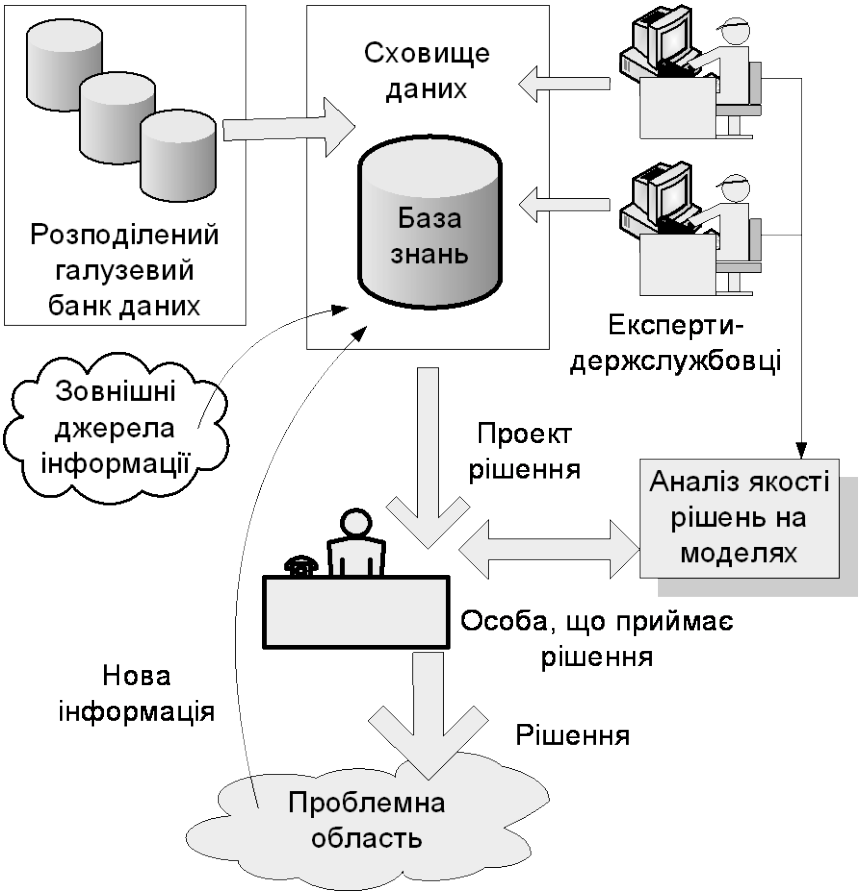

Рис. 5.27. Схема прийняття рішень з використанням аналітичної складової

Для ефективної роботи зі знаннями необхідно визначитися щодо методу опису знань і правил конструювання таких описів. Найчастіше для моделювання знань використовуються методи штучного інтелекту,

гіпертекст, методи моделювання бізнес-процесу (CASE-системи), карти понять.

За останні роки з'явилася низка нових засобів підтримки аналітичної діяльності в інформаційних системах, а саме:

1) DSS — система підтримки прийняття рішень (Decision support system);

2) ESS — система підтримки виконання (Executive support system);

3) KWS — система роботи зі знаннями (Knowledge work system);

4) MIS — адміністративна інформаційна система (Management Information System);

5) OAS — система автоматизації діловодства (Office automation system);

6) PSS — система планування робіт (Project scheduling system);

7) TPS — система обробки трансакцій (Transaction processing system).

Основою аналітичної діяльності в АІАС повинні стати спеціалізовані СППР на базі багатовимірних сховищ даних (OLAP-технології). Такі системи мають вмонтовані засоби, які можуть застосовуватись для проведення необхідного аналізу та підтримки прийняття рішень керівним складом органу державної влади.

OLAP-орієнтовані системи підтримки прийняття рішень можуть забезпечувати аналіз стану галузей у наступних напрямках:

а) контроль (моніторинг) стану галузі на основі базових і агрегуємих показників процесів, що відбуваються в галузі;

б) оцінка стану галузі на основі планових, фактичних і прогнозуємих показників;

в) виявлення залежностей між процесами та оцінка їхнього взаємовпливу;

г) багатоваріантне прогнозування розвитку ситуацій, пов'язаних з процесами, що аналізуються;

д) розрахунок макропоказників стану галузі на основі знань про процеси, що проходять у галузі;

е) вироблення оптимальних керівних рішень для досягнення необхідного рівня стану галузі.

В аналітичній роботі найважливіше значення мають дані, які повинні бути структуровані, узгоджені, достовірні, доступні. Пошук, «здобування», накопичення, збереження, відбір та надання користувачам релевантної інформації щодо їхніх задач виконують інформаційно-

пошукові системи. У цих системах, крім OLAP, можуть використовуватися такі технології:

- тематичних та інтеграційних сховищ даних на основі стандарту XML (Software AG Tamino, Microsoft Biz Talk);
- систем класифікації інформації і ведення каталогів (Microsoft Commerce Server);
- систем керування контентом (Microsoft Site Server);
- пошукових систем (Oracle Inter Text, Microsoft Index Server), здобування даних (Data Miting);
- геоінформаційних систем (ГІС, GIS);
- систем, які самонавчаються, на базі нечітких алгоритмів;
- лінгвістичних систем.

Отже, для забезпечення інформаційно-аналітичної діяльності в підрозділах ОДВ необхідно наступне:

1) створення аналітичної моделі системи, яка підтримує сформульовані вище напрямки аналізу;

2) створення моделі даних на основі технології сховищ даних;

3) розробка засобів аналітичної обробки даних на основі OLAP-технології;

4) використання сучасного програмного забезпечення, призначеного для проектування, створення та супроводження аналітичних досліджень.

Зазвичай аналітична модель будується на основі багатовимірної логічної моделі даних із використанням базових, агрегуємих (на основі ієрархії вимірів) та обчислювальних показників стану галузі (рис. 5.28).

Ці показники використовуються для побудови макропоказників і розробки критеріїв оцінки стану галузі. Основні об'єкти багатовимірної моделі даних — показники, виміри, ієрархії, OLAP-куби.

Модель даних в АІАС має будуватися на основі наступних понять:

а) джерела даних, зокрема, дані підпорядкованих організацій ОДВ, а також й інші зовнішні системи, в тому числі з Інтернету;

б) проміжні дані, які містять детальну та частково агреговану інформацію за певними напрямками діяльності ОДВ;

в) сховище даних на основі багатовимірної бази даних для оперативного аналізу даних і підтримки прийняття рішень;

г) функціонально-орієнтовані сховища (в складі сховища ОДВ) у відповідно до того напрямку, за яким виконується аналіз;

д) метадані.

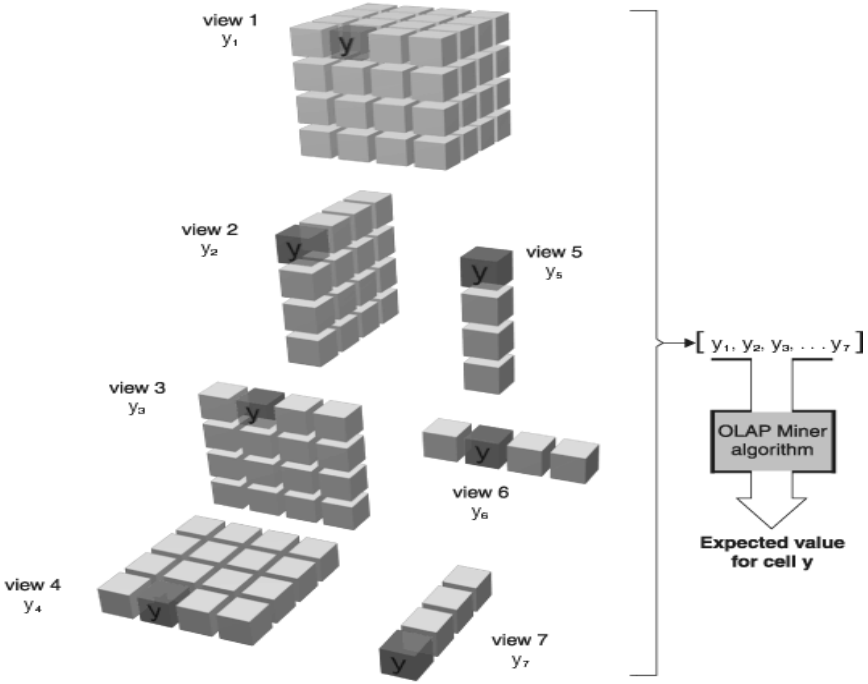

Рис. 5.28. Приклад схеми опрацювання даних із застосуванням OLAP-технології для побудови макропоказників і розробки критеріїв оцінки стану галузі

Підсистема запитів і подання даних має містити таке програмне забезпечення:

1) складних нерегламентованих запитів користувачів на основі технології MOLAP (моніторинг, аналіз і оцінка стану галузі на основі агрегування даних та обчислення показників);

2) добування знань, яке реалізує складні статистичні алгоритми і алгоритми пошуку прихованих закономірностей, подання цих закономірностей у вигляді моделей і багатоваріантного прогнозування з розвитку ситуацій за схемою «Що якщо…?»;

3) для вироблення оптимальних керуючих рішень.

Унікальні можливості для вироблення рекомендацій з прийняття рішень надає побудова СППР на базі геоінформаційних технологій (рис. 5.29).

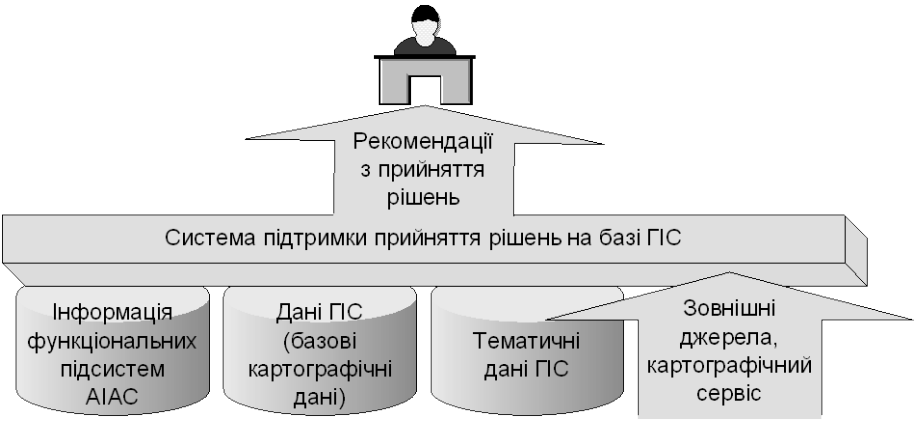

Рис. 5.29. Консолідація різнорідної інформації для підтримки СППР

Застосування ГІС-технологій для підтримки прийняття рішень. Впровадження ГІС-технологій для забезпечення інформаційно-аналітичної діяльності органів державної влади є достатньо складною комплексною проблемою. Тому нагальним завданням є не лише визначення таких шляхів організації інформації, які б дозволили ефективно її знаходити, видобувати і використовувати, а й напрямків комплексного використання ГІС.

Питання використання ГІС-технологій у спеціальних виробничо-технічних напрямках (екологічний моніторинг, надзвичайні ситуації, проектування й управління комунікаціями, управління і моніторинг землекористуванням, обладнання родовищ нафти і газу і т.ін.) достатньо добре освоєні, широко застосовуються в зарубіжних країнах і в Україні.

Одначе при локальному застосуванні ГІС-технологій неминуче можуть виникнути труднощі в організації, зберіганні, актуалізації і спільному використанні різнорідних баз даних і програмного забезпечення. За умови створення в органі державної влади єдиної концепції впровадження інформаційних технологій є можливість їх послідовного модульного впровадження на окремих робочих місцях, з використанням загальних баз даних, залежно від поставлених задач і фінансових можливостей. Це в подальшому призведе до переродження порівняно малопотужних систем, що виконують ряд локальних задач, у потужний інформаційно-аналітичний інструмент на базі сучасних інформаційних тех-

нологій. При цьому конкретні результати мають з'являтися вже з моменту впровадження першого елементу системи.

Впровадження ГІС-технологій оптимально виконувати в 3 етапи:

1) використання найпростіших функцій ГІС на локальних робочих місцях:

2) застосування ГІС з використанням єдиної просторової і атрибутивної бази даних;

3) інтегрування ГІС зі спеціалізованими аналітичними системами.

За всією різноманітністю задач, що можуть розв'язуватися підрозділами органу державної влади за допомогою ГІС, у них виділяються загальні напрямки:

1) відображення на картографічній основі об'єктів інтересу органу державної влади;

2) відображення на картографічній основі у вигляді ділової графіки (локалізовані діаграми, графіки, таблиці, растрова інформація та ін.) соціально-економічних показників, що знаходяться в базах даних різноманітних систем;

3) вирішення питань оптимізації транспортних потоків, розміщення об'єктів галузі, скорочення витрат та ін.;

4) аналіз і планування діяльності галузі в регіонах за заданими параметрами;

5) розповсюдження картографічної інформації серед об'єктів галузі по комп'ютерним мережам.

За виробничо-технологічним напрямком доцільно розпочати застосування ГІС у сферах управління виробничими процесами та аналізу оперативної ситуації у виробничих підрозділах на рівні підприємств, екологічного аналізу розповсюдження дільниць забруднення, оцінки фінансових ризиків і виробничої безпеки, контролю за експлуатацією комунікацій (трубопроводи, ЛЕП, лінії зв'язку), вибору альтернативних шляхів транспортування продуктів при аваріях вузлових об'єктів мереж, визначення черговості процедур перекриття трубопроводів, оцінки витоків і їхніх наслідків і т.ін.

Впровадження ГІС у координаційно-фінансово-економічну діяльність необхідно зосередити у першу чергу на підтримку стратегічного планування, подання і аналізу поточної ситуації в галузі для прийняття рішень, аналізу і планування інвестиційних програм, оцінки економічного ризику, врахування об'єктів і аналізу витрат на їхнє утримання, економічного моделювання, аналізу і прогнозування розвитку існуючих

і підготовки нових ринків збуту, оптимізації матеріально-технічного постачання, раціонального розміщення персоналу і технічних засобів.

Підсистеми АІАС повинні бути взаємопов'язані та розроблятися з застосуванням єдиних компонент. Особливо це стосується такої інтеграційної складової як ГІС. Як уже зазначалося, значний ефект при організації корпоративної системи, зокрема і в органах державної влади, можуть дати програмні продукти ArcGIS корпорації ESRI.

Нову істотно дороблену версію представляє сімейство ArcGIS 9. У цих продуктах пропонується розвинене середовище геообробки та технологія глобальної 3D візуалізації.

ArcGIS 9 побудована на основі стандартів комп'ютерної галузі, до яких також належить об'єктна архітектура COM, .NET, Java, XML, SOAP, за рахунок чого забезпечується підтримка загальноприйнятих стандартів, гнучкість пропонованих рішень, широкі можливості взаємодії й спільної роботи, створення різноманітних сервісів.

Фундаментальна архітектура ArcGIS 9 забезпечує впровадження ГІС-функціональності та бізнес-логіки (процедур використання просторових даних) у різних прикладних сферах, на різних рівнях організації роботи — на персональних комп'ютерах, на серверах, через Web, у польових умовах. Підтримується як робота окремих користувачів, так і багатокористувальницький режим обробки і аналізу даних. Структура ArcGIS 9 складається з наступних основних блоків:

1) настільні ГІС-продукти (Desktop GIS) — ArcReader, ArcView, ArcEditor, ArcInfo, а також додаткові модулі ArcGIS (Spatial Analyst, Network Analyst, 3D Analyst та ін.);

2) серверні ГІС — ArcGIS Server, ArcIMS і ArcSDE. Вони дозволяють підтримувати й поширювати просторові дані в межах великих організацій або багатьом іншим користувачам через Інтернет;

3) ГІС, що вбудовуються — ArcGIS Engine. Це бібліотека компонентів для розроблювачів ГІС;

4) Мобільні ГІС — пакет ArcPad, що встановлюється на мобільних пристроях з підтримкою GPS;

5) ArcObjects — загальна модульна бібліотека ГІС-компонентів, що вбудовуються.

Можливу загальну схему засобів організації обробки даних в АІАС з використанням ГІС-продуктів ESRI наведено на рис. 5.30.

За основну компоненту доцільно брати ArcGIS Server у поєднанні з картографічним сервером ArcGIS Internet Map Server та з сервером просторових баз даних SDE (Spatial Database Engine), що розширює

можливості звичайної реляційної бази даних і дозволяє водночас зберігати в єдиній базі величезні обсяги картографічної та атрибутивної (фактографічної) інформації, робити просторові запити і первинний просторовий аналіз. SDE працює з багатьма комерційними системами керування базами даних, такими як Oracle, Informix, Sybase, DB2 і MS SQL Server, використовуючи відкриті стандарти і реальну клієнт/серверну архітектуру.

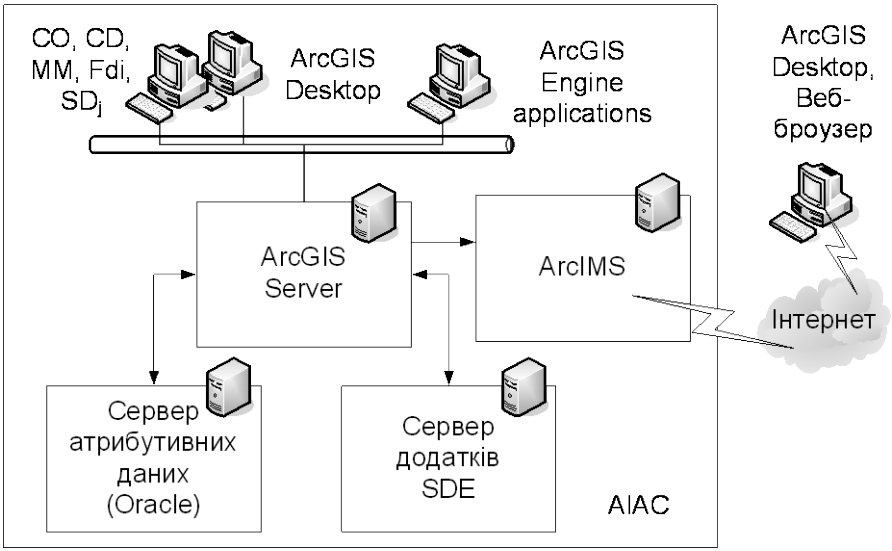

Рис. 5.30. Загальна схема засобів організації обробки даних в АІАС із використанням ГІС-продуктів ESRI

Архітектура та програмне забезпечення аналітичної складової. Як зазначалося, «клієнтська» орієнтація «бізнес-процесів» є визначальною у методах автоматизації управлінської діяльності. АІАС має базуватися на трирівневій архітектурі клієнт–сервера, що зумовлює існування трьох основних компонентів (рис. 5.31), а саме:

1) сервера системи керування базами даних;

2) сервера застосувань — відповідає за взаємодію інших компонентів системи та сторонніх систем з системою управління базами даних (оброблює запити від користувачів і формує відповіді на запити згідно даних системи);

3) автоматизованого робочого місця користувача системи, що реалізує інтерфейс кінцевого користувача системи (формує запити та відображає відповіді).

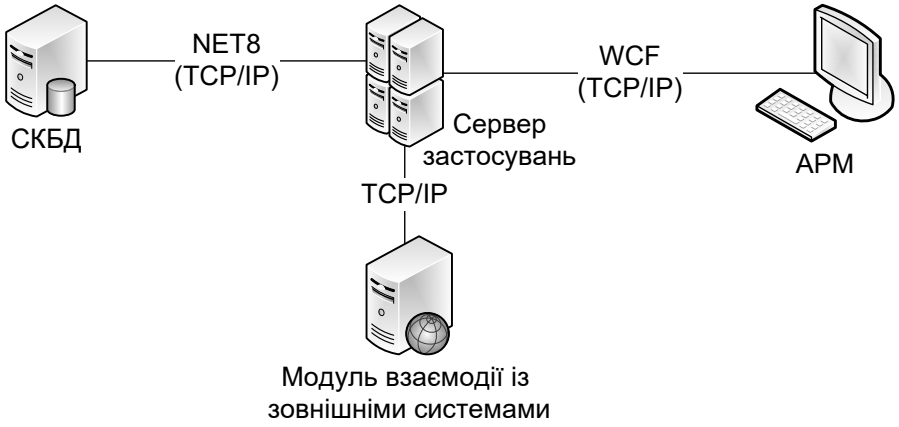

Рис. 5.31. Схема взаємодії компонентів АІАС

Таку систему доцільно розробляти на технологіях Microsoft WCF (Windows Communication Foundation) та Entity Framework (.Net Framework 3.5 SP1), що виводить АІАС на рівень індустріальної платформи для розвитку та майбутньої інтеграції компонентів інших виробників. Як середовище для забезпечення зв'язку між зазначеними компонентами використовується Ethernet-мережа передачі даних.

Технологічно сервер СКБД функціонує автономно та не ініціює сеансів зв'язку. Сервер застосувань є ініціатором з'єднань лише з СКБД, для чого використовується протокол NET8, розроблений компанією ORACLE. Як транспортний протокол використовується TCP/IP. Автоматизовані робочі місця та модуль зв'язку із зовнішніми системами для зв'язку із сервером застосувань використовують WCF, а як транспортний протокол — TCP/IP.

ПЗ аналітичної складової має розроблятися як універсальний інструмент для аналітиків, що самі можуть створювати програми для розв'язання аналітичних задач. Задачі аналізу проблемних ситуацій потребують саме наявності такого виду аналітичної складової в АІАС, оскільки цей інструментарій дозволяє коректно провести декомпозицію

проблеми, з'ясувати основні взаємозв'язки між цілями і ресурсами, гарантувати об'єктивність рішень.

Аналітичну складову АІАС мають утворювати програмні засоби, які реалізують конкретні методи, методики, технології розв'язання задач, що важко формалізуються. Як методичний інструментарій при створенні аналітичної складової необхідно використовувати евристичні стратегії, тактики, методи конкретної професійної діяльності, виявлення та вирішення протиріч різної природи та походження, систематизації функцій і властивостей технологій, інформації тощо. У цих випадках суттєве значення має застосування експертних систем. При цьому бази знань експертних систем повинні містити інформаційне середовище різних відомств, що дозволяло б формулювати до них складні запити логічного порівняння за множиною полів різних сегментів.

Також необхідно передбачити забезпечення аналізу стану суспільних процесів шляхом відеоконференцій, із залученням необхідних технічних та програмних засобів колективного обговорення та прийняття рішень.

Як приклад можна привести рішення зі створення СППР в ІАС НКРЗ. Ця система має забезпечити керівництво, зокрема Національної комісії з питань регулювання зв'язку України, аналітичною інформацією з урахуванням її характеру, важливості, оперативності, періодичності та конфіденційності з метою своєчасного прийняття обґрунтованих, взаємоузгоджених рішень, спрямованих на найбільш ефективну стратегію розвитку галузі зв'язку, на основі залучення експертного оцінювання та комплексу математичних методів і програмних засобів оптимізації, моделювання, прогнозування та передбачення для різних галузей практичної діяльності та побудованої на цій основі людино-машинної системи обробки та аналізу великих обсягів інформації різної природи.

Система складається з наступних частин (рис. 5.32):

- підсистеми первинного збору даних;
- аналітичного блоку;
- підсистеми керування інформаційними процесами;
- інтерфейсу користувача;
- бази даних для збереження інформаційних об'єктів.

Втілити СППР має «Ситуаційна зала» Національної комісії з питань регулювання зв'язку України. Новітня концепція побудови ситуаційних кімнат, що застосовується у багатьох корпораціях, полягає у використанні ідеї взаємодії керівників вищого рівня із групою інтерактивного супроводу та на використанні найновіших сучасних електрон-

них засобів подання та виведення інформації. Територія ситуаційної зали поділена на сегменти групової роботи за допомогою візуальних елементів дизайну та фізичних перегородок (рис. 5.33), що формують робочі зони.

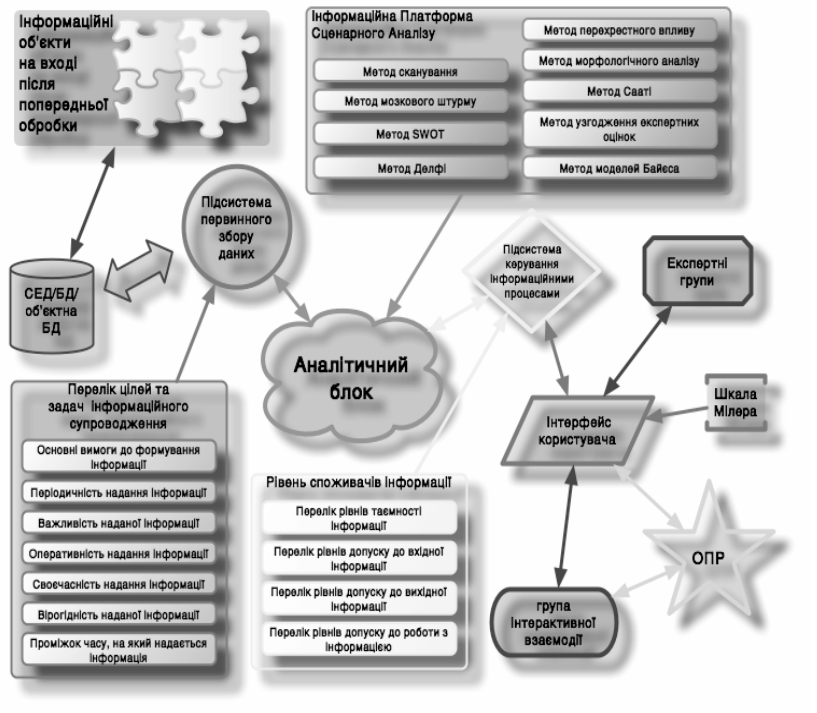

Рис. 5.32. Функціональна схема підсистеми аналітичного супроводження підготовки і прийняття рішень ІАС НКРЗ

Підсистема підтримки прийняття рішень потребує мінімального вводу інформації та працює у діалоговому режимі, що є найзручнішим для користувачів. Для осіб, що забезпечують технічну підтримку користувачів та для операторів, що відповідають за вивід інформації, передбачені спеціальні робочі місця із засобами керування технікою та планування подіями. Крім того, завдяки залученню сучасних засобів відеоконференцзв'язку та IP-телефонії, можливі сеанси віддаленої роботи та нарад, а також онлайнові телеконференції та консультації.

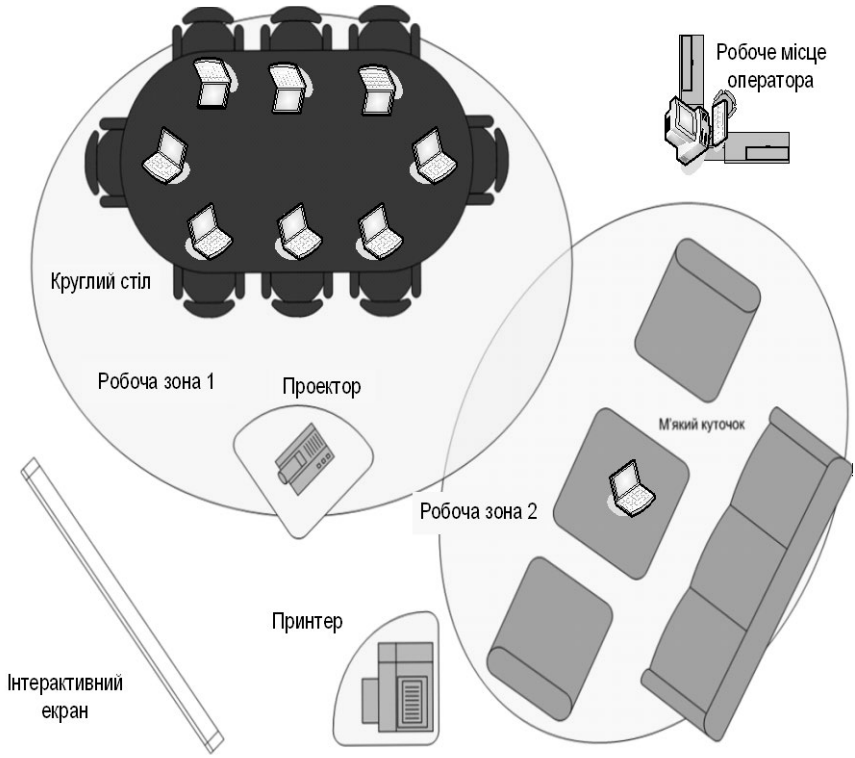

Рис. 5.33. План ситуаційної зали ІАС НКРЗ

Таким чином, запропонована система надасть можливість особам, що приймають рішення на різних рівнях управління в галузі зв'язку, отримати інформацію у режимі реального часу для прийняття максимально обґрунтованих стратегічно важливих рішень.

Наступним рішенням, направленим на зниження обсягів адміністративної роботи й оптимізацію роботи державних служб в умовах автоматизації («електронізації») документообігу, має стати методологія забезпечення спільної роботи над документами на базі Інтернет-технологій із використанням внутрішнього («корпоративного») веб-порталу. Органи влади, перш за все місцеві і регіональні, мають використовувати методологію *надання онлайнових послуг* за допомогою центрів телефонного обслуговування (Call-центрів), веб-порталів, Інтернет-приймалень та ін.

Тому схема обробки інформації в АІАС органу державної влади має бути зорієнтована на Інтранет/Інтернет-технології [219] і використання в АІАС рішень на базі відкритих стандартів, таких як XML. У цьому сенсі важливе значення має використання портальних технологій (рис. 5.34).

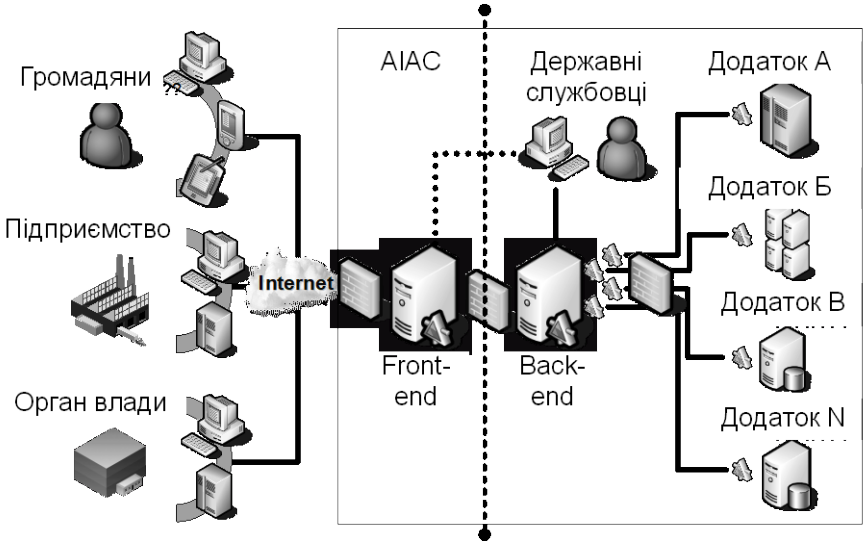

Рис. 5.34. Схема обробки інформації та розв'язання функціональних задач в АІАС, зорієнтована на Інтранет/Інтернет-технології

Портал, що структурований за тематичними розділами, дозволяє забезпечити його використання як сукупності посилань на високоякісну інформацію. Портал є ієрархічним деревом зон («areas»), кожна зона порталу уявляє собою окремий сайт. Зони об'єднані разом загальною навігацією й централізованим керуванням. Розширювані шаблони публікації дозволяють формувати посилання й зміст, спрямовані на визначену аудиторію («Audience»), а також забезпечувати спрощений процес публікації інформації — запропонована, затверджена, застаріла.

Як приклад організації порталу доцільно розглянути рішення щодо галузевого веб-порталу в ІАС Держкомзв'язку. При розробці порталу за основу були взяті вимоги діючих нормативних документів, що регламентують порядок оприлюднення в мережі Інтернет інформації про діяльність органів виконавчої влади, перелік і порядок надання інформа-

ційних та інших послуг із використанням електронної інформаційної системи «Електронний Уряд» (рис. 5.35).

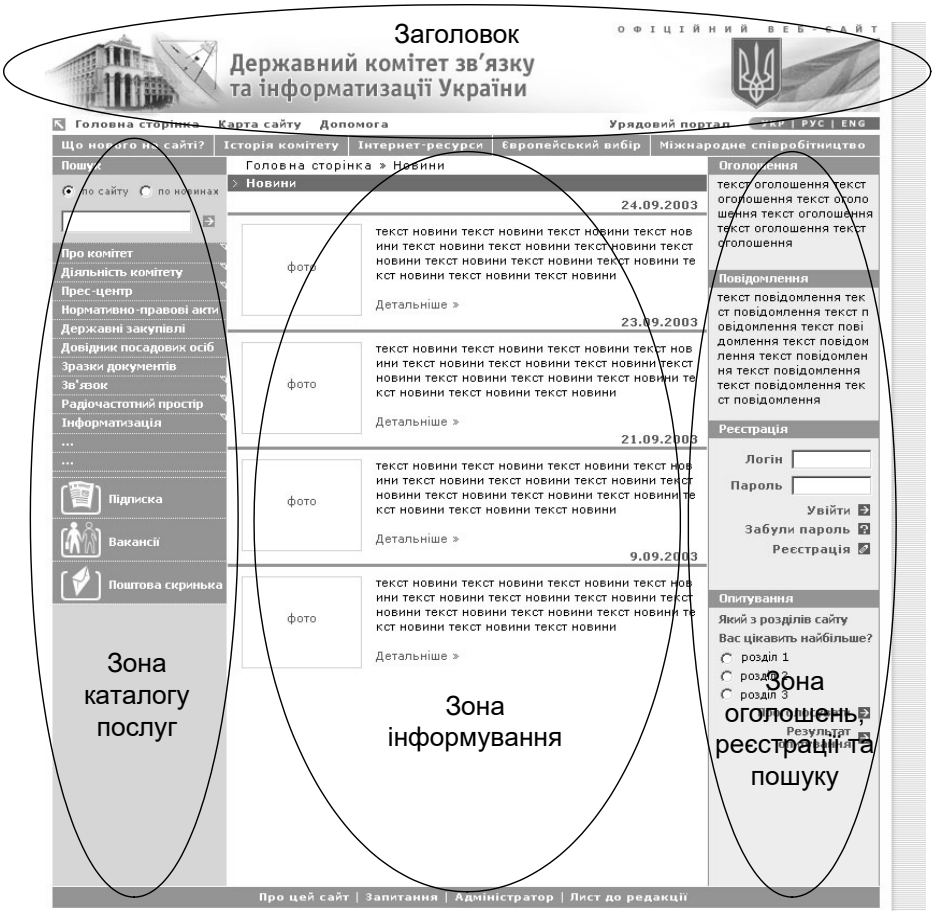

Рис. 5.35. Загальний дизайн головної сторінки веб-порталу органу влади

Веб-портал спрямовувався на надання доступу до інформації про підприємства, установи та організації, що належать до сфери управління Держкомзв'язку; про цільові програми у відповідній сфері; інформаційні ресурси з питань, що належать до компетенції Держкомзв'язку; поточні та заплановані заходи і події у відповідній сфері; відомості про наявні вакансії; новини про події, що сталися та щоденну інформацію.

Особливе значення має наявність зворотного зв'язку — публікація матеріалів телефонних гарячих ліній по актуальним питанням, запис прямих ефірів на телебаченні і радіо, розміщення узагальненої інформації про роботу зі зверненнями громадян, система онлайнових форумів і проведення голосувань. На галузевому веб-порталі передбачено представлення інформаційних послуг, що розподілені за категоріями користувачів, а саме — громадянам, юридичним особам, держслужбовцям, міжнародній спільноті. В умовах функціонування електронного уряду значна увага має бути приділена опрацюванню запитів громадян до органу влади. Такі запити мають надходити через Інтернет, але доцільно також організувати й опрацювання запитів у вигляді SMS, що можуть надходити від абонентів мобільного (рухомого) зв'язку (рис. 5.36).

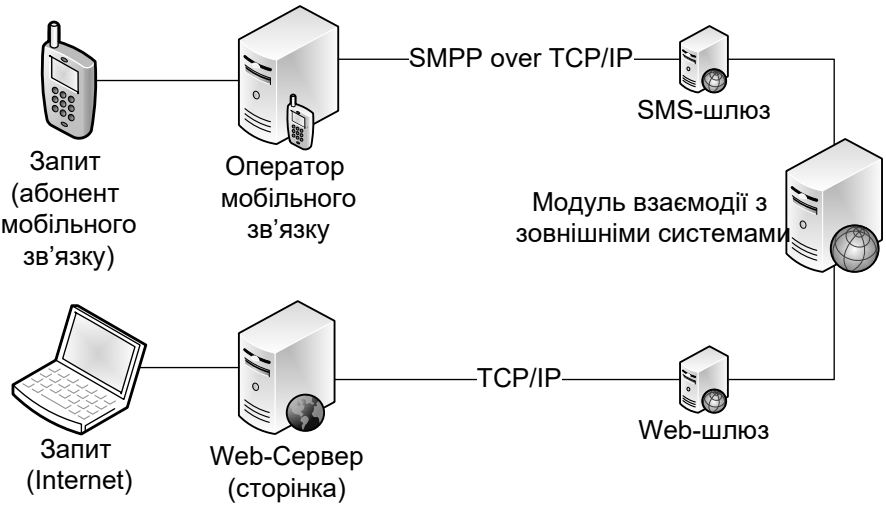

Рис. 5.36. Схема опрацювання в АІАС запитів громадян

Забезпечення регулювання виконавчої обов'язковості. Як зазначалось, одним із основних завдань АІАС є вичерпна інформаційна підтримка рішень. На концептуальному рівні пропонується методологія забезпечення виконання політики ВО, яка має поєднувати (інтегрувати) окремі підсистеми, АРМи експертів і зовнішні інституції через керований *процес опрацювання документів (ПОД)*, який є анало-

гом поняття «бізнес-процеси» (Business Process — BP), що використовується при автоматизації управління підприємствами (рис. 5.37).

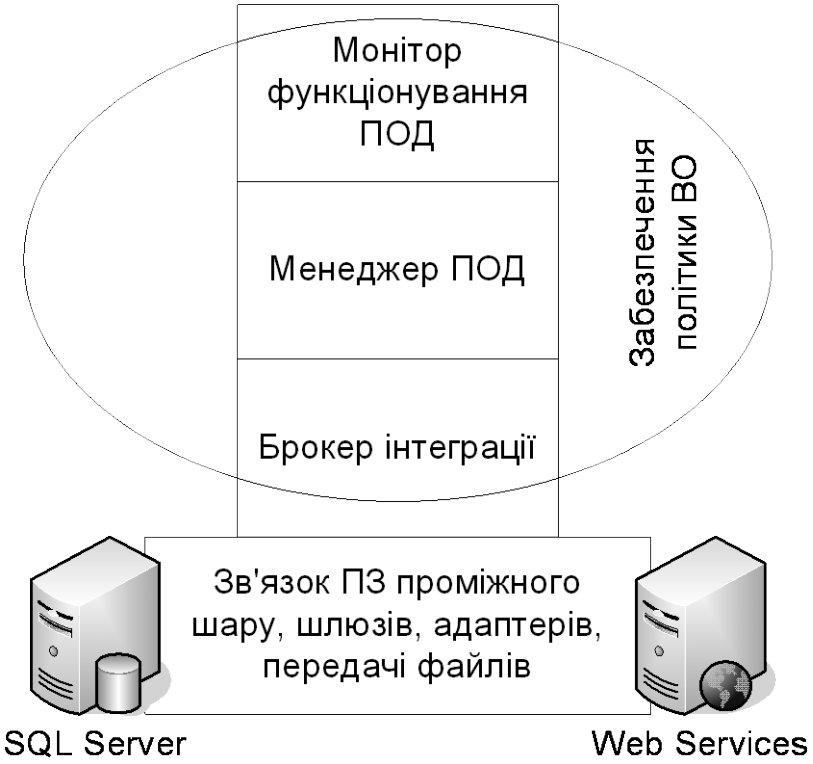

Рис. 5.37. Архітектура засобів забезпечення політики ВО

При цьому мають застосовуватись стандартизовані інтерфейси до функціональних можливостей системи, стандартизовані зв'язки із підсистемами та стандартизоване подання даних ПОД, знань і власне самих процесів. Основним механізмом має бути регулювання й сполучення веб-послуг (Web Services), що базується на архітектурі публікації та підписки (Pub/sub architecture) (рис. 5.38).

Процес, направлений на опрацювання визначеного документа, підписується на певну інформацію (інші документи, публікація у веб, аналітика зі сховища даних), що вибираються з так званого вхідного конвеєра інформації (Receive Message Pipeline), опрацьовуються за підпискою та подаються до вихідного конвеєра інформації (Send Pipeline), з

якого інформацію отримують АРМи експертів, що розглядають дану проблему (документ). При цьому ця конфігурація виконує шляхом використання механізмів ситуаційного регулювання збалансування навантаження (Load Balance) та відстеження ситуацій у режимі реального часу.

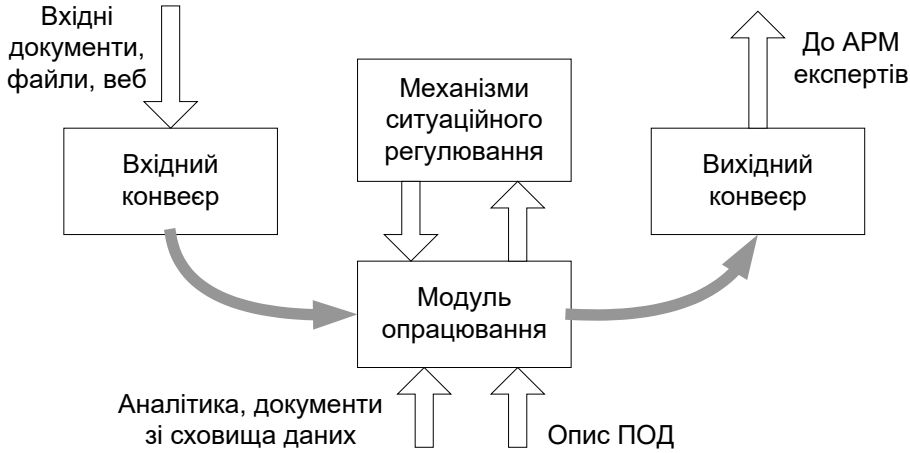

Рис. 5.38. Архітектура публікації та підписки ПОД

Як стандарт для моделювання та опису ПОД доцільно використовувати нотацію моделювання бізнес-процесів BPMN (Business Process Modeling Notation), що розроблена організацією Business Process Modeling Initiative (BPME.org) та зараз отримує визнання[67]. Це виправдано тим чинником, що BPM-системи підходять саме для розробки ефективних бізнес-процесів, які повинні швидко реагувати на умови, що постійно змінюються.

Основне призначення BPMN полягає в наданні нотації, легкої у використанні й розумінні для користувачів, серед яких аналітики, що моделюють бізнес-процеси, технічні розробники, які створюють системи автоматизації підтримки цих процесів, а також керівники різних рівнів, які повинні швидко читати й розуміти процесні діаграми, щоб приймати рішення.

BPMN прямо відображається на мови виконання бізнес-процесів, такі як BPEL (Business Process Execution Language) і BPML. BPMN на-

[67] Bhagat Nainani, переклад в «Oracle Magazine/Русское издание».

дає нотацію для моделювання, а BPEL є мовою опису виконання процесів.

При розробці BPEL скористалися такими концепціями, як WEB Services/WSDL — як компонентна модель, XML — як модель даних, ієрархічне керування винятковими ситуаціями та ін.

Про ефективність використання цього стандарту свідчить той факт, що корпорація Oracle розробила і поставляє такі засоби моделювання й імітації як Oracle BPEL Process Manager і інструмент Oracle Business Activity Monitoring. При цьому застосовується BPMN і експорт у форматі BPEL для розгортання на платформі Oracle. Також система Oracle AS Integration є в цей час найбільш повною BPM-платформою, що забезпечує реалізацію всього життєвого циклу процесу, включно з моделюванням, імітацією, впровадженням, виконанням, моніторингом і оптимізацією процесів [220].

До ключових особливостей BPMN відноситься й те, що BPMN надає нотацію моделювання, що забезпечує перехід від бізнес-визначень до карти виконання процесу (process execution map). Нотація BPMN є розширюваною й дозволяє використовувати асоціації й анотації для встановлення взаємин з іншими артефактами усередині або поза системою. Наприклад, можна співвіднести бізнес-процеси з функціями, які вони виконують, з даними, які вони використовують, із системами, на яких вони розгорнуті, і т.ін.

Інституційні складові. Як було відмічено, враховуючи значні масштаби, які набуває така система, як АІАС, забезпечення її функціонування та генерацію аналітики доцільно покладати на Інформаційно-аналітичний центр (ІАЦ) органу влади. ІАЦ забезпечує багатоступеневий процес генерації аналітичної інформації, проведення фундаментальних і прикладних досліджень з проблематики управління галуззю, з розробки, створення й тиражування нормативно-правових, методичних документів зі сфери діяльності органу влади.

ІАЦ організаційно зазвичай є підпорядкованим підприємством органу влади, і його організаційна структура визначається характером та тематикою аналітичних досліджень, науково-дослідних робіт, а також масштабами АІАС. Функціонально ІАЦ має бути пов’язаним з усіма підрозділами органу влади, з науково-дослідними та навчальними інституціями галузі, країни, а також країн ближнього та далекого зарубіжжя, що мають відношення до сфери діяльності галузі.

Основні функції ІАЦ полягають у наступному:

- інформаційна, аналітична та наукова підтримка діяльності органу влади;
- впровадження сучасних комп'ютерних технологій, підтримка функціонування, розвиток та модернізація АІАС;
- забезпечення інформаційної безпеки в АІАСРЗ, зокрема в надзвичайних ситуаціях і особливий період;
- наукове супроводження, підготовка до впровадження та тиражування нормативно-правових документів зі сфери діяльності органу влади;
- розробка системи показників формування статистичної звітності в галузі відповідно до міжнародних вимог;
- забезпечення виконання функцій центру сертифікації ключів, засвідчувального центру системи електронного цифрового підпису для органу влади;
- забезпечення ведення галузевого веб-порталу та внутрішнього Інтранет-сайту;
- забезпечення видавничої діяльності;
- забезпечення консультативного обслуговування учасників галузевого ринку та споживачів послуг, зокрема стосовно виконання нормативних актів органу влади;
- забезпечення проведення конференцій, семінарів, міжвідомчих нарад, участі у міжнародних виставках і конференціях тощо;
- підготовка, перепідготовка та підвищення кваліфікації вітчизняних та іноземних фахівців;
- підтримка міжнародних зв'язків органу влади та взаємодії з міжнародними організаціями.

Згідно з наведеними функціями загальна структура ІАЦ представлена на рис. 5.39.

Як вже зазначалося, на тлі постійно зростаючих обсягів даних і вимог до їхньої якості існуюча система зберігання та обробки даних, що накопичувались роками, вже не може задовольняти потреби працівників та керівництво органу влади, а також його організаціями (підприємствами). Потрібен новий підхід, який полягає у побудові центру обробки даних (ЦОД), що має задовольняти сучасним вимогам. Тема проектування й будівництва ЦОД є дуже актуальною. Кількість таких центрів стрімко зростає в усьому світі.

Створення та підтримка функціонування ЦОД (розробка структури ЦОД й алгоритмів функціонування його різноманітних служб, роз-

робка програмних засобів, баз даних, підтримка функціонування тощо) покладається на ІАЦ.

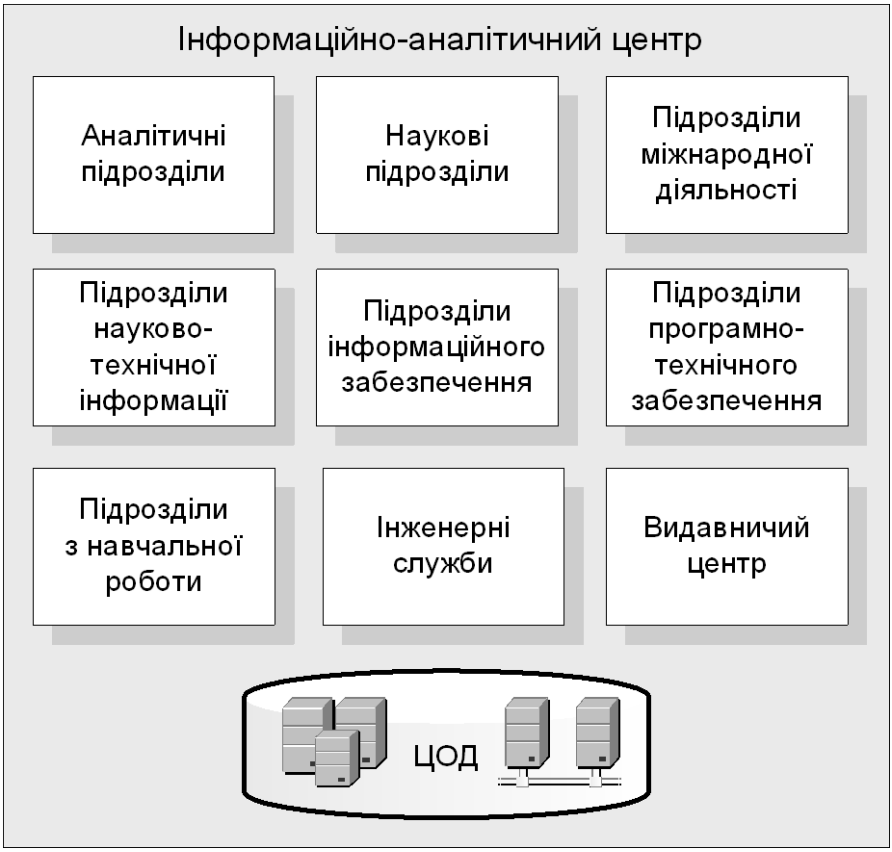

Рис. 5.39. Загальна структура ІАЦ

Сучасні системи зберігання являють собою складні ієрархічні структури, що нараховують 15 і більше підсистем і показують життєві цикли різних видів інформації. Базою ЦОД є серверні рішення, які зараз набувають стрімкого розвитку. Мова йде, з одного боку, про дво- та чотириядерні системи, 2-, 4- та більш процесорні 64-розрядні архітектури, а з іншого — про консолідацію серверної інфраструктури на основі віртуалізації серверів (рис. 5.40). Перехід до роботи із сервісами та даними веде до утилізації обчислювальних ресурсів і збільшення рівня

навантаження на сервери з метою збільшення ефективності їх використання.

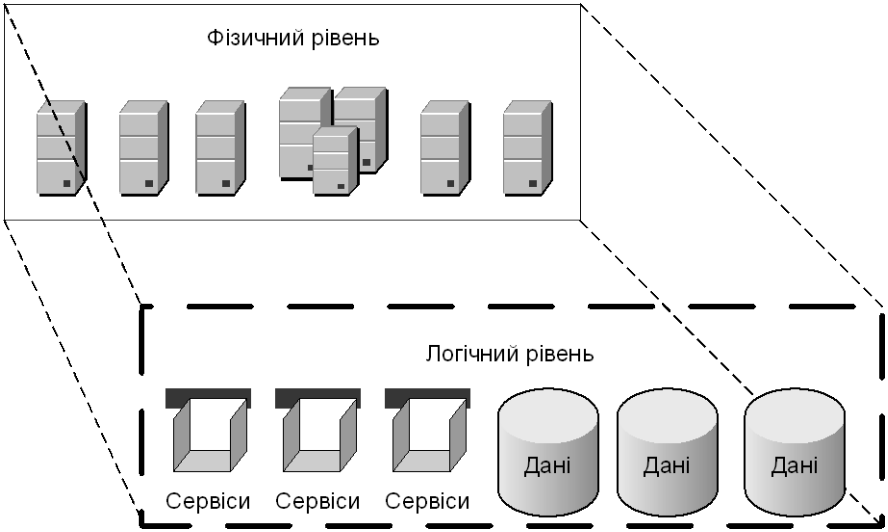

Рис. 5.40. Віртуалізація серверів в ЦОД

Як платформу доцільно використовувати сучасні сервери-лези (blade-сервери), які до того ж забезпечують економію місця, простоту управління, масштабування рішень, відмовостійкість. Прикладом таких засобів є сервери HP Proliant на базі AMD Opteron.

Для реалізації ЦОД необхідно вирішити три основні проблеми:

- продуктивність IT-інфраструктури в цілому;
- розподіленість джерел інформації, місць її зберігання та використання;
- інженерна інфраструктура.

Розрізняються декілька основних моделей ЦОД[68], які пов'язані з методологією застосування серверів — консолідація розрізнених систем, співіснування декількох додатків у рамках однієї системи тощо. Найскладнішою, але й найефективнішою моделлю є віртуалізація на вимогу серверів або додатків у мережі («динамічні ЦОД»).

[68] За ідеологією компанії Intel.

Згідно з даною концепцією, ЦОД органу влади може бути побудований за другою і навіть третьою моделлю складності, яка відноситься до тих компаній, вимоги яких до ІТ-систем зазвичай обмежені рамками можливої працездатності протягом нормального робочого часу («5×8»), коли є можливість робити планову зупинку ІТ-систем для проведення регламентних робіт, та які працюють у режимі онлайн через Інтернет, не пов'язаному із серйозними штрафами за якість надаваного сервісу.

Найбільш складним питанням для системної інтеграції є вимоги до продуктивності ІТ-інфраструктури. А найбільш капіталоємними є інженерні системи ЦОД, основні з яких — приміщення, електроживлення й відведення тепла від навантаження. На цей час має місце формула 1 кВт потужності = 1 кВт охолодження, тобто потужність процесорів вимагає рівного споживання енергії на заходи з відведення тепла, кондиціювання тощо.

Сучасні інженерні системи містять у собі також системи заземлення, пожежогасіння, контролю доступу, моніторингу параметрів середовища і т.ін. При цьому обсяги електроживлення та тепловиділення становлять на сьогодні одну з основних проблем інженерного рішення.

Вихід бачиться у використанні гнучких ІТ-інфраструктур, що адаптуються до змін. Для скорочення витрат на підтримку інженерної інфраструктури необхідно використовувати модель ЦОД, орієнтовану на масштаби й характер використання. Для цього доцільно, враховуючи вартість розгортання й розширення, експлуатацію, обслуговуючий персонал, наявність WAN-каналів зв'язку, близькість до органів влади тощо, створювати великі державні міжвідомчі ЦОД, що підтримують діяльність цілих груп органів влади.

Також актуальним залишається питання захисту даних і у цьому сенсі — скорочення витрат на ЦОД. Наприклад, центр із повним резервуванням (рівень 4 з готовністю 99,995 %) коштує у два з половиною рази дорожче простого ЦОД (рівень 1).

На сьогодні чимало компаній пропонують рішення для побудови ЦОД, навіть «коробкові» варіанти. Так, для вибраної моделі ЦОД може бути використано архітектуру InfraStruXure на базі нової моделі джерел безперебійного живлення Smart-UPS VT від компанії APC. Це рішення дозволяє знизити вартість утримання ЦОД за рахунок скорочення займаної площі й зменшення витрат на установку, функціонування й масштабування.

5.5. Основні вимоги до телекомунікаційного середовища АІАС

Згідно з тим, що відомчі структури органів влади зазвичай є розподіленими, а АІАС слід розглядати як інформаційно пов'язані між собою структурні елементи інтегрованої ІАС держави, підтримка взаємодії між АІАС, її компонентами на різних рівнях (та в межах рівня) покладається на *телекомунікаційне середовище* (ТС).

Аналіз стану розвитку в Україні первинних мереж зв'язку загального користування та спеціального призначення, цифровізації телекомунікаційних технологій, розвитку Інтернет свідчить про наявність необхідної бази для вирішення проблем телекомунікацій для органів влади [221, 222].

З огляду на викладене, формування ТС як кожної АІАС ОДВ, так і ІІАС в цілому є найважливішим завдання інформатизації органів державної влади. Які ж принципи створення ТС АІАС мають цьому відповідати?

У зв'язку з тим, що Інтернет є відкритою мережею, яка сама по собі не може забезпечити гарантовану доставку інформації та її захист, для забезпечення взаємодії АІАС та їхніх елементів із забезпеченням інформаційної безпеки держави виникає необхідність створення окремої інтегрованої транспортної мережі (базової магістралі). Відсутність такої базової мережі створює умови виходу значного обсягу внутрішнього трафіку за межі держави, що, з одного боку, призводить до підвищення цін за надання послуг, а, з іншого боку, може призвести до часткового або повного порушення обміну електронною інформацією між державними установами в межах держави.

Це свідчить про необхідність побудови національної захищеної спеціальної інформаційно-телекомунікаційної системи органів державної влади як багатофункціонального комплексного об'єкта, що забезпечить інтеграцію розрізнених інформаційних ресурсів ОДВ на основі сучасного мережного обладнання, цифрових каналів зв'язку та Інтернет/Інтранет-технології.

Вона, з технічної та технологічної точки зору, має сформуватися в обчислювальну мережу національного масштабу, що спирається на ядро мережі, яке охоплює центральні органи державної влади (рис. 5.41), та мережу доступу для місцевих органів влади.

В Україні вже створено та завершено дослідну експлуатацію Головного комутаційного центру (ГКЦ) Спеціальної інформаційно-теле-

комунікаційної системи органів виконавчої влади (СІТС) як першої ланки Національної системи конфіденційного зв'язку. У рамках створення ядра транспортної мережі в цілому завершено будівництво двох волоконно-оптичних кілець у м. Києві з метою підключення до ГКЦ СІТС абонентських пунктів центральних органів влади.

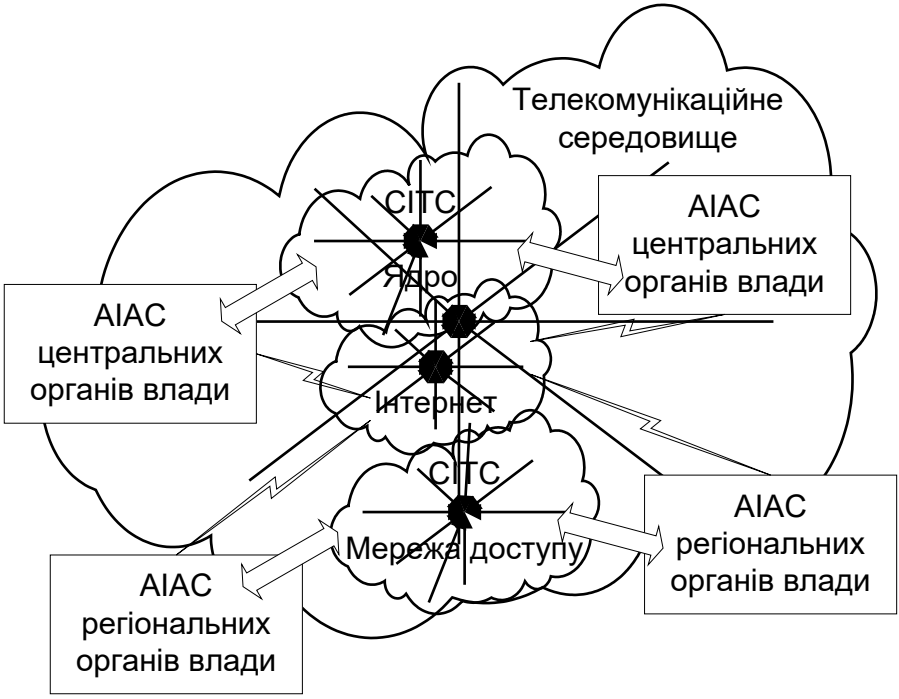

Рис. 5.41. Інтегроване телекомунікаційне середовище органів влади

Водночас майже кожний з органів влади потребує побудови власної спеціалізованої закритої корпоративної телекомунікаційної мережі на базі сучасних технологій як системи передачі даних, створення якої має забезпечуватися за технологіями Інтернет/Інтранет на базі веб-сервісів. Але у цій сфері ще чимало невирішених питань.

По-перше, побудова телекомунікаційного середовища АІАС має здійснюватися згідно з сучасними вимогами до організації, функціонування та розвитку державних корпоративних інформаційно-телекомунікаційних систем, до світових стандартів у галузі телекомунікацій і інформатики, стандартів і рекомендацій відповідного комітету Міжна-

родного союзу електрозв'язку (ITU-T), до принципів Відкритих інформаційних технологій [223].

По-друге, при формуванні телекомунікаційного середовища АІАС необхідно враховувати забезпечення можливостей по нарощуванню та масштабуванню системи; забезпечення надійного обміну повідомленнями всіх видів зв'язку з нормованою якістю обслуговування для категорій користувачів, що встановлюються на телекомунікаційній мережі; забезпечення можливості передачі повідомлень до основних інформаційних напрямків телекомунікаційної мережі не менш ніж за двома незалежними шляхами і наявність резервних каналів; забезпечення належного рівня інформаційної безпеки; забезпечення підтримки централізованої системи управління в режимі реального часу як через саму мережу, так і через мережу загального користування (при виникненні такої необхідності) [224].

Склад задач забезпечення інформаційного обміну між складовими корпоративної мережі АІАС визначається необхідністю комплексного виконання функцій АІАС. При цьому мають реалізовуватися управління мережею шляхом контролю та змін (за необхідністю) режимів функціонування мережі на базі оперативної інформації, а також збирання та накопичення інформації щодо параметрів функціонування програмно-технічного комплексу АІАС з метою аналізу і планування технічних заходів.

Забезпечення таких розширених вимог покладається на підсистему моніторингу та управління об'єктами мережної інфраструктури (рис. 5.42).

Дана підсистема забезпечує функцію візуалізації відомостей про стан мережі та дозволяє швидко перейти до детальних списків подій чи візуальних карт мережі, а графічний інтерфейс наочно відображає стан активних пристроїв мережі та місця виникнення неполадок, що допомагає вчасно знайти і усунути проблеми в роботі мережі.

Як уже зазначалось, ядром АІАС має бути відповідний інформаційно-аналітичний центр (ІАЦ), який є засобом інформаційного супроводу вирішення завдань забезпечення процесів напрацювання та прийняття рішень. Він же є й адміністративним засобом забезпечення управління телекомунікаційної взаємодії ОДВ.

Ураховуючи ієрархічний принцип організації АІАС та її територіальну розподіленість, ТС структурно має являти собою комплекс зв'язку і передачі даних (КЗПД), а архітектурно — глобальну відомчу мережу (ГВМ).

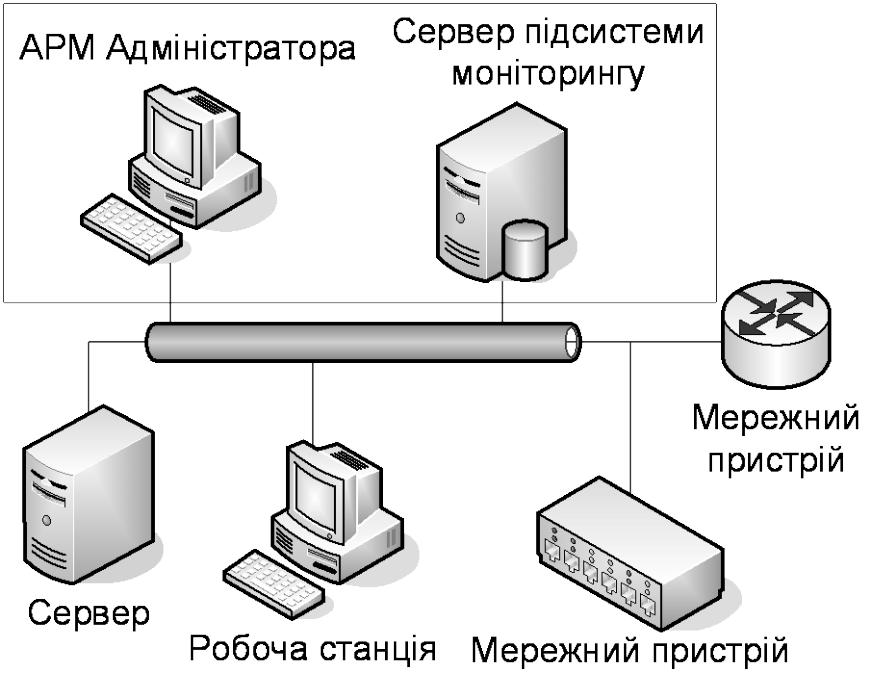

Рис. 5.42. Структурна схема підсистеми моніторингу та управління об'єктами мережної інфраструктури

ГВМ, за сучасними уявленнями, будується з використанням високопродуктивного обладнання комутації повідомлень, з'єднаного виділеними каналами зв'язку, за яких можуть бути (залежно від конкретних умов дислокації і специфічних вимог) використані телефонна мережа загального користування (ТМЗК), цифрові наземні канали (ВОЛЗ, кабельні), канали радіорелейних ліній (РРЛЗ), радіозасоби (стільниковий, транкінговий зв'язок), канали супутникової системи зв'язку (ССЗ).

При цьому особливого вирішення потребує проблема «останньої милі», яка полягає у тому, що фактично з районних установ задовільний зв'язок з областю і центром мають не більше 50 %; особливо гостро стоїть проблема зв'язку з підприємствами та установами, дислокованими окремо.

Таким чином, при створенні ТС ОДВ необхідно вирішувати наступні задачі:

а) створення транспортної інфраструктури з певною продуктивністю;

б) вибір технології міжоб'єктних з'єднань;

в) визначення раціональної структури зв'язків;

г) вибір телекомунікаційного обладнання;

д) визначення мережної структури (вибір протоколу мережного рівня).

Невирішеними частинами загальної проблеми побудови ТС ОДВ є використання стандартів Інтернет/Інтранет-технологій для побудови такого середовища [225]. За допомогою даних досліджень також робиться спроба подальшого розвитку основних положень використання зазначених стандартів.

АІАС органу влади має повноцінно функціонувати в умовах ІІАС. Можна виділити чотири управлінських рівня ІІАС — вищий рівень, рівень центральних органів виконавчої влади та органів управління міста Києва, обласний рівень органів державного управління, Автономної Республіки Крим і м. Севастополя, а також рівень районів та органів місцевого самоврядування (рис. 5.43).

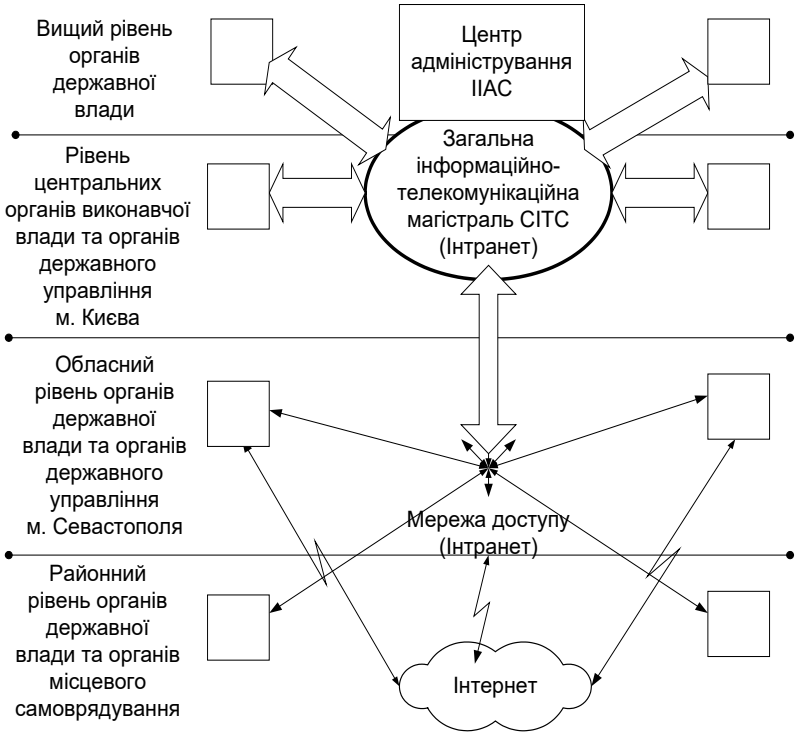

Рис. 5.43. Багаторівнева структура ТС ІІАС

Згідно з державним значенням інформаційного обміну між органами влади та враховуючи питання інформаційної безпеки, як було зазначено, взаємний зв'язок структурних елементів ІІАС у центрі доцільно здійснювати за допомогою виділеної загальної спеціальної інформаційно-телекомунікаційної магістралі.

Обласні та районні структурні елементи мають під'єднуватися до цієї магістралі за допомогою захищених каналів мережі доступу. Для доступу, особливо в районах, також може використовуватись мережа Інтернет. Крім того, Інтернет є відкритим засобом організації взаємодії органів влади та місцевого самоврядування на всіх рівнях з населенням, підприємствами та міжнародними організаціями.

Така загальна мережа, що об'єднує органи влади, повинна охоплювати територію усієї країни. Для побудови такої розподіленої мережі в реальні терміни необхідно використати існуючі у країні публічні мережі. Для забезпечення доступу до різнорідних баз даних та обміну різними видами інформації ця мережа повинна бути мультисервісною.

Переліченим вимогам відповідає мережа, що будується з використанням IP-технологій, завдяки її відкритості, здатності інтегрувати будь-які інші мережні технології, а також налагодженості, надійності та масштабуванню [226].

У свою чергу, корпоративна частина ТС АІАС, у загальному випадку, також може поділятися на чотири рівні (рис. 5.44). Вищим тут є рівень центрального апарату ОДВ разом з ІАЦ, який відіграє роль центрального вузла мережі системи, а також вузла доступу до загальної інформаційно-телекомунікаційної магістралі органів влади.

Другим є рівень підпорядкованих органу влади підприємств та об'єктів, що знаходяться в м. Києві, інших будинків, якщо центральний апарат розташований у кількох будинках у різних районах міста, а також пересувних засобів зв'язку та інформування.

Майже кожен орган влади має в регіонах власні органи управління, а також підпорядковані підприємства та об'єкти, пересувні засоби, що утворюють відповідно третій та четвертий рівні структури.

Таким чином, згідно з викладеними даними, для забезпечення ефективної інформаційної взаємодії зазначених компонент АІАС та ІІАС постає завдання інтегрування різних систем (підсистем) на базі єдиної технології пошуку, передачі та подання інформації для користувача. Одним із вирішень цієї проблеми, яке може суттєво скоротити терміни створення окремих ІАС та ІІАС у цілому, заощадити кошти та забезпечити інтеграцію цих систем у світовий інформаційний простір, є

використання апробованих технологічних рішень і складових систем на базі стандартів Інтернет/Інтранет [226].

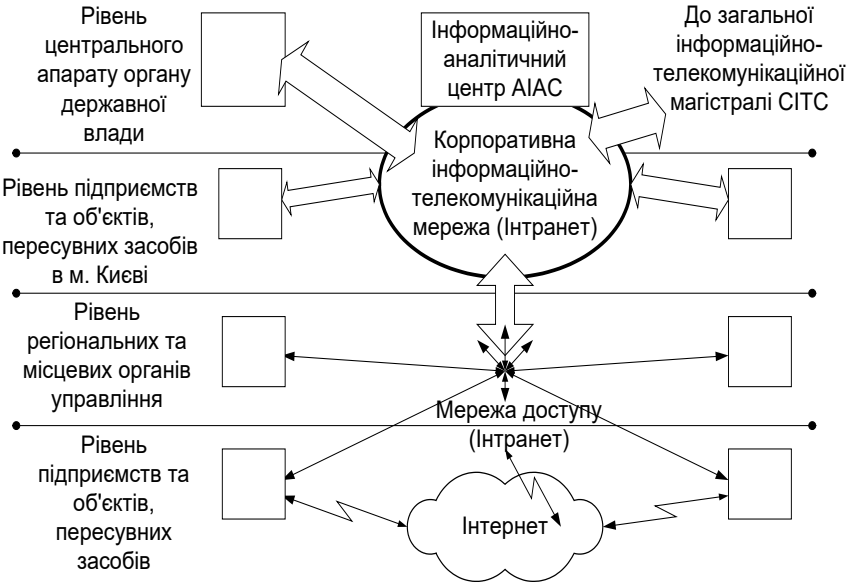

Рис. 5.44. Рівнева структура ТС АІАС

Структура засобів Інтернет/Інтранет для використання в АІАС. Найбільш поширені на теперішній час Інтернет/Інтранет-технології базуються на стандартах Інтернет (RFC — Requests For Comments), які розробляються інженерною проблемною групою Інтернет (IETF — Internet Engineering Task Force).

Ураховуючи численність і розгалуженість системи стандартів, на якій базується Інтернет, у [226] його визначають як сукупність різних телематичних служб і служб даних, що базується на взаємооб'єднаних мережах зв'язку та побудованих на основі стандартів протоколів TCP/IP [227, 228].

Усі функції міжмережного протоколу IP реалізує спеціальне обладнання (маршрутизатори). Така орієнтація Інтернет-технологій на об'єднання різнорідних мереж сприяє їх використанню в системах, апаратно-програмні платформи яких можуть значною мірою відрізнятися, що власне й притаманне АІАС ОДВ.

Рішення на основі Інтернет/Інтранет-технологій для інтеграції ІАС органів влади значною мірою відповідають положенням моделі розподіленої інформаційної системи широкого застосування.

Ця модель базується на концепціях і принципах, що враховують стандарти та протоколи Інтернету, а саме: єдиному інтерфейсі для користувачів і задач управління адміністрування ІС; взаємодії компонентів ІС на рівні протоколів; максимальному використанні стандартних програмних компонентів; використанні Інтернет/Інтранет-технологій в основних сервісах.

Використання в АІАС технології віртуальних приватних мереж. Розглянуті вище підходи до використання засобів Інтернет/Інтранет в АІАС орієнтовані на використання ідеології глобальних корпоративних мереж. Розвиток Інтернет/Інтранет-технологій, з одного боку, а також номенклатури та якості послуг, що надаються провайдерами Інтернету — з іншого, дозволяють розглядати варіанти інтеграції АІАС, а також побудову окремих корпоративних мереж органів влади на основі використання розвинутих ресурсів суспільних мереж (перед усім мережі Інтернет) шляхом побудови VPN — віртуальних приватних мереж (ВПМ). ВПМ є логічним кроком в еволюції корпоративних мереж і дозволяють комп'ютерам безпечно обмінюватись даними, навіть якщо вони проходять через мережу загального користування.

Рішення на основі ВПМ набули значного поширення у світі [229], а за останні роки й в Україні послуги ВПМ почали надаватися провайдерами Інтернету та телекомунікаційних сервісів [230], якими вже побудовані десятки мультисервісних корпоративних ВПМ.

ВПМ надають ряд переваг при забезпеченні взаємодії віддалених локальних мереж, зокрема, гарантують більш високий рівень безпеки, ніж традиційні корпоративні мережі, розгорнуті поверх телефонних каналів, а також зменшують вартість послуг зв'язку при передачі даних, голосу, відео, факсів.

У ВПМ використовується технологія тунелінгу та протоколи L2TP, IPSec. Існують різні варіанти побудови ВПМ [231]: на базі брандмауерів (програмний пакет FireWall-1), маршрутизаторів (пристрої фірми CISCO), спеціального програмного забезпечення (наприклад, AltaVista Tunnel 97), мережних ОС (Windows NT) або спеціальних апаратних засобів (cIPro-VPN).

Послуги ВПМ можуть надаватися на основі публічних мереж ATM або Frame Relay, які мають вбудовану підтримку якості транспорт-

ного обслуговування. Впровадження в IP-мережах технологій управління якістю обслуговування (RSVP, Diff Serv, MPLS) дозволяє надавати послуги ВПМ і в середовищі Інтернету. При побудові ВПМ використовуються варіанти на основі обладнання користувача (користувач бере на себе забезпечення безпеки, а від провайдера отримує гарантовану пропускну спроможність), на основі обладнання провайдера (ВПМ повністю організовано засобами провайдера) та змішаний варіант (частина засобів ВПМ розміщується в мережі провайдера, а частина — у мережі користувача).

Таким чином, аналіз Інтернет/Інтранет-стандартів і структури засобів Інтернет/Інтранет, а також їх застосування у відповідних проектах і можливих технічних рішеннях показує ефективність використання цих технологій, зокрема, мультисервісних віртуальних приватних IP-мереж, для інтеграції розподілених складових АІАС в єдину систему.

Програмне забезпечення електронної пошти, засобів доступу до Інтернету. Електронна пошта зараз є невід'ємним засобом ділового й особистого спілкування. З розвитком засобів комунікації коло розв'язуваних задач розширилося від обміну електронними листами через Інтернет чи корпоративну поштову систему до застосовувань для керування всіма повідомленнями, що знаходяться в поштовій скриньці [232] (рис. 5.45).

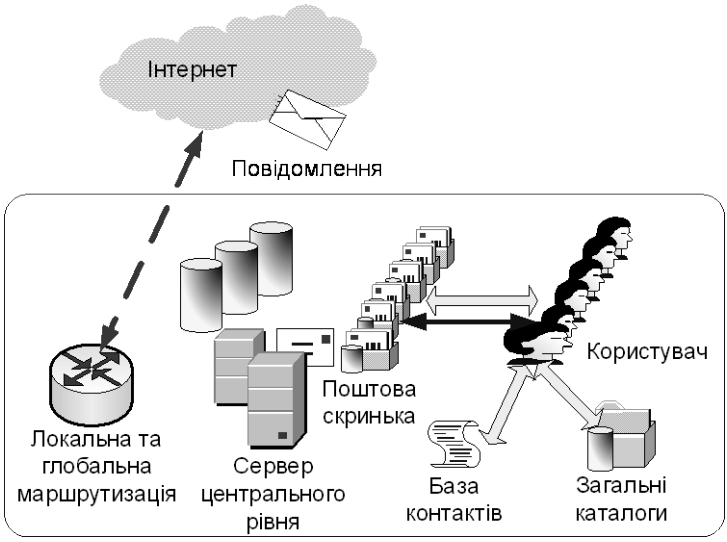

Рис. 5.45. Функціональна схема підсистеми обміну повідомленнями

Щоб вибрати оптимальну поштову програму, варто з'ясувати усі обставини майбутньої роботи, адже, враховуючи занадто різноманітні умови, в яких застосовується електронна пошта, ідеальної поштової програми не існує.

Поштовий клієнт повинен підтримувати основні функції і простий користувальний інтерфейс, не бути перевантаженим зайвими кнопками і панелями. Якщо обсяг пошти значний, то варто встановити поштову програму з розвиненими засобами фільтрації за такими критеріями, як текст повідомлення, автор, адреса відправника, розмір файла й ін. Для ефективної роботи також можуть знадобитися вбудовані чи інтегровані засоби керування контактами і календарним плануванням.

Для підтримки певних процесів в АІАС багато користувачів можуть мати більше однієї поштової адреси. Більшість поштових програм дозволяють не тільки одночасно використовувати кілька облікових записів, але й вибирати, з якої адреси варто відправляти те чи інше повідомлення.

Щоб повідомлення електронної пошти не переглядали сторонні особи, варто скористатися поштовим клієнтом, що містить функції шифрування та електронного підпису.

З урахуванням наведених вище особливостей для правильного орієнтування при виборі потрібного поштового клієнта найбільш розповсюджені поштові пакети доцільно оцінювати за трьома категоріями — «Функціональність», «Супровід» і «Ресурси».

У категорії «Функціональність» слід оцінювати можливості фільтрації повідомлень, підтримку декількох облікових записів, шифрування і цифрового підпису, кирилиці, поштових стандартів і HTML. Додатково оцінюються спеціальні функції, наприклад, органайзер, засоби підтримки графіки, режим декількох користувачів, перевірка орфографії, робота з групами новин і ін. У категорії «Супровід» необхідно оцінювати довідкову систему і керівництво користувача, їхню мову, а також підтримку компанією-ділером і онлайнову підтримку через Інтернет.

У категорії «Ресурси» оцінюється співвідношення ціни і функціональності. При цьому враховується не тільки вартість поштових програм, але й вимоги, запропоновані до апаратного забезпечення, а також «поведінка» поштових програм при їхній установці й деінсталяції.

Необхідним інструментом для роботи з Інтернетом є програми пошуку і перегляду веб-вмісту, відомі як веб-браузери. При оцінці рівня веб-браузерів потрібно враховувати швидкість завантаження і зручність перегляду різної інформації, можливість настроювання подання

інформації, а також спільної роботи з іншими додатками. Також треба враховувати, чи передбачають вони повну підтримку останніх стандартів HTML, опублікованих консорціумом W3C.

Для забезпечення інформаційно-аналітичної діяльності потрібна підтримка мультимедійних засобів, зокрема, підтримка відеозаписів з повним поданням руху — як мінімум, форматів AVI, QuickTime і MPEG. Тому серед вимог має бути забезпечення використання в одній програмній оболонці широкого спектра аудіо- і відеоформатів, таких як WAV, AU, AIFF, MIDI і MPEG, а також можливості поетапного завантаження графіки. Не виключена можливість підтримки додатків тривимірної графіки при безпосередній підтримці застосування мови Virtual Reality Markup Language (VRML).

Нарешті, слід зазначити, що при відкритості Інтернету на передній план виступають питання захисту і безпеки. При атаках хакерів і вірусів веб-браузери повинні підтримувати найсучасніші засоби захисту. Також, підтримка цифрового підпису програмного коду дозволяє визначити, ще до його завантаження, хто є видавцем програмного забезпечення. Для користувачів також важливо бути впевненими у тому, що програмне забезпечення не змінювалося в процесі завантаження.

Крім перерахованих вище важливих характеристик сучасних веббраузерів, важливе значення мають додаткові утиліти для них. Серед них можна виділити Cache for Internet Explorer для перегляду кешпам'яті Internet Explorer. Вона дозволяє групувати вміст кешу, виділяти підкаталоги веб-сайтів, експортувати в зовнішні файли й розміщати в архіві.

5.6. Вибір апаратного та програмного забезпечення АІАС

Основні засади застосування апаратного та програмного забезпечення в АІАС. Застосування апаратного та програмного забезпечення в АІАС має базуватися на наступних загальних вимогах:

а) забезпечення ієрархічної організації АІАС (центральний, регіональний і місцевий рівні);

б) використання сучасних принципів побудови на базі модульної системи і типових проектних рішень з метою досягнення необхідної гнучкості розвитку конфігурації АІАС, нарощування функціональних можливостей і пропускної спроможності;

в) підтримка клієнт-серверних технологій;

г) забезпечення можливості взаємодії АІАС з існуючими і тими, що розробляються, автоматизованими системами іншого функціонального призначення, які є зовнішніми відносно АІАС;

д) використання апаратних засобів, які мають відповідні сертифікати та дозволені до використання на території України;

е) забезпечення ефективного захисту інформації та максимальна інтеграція мережних сервісів з метою накопичення всебічної інформації щодо дій користувачів;

ж) наявності ефективних централізованих засобів управління та адміністрування, що дозволяють виконувати наскрізний нагляд і контроль за функціонуванням системи в цілому й управління на всіх рівнях її ієрархії, а також забезпечують необхідну гнучкість і динамічну зміну конфігурації.

Апаратне забезпечення. Апаратне забезпечення АІАС має містити наступні основні компоненти:

1) виділені та комутовані канали зв'язку;

2) автоматизовані робочі місця та сервери — програмно-апаратні комплекси, які входять до складу локальних обчислювальних мереж вузлів АІАС і забезпечують управління інформаційними потоками;

3) телекомунікаційне обладнання — маршрутизатори, сервери віддаленого доступу, модеми та інше обладнання, яке забезпечує підключення локальних мереж вузлів ІАС до каналів зв'язку глобальних мереж.

Основні апаратні компоненти АІАС мають відповідати державним та міжнародним стандартам у галузі інформаційних технологій, використовувати протоколи TCP/IP єдиної версії, забезпечувати урахування тимчасових погіршень характеристик каналів зв'язку.

Маршрутизатори мають забезпечувати модульну архітектуру побудови; не менше двох модулів для підключення цифрових каналів зв'язку; не менше одного модуля для підключення до локальної обчислювальної мережі; підтримку засобів фільтрації IP-пакетів; підтримку протоколів для захисту інформації; спеціалізоване програмне забезпечення, яке забезпечує ефективне управлінням маршрутизатором і підтримку протоколів IP, SNA; зовнішнє джерело безперебійного живлення.

Сервери віддаленого доступу повинні забезпечувати модульну архітектуру побудови; мати спеціалізоване програмне забезпечення для ефективного управління сервером віддаленого доступу.

Комп'ютери для АРМів управління та адміністрування мережі мають забезпечити вимоги масштабованості; мати пристрій безперебійного живлення.

Програмне забезпечення. Програмне забезпечення комплексів АІАС має забезпечувати виконання основних задач щодо підтримки процесів у рамках усіх задач, а також таких, як управління обліковими записами; управління конфігурацією; управління обробкою помилок; управління продуктивністю; управління безпекою.

Програмне забезпечення, що застосовується в АІАС, за своїм призначенням поділяється на:

а) операційні системи загального призначення;

б) операційні системи локальних мереж;

в) програмні засоби для доступу до глобальних мереж;

г) прикладні програмні засоби загального призначення;

д) прикладні програмні засоби аналітичних досліджень;

е) офісні системи;

є) системи автоматизації документообігу;

ж) програмні системи для розв'язання допоміжних функціональних задач (бухгалтерські системи й ін.);

з) засоби управління та адміністрування мережі.

Ці засоби мають забезпечувати:

а) багатокористувацький та багатозадачний режими роботи;

б) функціонування корпоративної мережі ІАС за моделлю з декількома головними доменами;

в) підтримку стандартних протоколів TCP/IP для управління передачею інформації, як по локальній мережі, так і по каналах зв'язку;

г) режим функціонування розподіленої бази даних у режимі «клієнт–сервер»;

д) ведення каталогів користувачів з ідентифікацією та автентифікацією;

е) мережні функції;

є) автентифікацію, шифрування інформації.

Так само це відноситься й до СКБД, які мають забезпечувати повний набір вимог до збереження та цілісності інформації, механізму її обробки, а також адміністрування доступу.

На офісному робочому місці повинна функціонувати ОС Windows або Linux, бути установленим та налагодженим офісне програмне забезпечення — текстові редактори, графічні редактори, редактор електронних таблиць, поштове клієнтське програмне забезпечення, програм-

не забезпечення органайзера, забезпечений доступ до периферійного обладнання: принтерів, сканерів, організований доступ до корпоративної мережі АІАС та Інтернету.

Спеціалізовані робочі місця мають бути налаштовані для виконання функцій, що визначаються спеціалізацією користувача. Окрім офісного пакету програмних продуктів та поштового клієнта повинно бути встановлене та налагоджене відповідне специфічне програмне забезпечення, налагоджений доступ до периферійного обладнання, при необхідності організований доступ до корпоративної мережі та Інтернету.

Прикладне програмне забезпечення повинно розроблятися мовами високого рівня з використанням сучасних інструментальних засобів, що забезпечує високий ступінь супроводження програмного продукту і максимальну його незалежність від програмно-апаратної платформи. Прикладне програмне забезпечення повинно будуватися за модульним принципом, бути високотехнологічним і максимально уніфікованим.

Програмні засоби мають забезпечувати також вимоги багатоплатформеності — функціонувати на платформах операційних систем ОС Linux, Microsoft Windows [233].

Програмне забезпечення веб-порталу. При створенні у складі АІАС нового порталу має сенс починати з деякого базового сайту, що реалізує максимум необхідної функціональності й дозволяє надалі проводити його модернізацію. Наприклад, при використанні засобів Microsoft варіант такого сайту використовує Content Connector Solution Site, що поставляється разом з Content Management Server (рис. 5.46).

Багатотермінальні комплекси. Альтернативою організації АРМ фахівців на персональних комп'ютерах є багатотермінальні комплекси (з так званими «тонкими клієнтами»). Умовою їхнього використання є застосування операційних систем Unix або Linux. Застосування багатотермінальних комплексів надає суттєву економію при придбанні технічних засобів [234]. Але це лише одна з переваг такого рішення. Завдяки простоті побудови термінал є дешевим засобом, термін дії якого до того ж практично необмежений, а його встановлення або заміна зводиться лише до підключення до розеток. Слід додати, що при цьому також вирішуються й проблемні питання безпеки. По-перше, це запобігання несанкціонованих крадіжок прикладного програмного забезпечення та інформації, адже усі процеси відбуваються на сервері. По-друге, це антивірусний захист. По-третє, виключається можливість

здійснення на робочому місті непередбачених виробничим процесом дій (комп'ютерні ігри, приватні опрацювання інформації тощо).

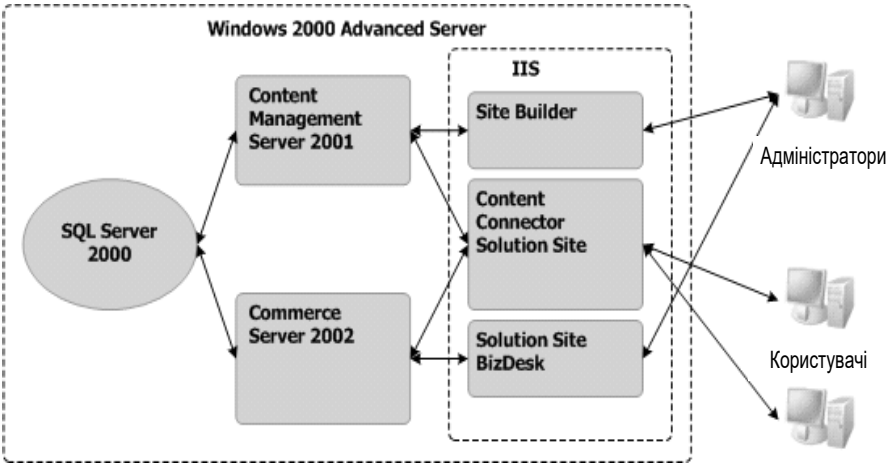

Рис. 5.46. Базовий варіант порталу на засобах Microsoft

Технічні засоби багатотермінального комплексу містять у своєму складі комп'ютер серверного типу для розміщення на ньому сервера баз даних і файл-сервера, робочі станції фахівців для розміщення на них функціональних додатків, спеціалізовані робочі місця, робочі місця розробника програмного забезпечення, Х-термінали та допускають підключення комп'ютерів зі складу технічних засобів, на яких розташовані прикладні додатки в середовищі Windows.

Організаційно багатотермінальні комплекси підключаються як окрема ЛОМ у корпоративну мережу. Взаємодія в мережі здійснюється на базі протоколу Ethernet (IEEE802.3). Можливі два варіанти структурної схеми багатотермінальних комплексів: перший, коли робочі станції і Х-термінали підключені до сервера, на якому встановлено сервер баз даних, файл-сервер, веб-сервер, і другий, коли Х-термінали підключені до окремого термінального сервера (рис. 5.47).

Х-термінали в середовищі ОС Linux — це функціонально повні робочі місця з мінімальними вимогами до технічних засобів і зі зручним способом взаємодії з термінальним сервером. На Х-терміналі повинна бути встановлена операційна система Linux, ядро якої зкомпільовано з підтримкою можливості завантаження по мережі та з підтримкою апаратного забезпечення (клавіатури, миші, мережної карти, мо-

жливо звукової карти). Обов'язково повинні мати місце пакети підтримки протоколу tftp — протокол обміну графічними екранами; функції dhcp — можливість визначати IP-адресу; мережної файлової системи NFS.

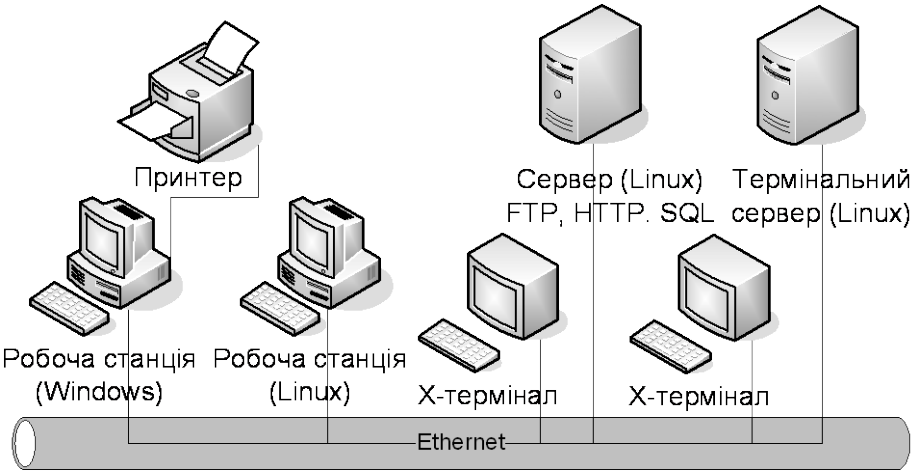

Рис. 5.47. Структурна схема багатотермінального комплексу з підключенням X-терміналів до окремого термінального сервера

Для забезпечення роботи X-терміналів необхідна наявність одного або більше термінальних серверів, залежно від інтенсивності їх роботи. Велика кількість одночасно працюючих X-терміналів значно збільшує трафік і знижує продуктивність системи, тому їх оптимальна кількість на один сервер — 6–9 терміналів. Крім того, при великому навантаженні небажано поєднувати функції термінального сервера та сервера інших служб: файл-сервера, SQL-сервера тощо.

У випадках, коли кількість працівників до 100 осіб і більше 100 осіб рішення ускладнюються. Так, в останньому випадку необхідно будувати так звану «ферму», коли шлюзові засоби (Gate) обслуговують по 30–40 клієнтів (рис. 5.48).

Засоби локальної мережі. Серед мережних технологій для АІАС значне місце займає застосування локальних інформаційних мереж (ЛІМ).

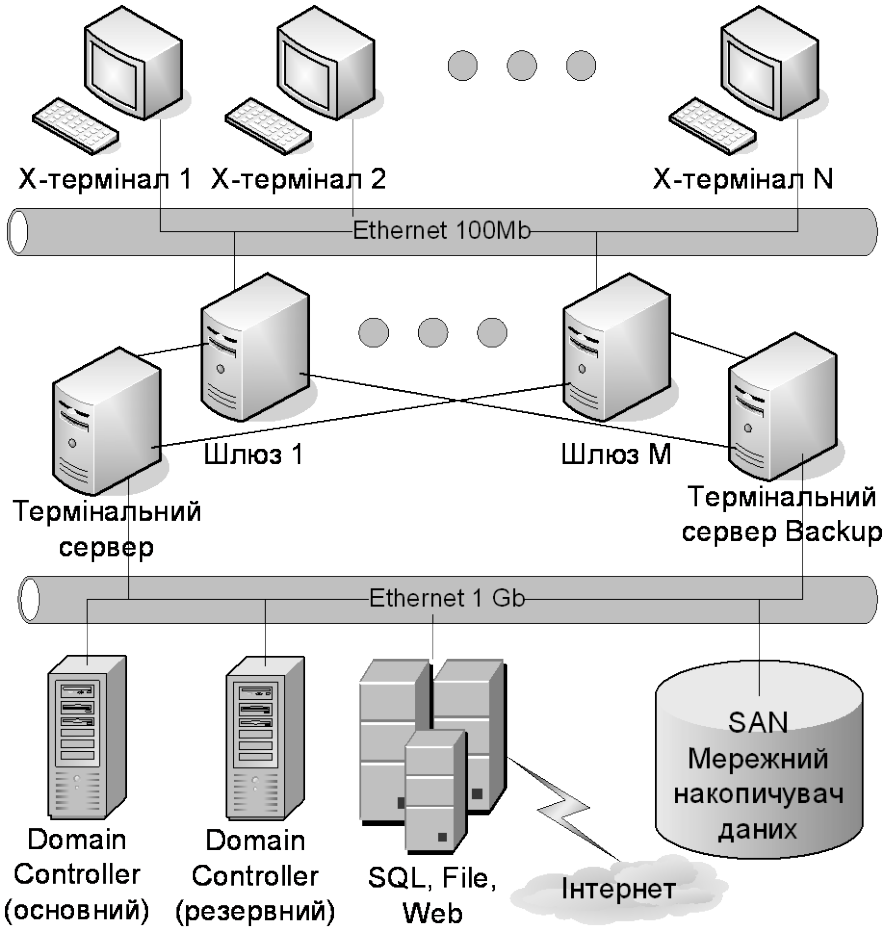

Рис. 5.48. Структурна схема багатотермінального комплексу у випадку кількості працівників більше 100 осіб

ЛІМ в органах влади дозволяють працівникам апарату взаємодіяти один із одним для виконання таких задач, як спільна робота з документами, збереження й архівування своєї роботи на загальному сервері, доступ до додатків на сервері, полегшення спільного використання дорогих ресурсів.

Вбудовуючи в базові локальні мережі функціональність територіально-розподілений мереж, реалізовану за допомогою модема чи сервера віддаленого доступу, можна вигідно використовувати технології зо-

внішніх комунікацій, у тому числі такі, як передачу і прийом повідомлень за допомогою електронної пошти (e-mail), доступ до Інтернету.

Як правило, ЛІМ АІАС функціонує на базі протоколу Ethernet (IEEE 802.3) з топологією типу «зірка». При цьому часто-густо центральний апарат органу влади розташовується на кількох поверхах (рис. 5.49). Наведена узагальнена функціонально-логічна структура мережі реалізована в ІАС Держкомзв'язку, до неї належать підсистеми обробки інформації, взаємодії користувачів та обміну даними.

Для передачі інформації застосовується неекранований кабель типу «звита пара» (UTP) категорії 5, який забезпечує швидкість передачі до 100 Мбіт/с. Сервери і робочі станції об'єднуються у ЛІМ мережними кабелями за допомогою мережного маршрутизатора, мережного концентратора, мережних кабелів і рознімів типу RJ-45.

Мережний маршрутизатор має бути мультипротокольним маршрутизатором мережі типу Ethernet, кількість портів — від 8 та більше, які забезпечують швидкість передачі інформації не менше 100 Мбіт/с.

Організація вибору програмного забезпечення для побудови АІАС. Проблеми ліцензування ПЗ, що застосовуються в ОДВ. Методологія вибору ПЗ є регламентованою й широко відомою. Але необхідно враховувати, що Україна входить у п'ятірку найбільш піратських країн світу щодо використання контрафактних програмних продуктів (за оцінками до 80 відсотків програмних продуктів, що використовуються в Україні, є неліцензійними).

Значною мірою йдеться про нелегальне використання продуктів компанії Microsoft, і не менш суттєво це стосується й органів державної влади. Головною причиною становища з нелегального використання є цінова політика Microsoft, яка, враховуючи домінуючий стан на ринку ПЗ, дає корпорації змогу утримувати значні ціни на свої продукти, внаслідок чого на закупівлю програмних засобів витрачаються чималі кошти (рис. 5.50).

Окрім нелегального розповсюдження, з програмними продуктами корпорації Microsoft пов'язані й інші труднощі. Перш за все, це стосується уразливості цих продуктів шкідливими програмами (вірусами та ін.). Крім того, існує й проблема закритості кодів цих ПЗ. Існують висновки про виявлення в програмах Microsoft так званих «закладок» або «ключів», що забезпечують прихований відтік інформації з комп'ютера, що з точки зору інформаційної безпеки не дає впевненості в «чистоті» кодів цих програм.

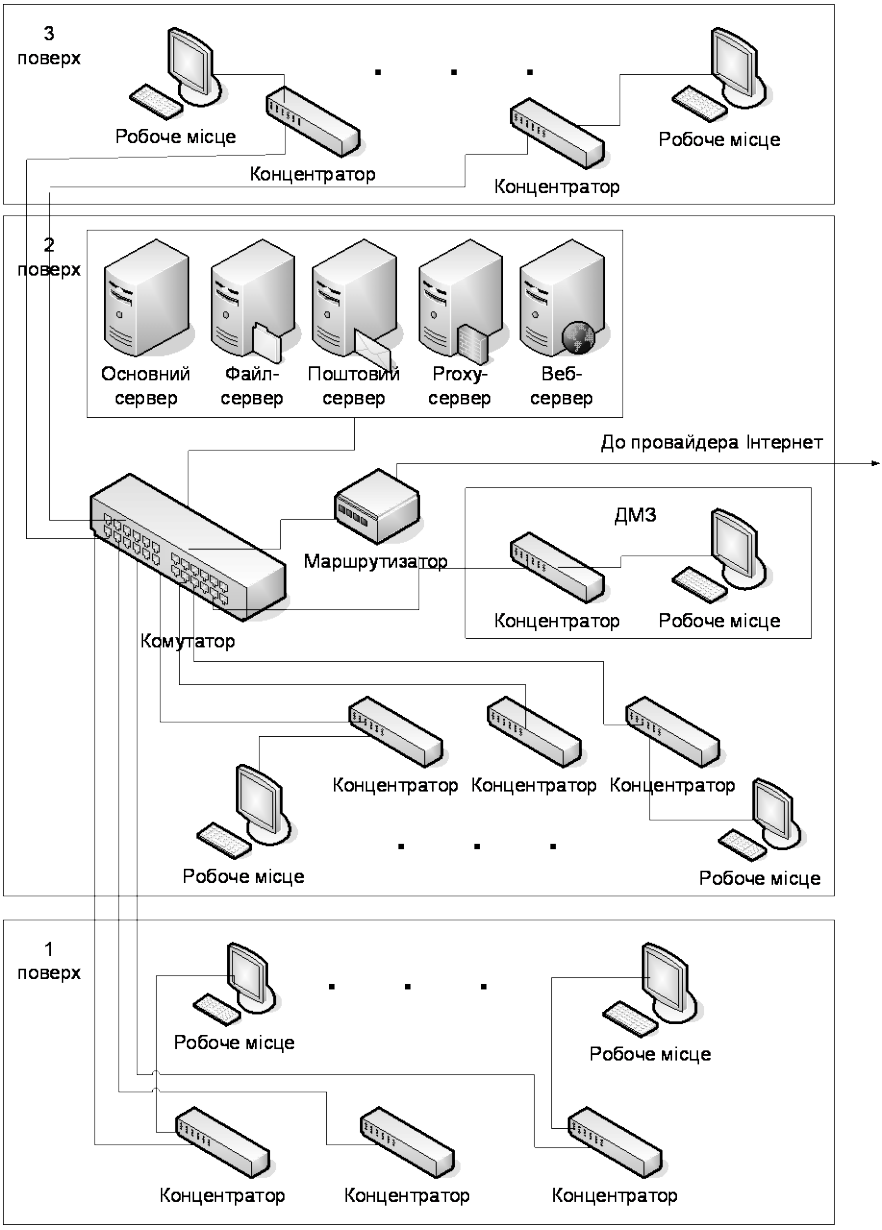

Рис. 5.49. Типова схема ЛОМ АІАС із розташуванням робочих місць на трьох поверхах

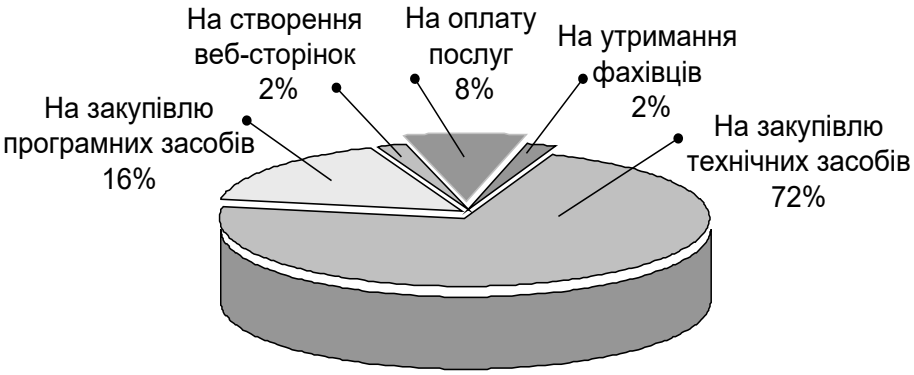

Рис. 5.50. Усереднене співвідношення даних щодо потрібних коштів на закупівлю засобів та оплату послуг при створенні АІАС

Отже, організація вибору програмного забезпечення для успішної реалізації проекту АІАС є досить важливою. Альтернативою програмному забезпеченню Microsoft є ПЗ із відкритими кодами, яке розповсюджується вільно (або умовно вільно). До такого ПЗ відносяться Unix-подібні програмні засоби, у тому числі система Linux. Зазначені фактори змусили урядові структури країн світу (зокрема, і країн-членів ЄС) звернути увагу на доцільність переходу на операційні системи з відкритими кодами. Про це свідчить факт розробки Європейською економічною комісією ООН і представниками держав, що входять у Європейський союз, «Посібника з переходу на програмне забезпечення з відкритим кодом».

Дослідну експлуатацію стендового макету багатотермінального комплексу на базі ОС Linux в органі влади у складі сервера графічного середовища та терміналів, у якості яких були задіяні застарілі ПЕОМ, було проведено й в Україні. При цьому перевірено та підтверджено працездатність і функціональну повноту цих засобів [233, 234].

Звісно, у середовища Linux є й чимало недоліків, але такі переваги операційних систем з родини Linux, як стабільність і надійність, порівняно низькі вимоги до апаратних ресурсів, відкриті вихідні тексти, великий набір «рідних» сервісів Інтернету і ЛІМ, наявність офісних додатків, достатніх для створення повноцінного робочого місця для обробки документів, графіки та відео будь-якого рівня складності, безпека, широко відомі. Крім того, завдяки Інтернету розвиток дистрибутивів Linux активно підтримується спільнотою розробників з усього світу — (http://

www.gnu.org/copyleft/gpl.html, http://www.gnu.org/gnu/linux-and-gnu.html, http://www.gnu.org/philosophy/categories.html, http://www.csis.org/tech/OpenSource, http://www.osdn.org.ua, http://www.linux.org.ua та ін.).

Повністю відмовитись від «закритих» комерційних програм на сьогодні неможливо, але вибір є очевидним: переходити на вільне (відкрите) ПЗ у всіх випадках ефективніше, коли воно не поступається за функціональністю «закритому» комерційному ПЗ, або коли виграє в «закритого» комерційного ПЗ за співвідношенням «ціна – функціональність». Нарешті, згідно з вимогами інформаційної безпеки влади, актуальним є питання створення вітчизняного програмного забезпечення на основі довгострокової державної програми. Про це свідчить досвід європейських країн і Росії.

Вимоги до програмного забезпечення щодо забезпечення його якості. Параметрами, що характеризують програму, можуть бути різні показники. Питання полягає в тому, щоб вибрати найбільш інформативні показники, відповідні підходи для їхнього зіставлення, знаходження компромісів і одержання інтегральних оцінок [235].

Складність оцінки якості ПЗ виникає через те, що необхідно зіставлення споживчих показників якості ПЗ і технічних. В остаточному підсумку, якість програм має вартісне втілення, що містить оцінку витрат на розробку й експлуатацію, економічні переваги використання програми порівняно з іншими засобами розв'язання даної прикладної задачі, перспективи подальшого використання ПЗ. У свою чергу, до базових технічних характеристик програми належить повнота (у програмі є все необхідне); відсутність переповнення (у програмі немає нічого зайвого); відповідність (програма та її частини відповідають правилам і законам зовнішнього середовища). Для оцінки програм, крім показників вартості, використовують ще й такі показники, як працездатність, час розробки й установки, термін служби.

Основою для формування функціональних показників ПЗ є аналіз властивостей, які характеризують якість його функціонування з урахуванням технологічних можливостей розроблювача, що оцінюється при сертифікації. Основним тут є затверджений у 1991 р. міжнародний стандарт ISO 9126:1991 «Інформаційна технологія. Оцінка програмного продукту. Характеристики якості і посібник з їхнього застосування», а також системи стандартів ISO/IEC у галузі програмної інженерії.

5.7. Організація захисту інформації та забезпечення живучості АІАС

Проблеми безпеки в інформаційних системах органів влади. Як вже зазначалося, одним з найважливіших підходів до забезпечення взаємодії уряду з бізнесом і громадянами в умовах функціонування АІАС має бути методологія захисту інформації. Це стосується не лише інформації, що є власністю держави і в умовах відкритості наражається на небезпеку, а й персональних даних клієнтів системи «електронний уряд». Держава повинна гарантувати повний захист подібних даних від несанкціонованого доступу на технологічному, процедурному та нормативному рівні.

Під інформаційною безпекою (ІБ) АІАС розуміється захищеність інформації, що має циркулювати в ній, та підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, здатних нанести збитки власникам або користувачам інформації та підтримуючій інфраструктурі.

До основних задач забезпечення інформаційної безпеки АІАС слід віднести:

1) виявлення, оцінка та прогнозування джерел загроз ІБ;

2) розроблення політики забезпечення ІБ і комплексу заходів і механізмів її реалізації (програма ІБ);

3) створення нормативних та організаційних засад забезпечення ІБ;

4) координація діяльності органів влади, що експлуатують власні АІАС, із реалізації політики ІБ;

5) постійний розвиток системи забезпечення ІБ, вдосконалення її організації, форм, методів і засобів запобігання загрозам ІБ та ліквідації наслідків її порушення.

Одна з суттєвих проблем — це побудова інформаційної інфраструктури державної влади України на базі імпортної техніки й технологій. Тому до наведеного переліку необхідно віднести й задачу максимально можливого застосування вітчизняних програмно-апаратних засобів.

При створенні АІАС необхідне проведення, перш за все, обстеження середовищ функціонування системи (обчислювальної та телекомунікаційної системи, середовища користувачів, фізичного середовища, власне оброблюваної інформації та технології її обробки), а також досліджень з моделювання оточуючого середовища з метою визначення джерел загроз та їх інтенсивності, розробки моделі загроз і моделі

потенційного порушника [236, 237]. На цій базі проводиться розробка правил взаємодії суб'єктів доступу до об'єктів захисту на рівні ролевої моделі, а також визначення функціонального профілю захищеності, який має реалізувати комплекс засобів захисту (КЗЗ) від несанкціонованого доступу.

Також при створенні АІАС має передбачатися певна архітектура безпеки. Враховуючи, що вся система розглядається зосередженою у мережному середовищі між двома закінченнями — переднім флангом (Frontend), що становлять клієнти системи (підприємства та громадяни), і заднім флангом (Backend), що містить автоматизовані місця держслужбовців, виникає проблема запобігання шкідливому зовнішньому втручанню та забезпечення конфіденційності (або таємності) закритих даних.

Методологія запропонованої безпечної архітектури передбачає перш за все поділення усієї сфери взаємодії в системі на окремі зони, захист яких одна від одної забезпечується відомими платформними рішеннями (Firewall, Proxy-сервер). Ще одне рішення — організація корпоративної мережі органу влади на базі технології ВПМ. Суттєвим рішенням є виділення так званої демілітаризованої зони та формування у центральному апараті двох (а то і трьох) окремих локальних мереж.

Нарешті, вважається також ефективним впровадження методології використання інтелектуальних карток. Реалізація на їх основі засобів автентифікації поряд зі здійсненням комплексу інженерно-технічних заходів для запобігання несанкціонованого доступу до самої картки дозволить створити для користувачів АІАС надійно захищений інструмент забезпечення доступу до об'єктів і ресурсів системи.

Розробка і впровадження нормативних, організаційно-технічних та апаратно-програмних заходів і засобів щодо забезпечення ІБ АІАС мають відповідати наступним принципам [238–243]:

1) базування захисту інформації в АІАС на положеннях і вимогах законів, стандартів, нормативно-методичних документів щодо захисту інформації, що діють або рекомендовані до застосування в Україні;

2) забезпечення гарантії інформаційної безпеки для всіх суб'єктів АІАС на основі єдиної нормативної бази та затверджених стандартів;

3) розгляд захисту інформації як регулярного, безперервного процесу, що здійснюється на всіх етапах життєвого циклу АІАС та інформації, яка циркулює в ній;

4) багаторівневість та всеосяжність захисту (в АІАС повинна реалізуватися концепція комплексної безпеки, коли захисту підлягають усі

структурні підрозділи суб'єктів АІАС, до яких належать рівні територій, будівель, споруд, рівні технологічних процесів збереження, обробки та передачі інформації);

5) побудова захисту інформації за комбінованою централізовано-децентралізованою схемою, що передбачає розподіл відповідальності між різними суб'єктами АІАС;

6) здійснення захисту переважно комплексом апаратно-програмних засобів, які підтримуються комплексом організаційно-технічних заходів;

7) переважне використання національних апаратно-програмних засобів та криптографічних систем;

8) постійне керування та контроль ефективності захисту;

9) неприпустимість отримання інформації, що захищається, через сегменти локальної мережі АІАС, які приєднані до мереж загального користування.

Відповідно до цих принципів на підставі розроблених нормативних документів у АІАС створюється ***комплексна система захисту інформації*** (КСЗІ), що виконує такі функції:

- забезпечення захисту конфіденційності, цілісності та доступності (попередження навмисних чи ненавмисних спроб блокування) інформації, яка обробляється в АІАС і програмного забезпечення і баз даних від несанкціонованого доступу;
- спостережність за технологічним процесом обробки інформації;
- забезпечення розмежування та контроль доступу користувачів різних категорій до ресурсів АІАС згідно з їхніми повноваженнями;
- забезпечення реєстрації даних про події, що відбуваються в АІАС і мають відношення до її безпеки;
- забезпечення цілісності та доступності критичних ресурсів комплексу засобів захисту, системного програмного забезпечення та прикладних програм АІАС;
- забезпечення замкненого середовища перевіреного програмного забезпечення з метою захисту від безконтрольного впровадження в АІАС потенційно небезпечних програм, а також від впровадження і поширення комп'ютерних вірусів;
- забезпечення управління засобами КСЗІ АІАС і контроль за її функціонуванням.

Основа забезпечення ефективності КСЗІ — це дотримання вимог державної нормативної бази, значну частину яких складають нормати-

вні документи уповноваженого органу з питань технічного захисту інформації, державні й міжнародні стандарти та рекомендації.

З метою запобігання як витоку інформації, так і навмисних та ненавмисних впливів на технологічні процеси її обробки технічними каналами в складі КСЗІ АІАС мають впроваджуватися заходи захисту інформації та програмно-апаратні засоби захисту інформації відповідно до встановлених згідно з відповідними державними нормативними документами категоріями об'єктів із урахуванням структури обчислювальної системи.

Обчислювальна система АІАС зазвичай проектується за стандартною 3-ланковою архітектурою. В ній виділяються 3 головні елементи: рівень даних (сервер БД), рівень бізнес-логіки (сервер застосувань), рівень графічного подання інформації (клієнтські робочі місця). При такій архітектурі кількість взаємних посилань між підсистемами є мінімізованою, дозволяє забезпечити легку її модернізацію у разі виникнення такої потреби. Ці складові працюють у комплексі та взаємодіють через уніфіковані інтерфейси.

До складу обчислювальної системи АІАС мають входити сервери, комутаційне обладнання, сукупність робочих станцій користувачів та адміністраторів різних рівнів. До ЛОМ системи через модуль взаємодії підключаються модулі інтерфейсу із зовнішніми користувачами (рис. 5.51). Таке технічне рішення забезпечує розмежування інформаційних потоків, що циркулюють в Інтернеті та в АІАС і унеможливлюють доступ користувачів, які є неавтентифікованими у системі, до конфіденційної інформації.

КСЗІ перш за все має бути спрямованою на захист системи інформаційних ресурсів органу влади [243]. Згідно з Законом України «Про інформацію», за режимом доступу інформація поділяється на відкриту та на інформацію з обмеженим доступом (ІзОД). До ІзОД відноситься також конфіденційна інформація. Інформацію, яка обробляється в АІАС, за режимом доступу зазвичай можна віднести до цих категорій таким чином.

До відкритої інформація відноситься публічно оголошувана інформація органу влади, користуватися якою можуть будь-які фізичні або юридичні особи. До відкритої критичної інформації, тобто інформації, яка потребує захисту цілісності і доступності, слід віднести технологічну інформацію щодо адміністрування та управління АІАС, тобто дані про мережні адреси, імена та ін.

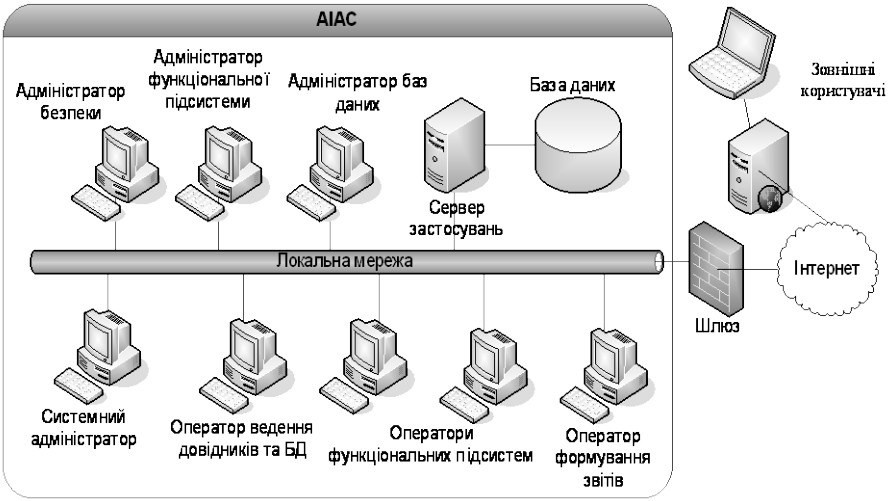

Рис. 5.51. Загальна структурна схема АІАС із засобами безпеки

До ІзОД відноситься перш за все конфіденційна інформація — інформація, захист якої визначається нормативними документами (це можуть бути персональні дані суб'єктів господарювання, інформація, яка міститься в різних заявах суб'єктів господарювання та наданих їм дозвільних документах та ін.). До цієї категорії слід віднести й технологічну інформацію КСЗІ, тобто персональні ідентифікатори та паролі користувачів, їхні повноваження та права доступу до об'єктів, інформація журналів реєстрації дій користувачів, установлені робочі параметри окремих механізмів або засобів захисту, інформація про профілі обладнання та режими його функціонування, робочі параметри функціонального ПЗ тощо.

До конфіденційної інформації повинні мати доступ тільки адміністратори системи відповідних категорій та уповноважені користувачі.

Одним із основних режимів обробки інформації АІАС є робота з електронними документами. Зважаючи на це, в АІАС має бути виділена й підсистема забезпечення захисту та юридичної значущості електронних документів.

Основними загрозами інформації в АІАС можна вважати тимчасові або остаточні втрати конфіденційності, доступності та цілісності ІзОД.

При цьому можна виділити такі зовнішні загрози, що можуть бути реалізовані навмисними діями порушників, а саме:

- несанкціоноване перехоплення інформації, що циркулює в АІАС (загроза спрямована на порушення конфіденційності інформації);
- несанкціонована модифікація інформації, що циркулює в АІАС (загроза спрямована на порушення цілісності інформації);
- блокування роботи АІАС через здійснення впливів, що призводять до відмови в обслуговуванні (загроза спрямована на порушення доступності інформації).

Несанкціоноване перехоплення інформації полягає у несанкціонованому підключенню до АІАС, перехопленні даних, що циркулюють в системі, аналізу трафіку тощо. Додатковим наслідком цієї загрози може бути отримання порушником відомостей про вразливості, наявні у системі.

Серед внутрішніх загроз передусім слід виділити помилки користувачів, адміністраторів, обслуговуючого персоналу при експлуатації, адміністраторів і розробників при конфігуруванні системи, розробників при створенні програмного забезпечення, недбале зберігання та облік документів, носіїв інформації, даних. Ці загрози спрямовані на порушення цілісності та конфіденційності інформації. Вони можуть бути реалізовані навмисними діями порушників та ненавмисними діями персоналу або розробників.

Загрози несанкціонованого копіювання носіїв інформації полягають у читанні залишкової інформації з оперативної пам'яті, зовнішніх запам'ятовувальних пристроїв, а також читанні даних, що виводяться на екран, читанні залишених без догляду документів. Ці загрози спрямовані на порушення конфіденційності інформації і можуть бути реалізовані навмисними діями порушників.

Загроза перевищення повноважень зводиться до одержання атрибутів доступу з наступним їх використанням для маскування під іншого користувача. Вона може бути спрямованою як на порушення цілісності, так і на порушення конфіденційності або доступності інформації, залежно від цілей порушника.

Загрози порушення нормальних режимів роботи полягають у:

- несанкціонованому внесенні змін у комплекс технічних засобів, у програмне забезпечення, в компоненти інформаційного забезпечення, впровадженні і використанні забороненого політикою безпеки ПЗ;
- знищенні компонентів програмного та інформаційного забезпечення;

- порушенні нормальних режимів роботи серверів, робочих станцій, активного мережного обладнання, периферійного обладнання;
- ураженні програмного забезпечення комп'ютерними вірусами;
- пошкодженні носіїв інформації.

Ці загрози спрямовані на порушення цілісності інформації, що обробляється в АІАС, а також цілісності програмних засобів. Порушення нормальних режимів роботи може бути спричинене відмовою окремих компонентів обладнання АІАС, умисними діями порушників, які безпосередньо спрямовані на АІАС або побічним результатом дії яких стали негативні наслідки для АІАС, недбалими або некомпетентними діями персоналу.

Можливим впливом порушення нормального режиму функціонування на АІАС може бути призупинення технологічного процесу обробки інформації в АІАС, втрата інформації, що обробляється, матеріальні збитки.

Суттєвий вплив можуть здійснити техногенні та стихійні загрози, до яких відносять відмови та збої основних технічних засобів, систем живлення, носіїв інформації, мережного обладнання. Ці загрози спрямовані на порушення доступності інформації, спостережуваності та керованості АІАС.

Тимчасові порушення функціонування АІАС можуть відбуватися через довготривале відключення енергопостачання, коли неможливе використання джерела резервного живлення, порушення контурів заземлення, створення умов фізичного середовища, які виключають можливість експлуатації АІАС або її компонентів (неприпустимі температура або вологість повітря, хімічне або радіаційне забруднення, пожежа, аварія тощо), інші форс-мажорні обставини. Ці загрози спрямовані на порушення цілісності і доступності інформації, спостережуваності та керованості АІАС, а також цілісності програмно-апаратних засобів АІАС.

Порушники політики безпеки в АІАС класифікуються головним чином як хакер, група хакерів і зацікавлені особи. Найбільш реальними вважаються загрози з боку груп хакерів і зацікавлених осіб. При цьому, як вже зазначалось і як свідчить практика використань ІКТ, найбільшу кількість порушень слід очікувати якраз від внутрішніх порушників.

Для вчинення негативних дій порушники зазвичай використовують такі методи та засоби:

1) агентурні методи одержання відомостей;

2) пасивні технічні засоби перехоплення інформації;

3) штатні засоби ІТС або недоліки проектування КЗЗ для реалізації спроб НСД;

4) способи і засоби активного впливу на програмно-апаратні засоби, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, несанкціоноване підключення до каналів передачі даних, впровадження і використання спеціального програмного забезпечення тощо).

Отже, згідно з викладеним на попередніх сторінках, АІАС є розподіленим багатомашинним багатокористувацьким комплексом, що обробляє інформацію різних категорій конфіденційності. Відповідно до нормативного документу ДСТСЗІ НД ТЗІ 2.5-005-99 така автоматизована система відноситься до 3 класу. Функціональний профіль захищеності такої системи є достатньо складним і потребує значних зусиль і коштів на створення КСЗІ.

Створення та актуалізація КСЗІ в АІАС має забезпечуватись реалізацією багатостадійного процесу інтеграції окремих складових АІАС до єдиної системи та створенням засобів захисту телекомунікаційного середовища. Етапами вказаного процесу інтеграції є такі:

1) аналіз фізичної й логічної архітектури комп'ютерних систем, а також схем автоматизованої обробки інформації, що використовуються в АІАС;

2) виявлення на підставі проведеного аналізу уразливих елементів, через які можлива реалізація загроз інформації;

3) визначення, аналіз і класифікація можливих загроз інформації;

4) оцінка поточного рівня безпеки і визначення ризику;

5) розробка політики безпеки;

6) формування повного переліку детальних вимог до систем захисту відповідно до класів захищеності АІАС;

7) розробка КСЗІ з урахуванням усіх пред'явлених вимог і чинників, що впливають на захист;

8) оцінювання рівня інформаційної безпеки.

Залежно від поточного етапу життєвого циклу АІАС на момент прийняття рішень стосовно створення КСЗІ окремі з наведених вище етапів можуть бути вилучені за умови надання результатів попередньо виконаних робіт, які складають зміст таких етапів.

Важливим питанням є присвоєння категорій усім користувачам, що мають доступ до АІАС, за рівнем повноважень відповідно до характеру та складу робіт, які виконуються ними в процесі функціонування системи. Користувачі зазвичай поділяються на користувачів АІАС (ад-

міністраторів і держслужбовців різних категорій), зовнішніх користувачів (громадяни, працівники підприємств, інших органів влади) та обслуговуючий персонал системи.

Перелік і обсяг функцій, що виконуються користувачем відповідно до своїх службових обов'язків, та ресурси АІАС, що використовуються для цього, складають поняття «ролі», яке забезпечує принцип розмежування прав доступу. Правила розмежування доступу (ПРД) реалізуються компонентою КЗЗ, розташованою, як правило, у сервері застосувань, під час визначення прав доступу до певних прикладних програм. При цьому на АРМі користувача з'являється відповідний інтерфейс із зазначенням списку доступних прикладних програм. Доступ до кожної з програм визначається списком керування доступу (СКД), який є їхнім невід'ємним атрибутом доступу.

У свою чергу для усіх типів інформаційних об'єктів, що підлягають захисту, а також для користувачів АІАС визначається множина атрибутів доступу — інформації, що однозначно характеризує об'єкт і використовується для розмежування доступу, згідно з якими здійснюється розмежування доступу користувачів до інформаційних об'єктів.

До ролей користувачів в АІАС зазвичай відносяться:

1) адміністратор безпеки — працівник, який відповідає за вирішення комплексу питань, пов'язаних із захистом інформації, зокрема, надання прав доступу до ресурсів АІАС адміністраторам інших категорій та іншим користувачам, за забезпечення надійного функціонування засобів захисту АІСА. Адміністратор безпеки виконує завдання щодо налаштування та управління функціонуванням програмно-апаратних засобів технічного та криптографічного захисту інформації та контролю за зберіганням та обігом носіїв ключових даних, супроводжує засоби антивірусного захисту АІАС та поновлює бази даних антивірусного захисту;

2) системний адміністратор — працівник, який забезпечує постійне функціонування серверного обладнання та робочих станцій користувачів, а також відповідає за реалізацію технічних заходів, що забезпечують доступність інформації та спостережуваність АІАС, постійне функціонування комутаційного обладнання та іншого мережного обладнання, що використовує АІАС, встановлює системне програмне забезпечення, надає методичні консультації користувачам системи;

3) адміністратор функціональної підсистеми — працівник, який відповідає за встановлення функціонального програмного забезпечення АІАС і контроль за процесом його експлуатації користувачами системи;

4) адміністратор баз даних — працівник, який забезпечує супроводження як системи керування базами даних, так і безпосередньо баз даних, які створені за допомогою цих СКБД, остаточне видалення інформації з бази даних, відповідає за реалізацію заходів, що забезпечують конфіденційність, цілісність і доступність інформаційних ресурсів та спостережуваність інформаційних ресурсів АІАС;

5) оператор функціональної підсистеми — держслужбовець, який виконує свої посадові обов'язки з використанням ресурсів АІАС;

6) оператор ведення довідників — працівник, якому надано повноваження внесення та редагування інформації в довідниках; перегляд інформації, що була внесена до довідників АІАС, із можливістю деталізації за конкретним видом; пошук інформації в довідниках;

6) оператор формування звітів — працівник, якому надано повноваження перегляду переліку заздалегідь визначених форм звітів, корегування визначених форм звітів, уведення початкової інформації для формування звітів (наприклад, дати початку та кінця звітного періоду), формування, перегляд і друк сформованого звіту.

Окремі ролі мають бути встановлені для представників сторонніх по відношенню до органу влади організацій — постачальників, розробників і проектувальників, які здійснюють розробку, впровадження та супроводження функціонального ПЗ АІАС, забезпечують інсталяцію, монтаж, поточне гарантійне, післягарантійне обслуговування засобів. Вони виконують роботи під контролем адміністраторів АІАС відповідних категорій.

Програмно-апаратні засоби та комутаційне обладнання АІАС мають знаходитись у приміщеннях, які належним чином охороняються та захищені від впливів техногенних і природних факторів. За приміщеннями має здійснюватися цілодобове відеоспостереження під цілодобовим наглядом служби охорони, вони мають бути обладнанні системою протипожежної та охоронної сигналізації.

Приміщення органу влади та розміщення засобів АІАС поділяються на зони. Такий розподіл здійснюється шляхом дозволу проходу в приміщення працівників ОДВ по електронним пластиковим карткам. Сервери та комутаційне обладнання розташовуються у спеціально обладнаній для них кімнаті. Обладнання кімнати забезпечує необхідний температурний режим і вологість повітря відповідно до технічних умов на встановлене устаткування. Доступ до серверної кімнати повинні мати тільки адміністратори відповідних категорій. Доступ повинен фіксуватися у відповідних реєстрах.

Розташування, монтаж і прокладка інженерно-технічних комунікацій АІАС, у тому числі заземлення та електроживлення апаратних засобів, які забезпечують обробку інформації, мають виконуватись з дотриманням вимог державних стандартів і настанов.

Структура КЗЗ. Розподіленою 3-ланковою архітектурою АІАС (клієнт – сервер застосувань – сервер БД) диктується й розподілена архітектура КЗЗ. Вона визначається такими основними підсистемами:

1) антивірусного захисту;
2) захисту від НСД;
3) аналізу захищеності й виявлення уразливостей;
4) виявлення вторгнення (IDS);
5) маршрутизації, комутації і міжмережного екранування;
6) криптографічного захисту інформації.

До складу КЗЗ АІАС мають входити такі компоненти:

- механізми захисту, вбудовані в операційну систему робочих станцій (зазвичай це Windows XP);
- механізми захисту, вбудовані в операційну систему сервера застосувань (наприклад, Windows 2008 Server і контролери домену Active Directory);
- механізми захисту, вбудовані в СКБД (часто це Oracle) сервера баз даних;
- механізми захисту, вбудовані в операційну систему сервера обміну;
- механізми захисту, вбудовані в ОС активного мережного обладнання;
- КЗЗ модуля веб-інтерфейсу;
- міжмережні екрани;
- засоби перевірки ЕЦП;
- антивірусні засоби, встановлені на робочих станціях, серверах та серверах обміну;
- засоби зберігання (резервування) файлів функціонального ПЗ, даних його конфігурації, файлів ПЗ КЗЗ, даних КЗЗ, журналів аудиту, поточних даних конфігурацій апаратного та програмного забезпечення мережних пристроїв тощо.

Служба Microsoft Active Directory призначена для організації сервера домену і містить у собі такі сервіси, як мережні папки, файлові ресурси, FTP сервери, маршрутизація, DNS, DHCP тощо, забезпечення політики безпеки домену та централізованого керування користувачами домену, а також захист ресурсів, що є доступними в мережі.

Керування службою Active Directory може здійснювати лише адміністратор безпеки, таким чином реалізується адміністративне керування доступом до робочих станцій (політика локального входу в систему, що є членом домену, визначається не локально, а службою домену) і до мережних ресурсів.

КЗЗ ОС, що встановлюється на серверах АІАС, має забезпечувати захист ресурсів серверів АІАС, безперервне в постійному режимі виконання програм на серверах, у тому числі підтримку серверів баз даних. Сервери баз даних забезпечують адміністративне керування доступом по відношенню до сильнозв'язаних об'єктів, захист цілісності об'єктів, доступ до об'єктів за технологією транзакцій, реєстрацію подій. Керування атрибутами доступу до захищених об'єктів сервера баз даних здійснює адміністратор безпеки.

Механізми захисту системи Windows XP, що встановлюється на робочих місцях користувачів АІАС, забезпечують захист локальних ресурсів кожного комп'ютера, проведення ідентифікації та автентифікації користувачів при їх вході в систему, запуск програм користувача з використанням клієнтського ПЗ сервера застосувань.

Система Windows XP має сертифікат відповідності вимогам стандарту ISO 15408, що є свідченням міжнародного визнання безпеки цієї ОС. Також ця система має висновок ДСТСЗІ СБ України від 12.07.05 р. № 70 з профілем {КД-2, КО-1, КВ-2, ЦД-1, ЦО-1, ЦВ-2, ДР-1, ДЗ-1, ДВ-1, НР-2, НІ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1, НА-1, НП-1}.

Заходи щодо забезпечення захисту мережі. Важливою складовою частиною АІАС, але і найбільш уразливою, є телекомунікаційне середовище органу влади. Однією з найпоширеніших загроз залишається несанкціоноване проникнення в інформаційні системи з мережі. За даними американського Інституту комп'ютерної безпеки (Computer Security Institute), найбільш широко хакерами використовуються наступні методи:

- підбір паролів (brute-force) — 13,9 % від загальної кількості;
- заміна Ip-адрес (IP-spoofing) — 12,4 %;
- ініціювання відмови в обслуговуванні (denial of service — DoS) — 16,3 %;
- аналіз трафіку (sniffer) — 11,2 %;
- сканування (scanner) — 15,9 %;
- підміна даних, які передаються мережею (data didling) — 15,6 %;
- інші методи — 14,7 %.

Ураховуючи, що існує й низка небезпечних загроз для функціонування корпоративної мережі, пов'язаних з поєднанням вказаних методів, таких як «Маскарад» (несанкціонований доступ до важливих систем), «Підслуховування» (отримання конфіденційної інформації для подальшого зловживання нею) та ін., безпека мережної інфраструктури має бути інтегрованою частиною сучасних мережних технологій, що застосовуються в АІАС.

Важливий елемент безпеки мережі АІАС становить безпека периметра — зв'язана з функціями міжмережних екранів, які дозволяють чи забороняють конкретні трафіки від різних зон мережі (класичним прикладом є перевірка трафіку між мережею та Інтернетом), а також безпека логічного доступу — відноситься до забезпечення механізмів ідентичності (ідентифікації та авторизації).

Задіяне активне мережне обладнання повинно мати наступні функції:

а) повне або часткове екранування із захистом внутрішньої мережі від вторгнення;

б) міжмережне екранування між групами у внутрішній мережі;

в) забезпечення безпеки з'єднань підрозділів ОДВ;

г) міжмережне екранування між мережею АІАС та іншими відомчими мережами;

д) шифрування трафіку;

е) моніторинг трафіку;

ж) забезпечення виявлення вторгнень (IDS).

Слід відзначити, що при наявності в АІАС власного веб-сервера необхідно забезпечити захист внутрішньої мережі від зовнішніх атак через цей веб-сервер, наприклад, розмістивши його в демілітаризованій зоні (DMZ).

У мережах органу влади як комутатори, маршрутизатори, сервери доступу зазвичай застосовують пристрої Cisco. Для керування ними використовуються засоби CiscoWorks NMS та Cisco Secure ACS (ACS) як важливі елементі архітектури Cisco Identity-Based Networking Services (IBNS), заснованою на стандартах забезпечення безпеки портів.

CiscoWorks NMS призначений для спостереження і формування звітів про стан устаткування, налаштувань і їхні зміни, керування конфігураціями і ПЗ пристроїв Cisco, аудиту мережних змін і зберігання журналу та ін. У свою чергу Cisco Secure ACS (ACS) розширює ресурси забезпечення безпеки доступу, об'єднуючи функції автентифікації,

призначеної для користувача і адміністративного доступу з політиками, включаючи рішення централізованої мережної ідентифікації.

Рішення щодо створення абонентського пункту спеціальної інформаційно-телекомунікаційної мережі органів влади. Спеціальна інформаційно-телекомунікаційна система органів виконавчої влади (СІТС) як перша черга Національної системи конфіденційного зв'язку створюється на виконання відповідного розпорядження Кабінету Міністрів України від 11 червня 2003 р. № 338. Її створення передбачено Законом «Про національну систему конфіденційного зв'язку», прийнятого в 2002 році. Йдеться про спеціальні мережі зв'язку, які за допомогою криптографічних і технічних засобів забезпечуватимуть обмін конфіденційною інформацією між органами державної влади та місцевого самоврядування для переходу до електронної безпаперової технології, упорядкування реєстрації документів і вилучення дублювання роботи з введення інформації за рішенням керівництва всіх рівнів, централізованого збереження даних про всі доручення, оперативного відбору документів тощо.

Згідно з концепцією СІТС в органах влади створюються абонентські вузли цієї системи. В абонентському вузлі СІТС як маршрутизатор доступу доцільно використовувати таку конфігурацію (рис. 5.52):

1) маршрутизатор Cisco2651XM із вбудованим блоком живлення, двома портами 10/100BaseTX, портами для керування та розширеним обсягом пам'яті;

2) міжмережна ОС IOS з функціональністю IOS Enterprise plus;

3) інтерфейсна карта VWIC-1MFT-E1 з портом E1.

Підключення маршрутизатора до абонентського мультиплексора здійснюється через пристрій криптографічного захисту інформації Д-300. Ethernet-порт маршрутизатора використовується для підключення АРМ системи «Контроль виконання доручень» (КВД), оснащеного мережним адаптером 100BaseTX.

Централізований захист мережного обладнання по мережі електроживлення здійснюється за допомогою джерела безперебійного живлення (ДБЖ) NetPro 2000 19". Для підтримки віддаленого нагляду та керування в цей пристрій установлено SNMP-карту. Мережене обладнання та ДБЖ установлюється в спільній комутаційній шафі 19".

Пристрій Д-300 криптографічного захисту інформації в цифрових потоках E1 (СЕРТ, РСМ 30, 2.048 Мбіт/с) здійснює прийом лінійного сигналу зі сторони відкритого потоку, шифрування інформації методом гамування відповідно до ГОСТ 28147-89, формування та передачу за-

критого сигналу в лінію, прийом закритого сигналу зі сторони закритого потоку, розшифрування, формування та передачу сигналу у напрямку відкритого потоку.

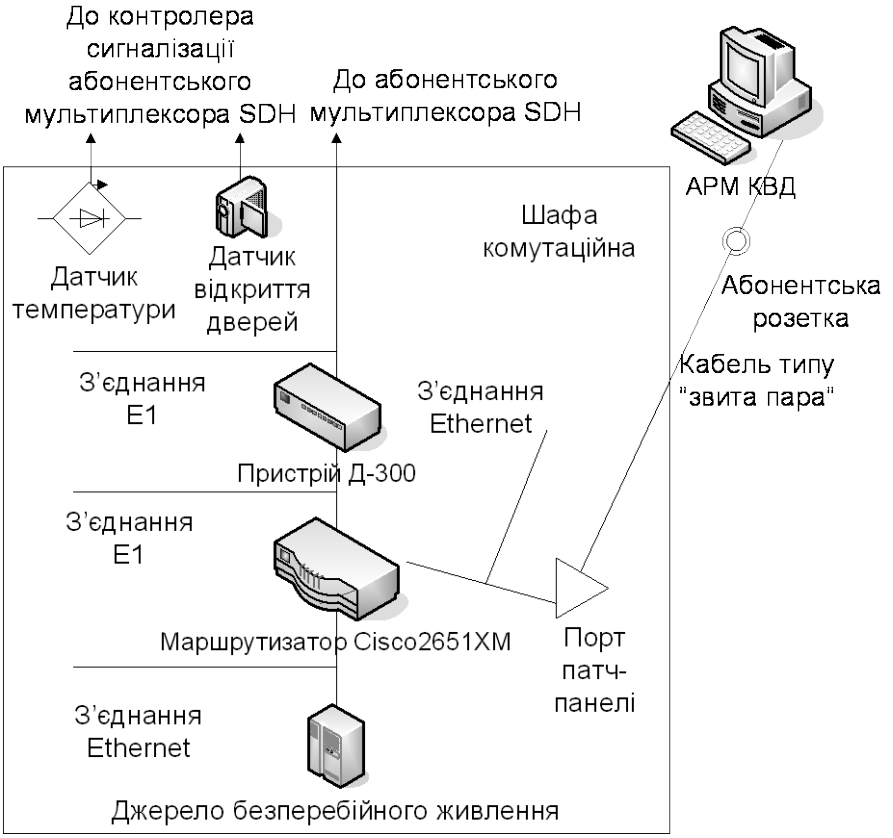

Рис. 5.52. Загальна схема з'єднань абонентського пункту СІТС

Об'єктом канального шифрування є фреймований потік E1, що відповідає рекомендаціям CCITT G.704, G.706, G.732, G.775, G.796, I.141 та системам часового розділення ETSI ETS 300 001. Види кодування сигнального рівня — HDB3.

Безпека Д-300 підтримується системою контролю та знищення критичної інформації як за командою оператора, так і при виявленні несанкціонованого доступу до апаратури.

Для об'єднання абонентського вузла та АРМ у разі їхнього знаходження в різних приміщеннях створюється кабельна система. До складу кабельної системи мають входити комутаційні шафи, крос-панелі, інформаційні розетки, кабелі та інші елементи, які дозволяють побудувати цілісну та гнучку мережу кабельних магістралей багатофункціонального призначення.

Пропонується кабельна система з елементною базою категорії FREENET виробництва швейцарської компанії R&M. Елемента база розрахована на передачу інформаційного сигналу зі смугою частот до 125 МГц. Вибирається інсталяційний кабель збалансованого типу «звита пара», який повинен мати відповідні параметри. У цілому кабельна система повинна повністю відповідати стандартам ANSI та IEEE, а також усім відомим європейським стандартам стосовно електромагнітної сумісності.

З метою забезпечення протипожежних заходів при створенні кабельної системи необхідно використовувати короби та комплектуючі з ПХВ виробництва «Kopos Kolin» та R&M.

Захист інформації на основі інфраструктури відкритих ключів. Як вище зазначалося, концепція безпеки в АІАС має передбачати реалізацію технологій захисту інформації на всіх рівнях інформаційної системи, передусім автентифікацію суб'єктів і контроль доступу до об'єктів. Серед цих технологій найважливіше місце займає захист інформації за допомогою засобів шифрування (рис. 5.53).

Засоби шифрування в системі безпеки АІАС відіграють важливу роль перш за все для забезпечення автентифікації суб'єктів, яка передбачає:

- автентифікацію користувачів у домені з використанням смарт-карток (протокол Kerberos PKINIT);
- автентифікацію віддаленого користувача (розширений протокол EAP-TLS);
- автентифікацію при встановленні захищеного каналу (протокол SSL/TLS);
- автентифікацію хостів при встановленні сеансу IP Security;
- відповідність сертифіката облікового запису домену;
- автентифікацію користувачів, що не мають облікових записів у домені.

Мікрочип, інтегрований у пластикову картку, містить сертифікат користувача та особистий ключ користувача. Ідентифікація власника відбувається завдяки його персонального ідентифікаційного номера

(PIN). Підтримка смарт-карток вбудована в сучасні операційні середовища, зокрема такі, як Windows 2003 і Windows XP.

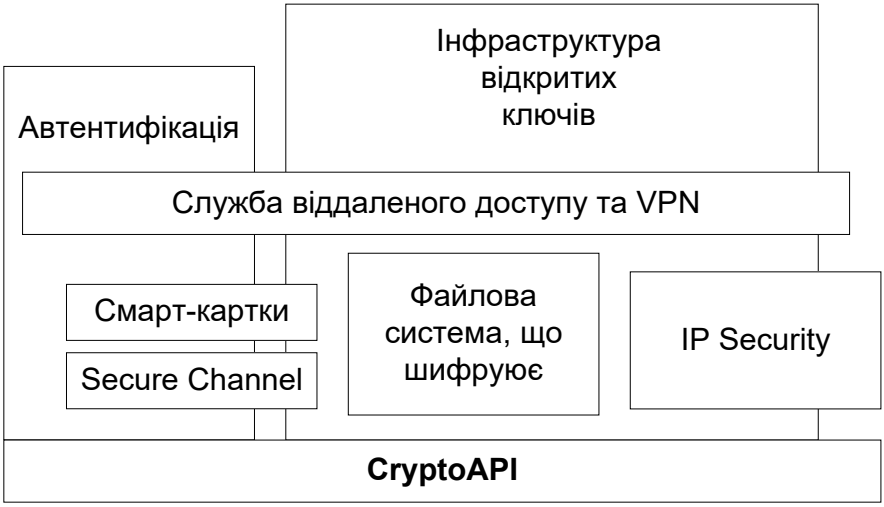

Рис. 5.53. Технології захисту інформації в АІАС за допомогою засобів шифрування

Файлова система, що забезпечує шифрування (EFS), має відповідати таким вимогам, як шифрування даних на рівні файлових операцій NTFS з використанням пари ключів, прозорий доступ до зашифрованих даних з додатків, можливість доступу декількох користувачів до зашифрованих даних, а також мати графічний інтерфейс для підключення інших користувачів до зашифрованого файла (рис. 5.54, 5.55).

Підвищення безпеки на засадах методів і механізмів забезпечення живучості АІАС. Для сучасних інформаційних систем характерним є функціонування в необмежених мережних середовищах, таких як Інтернет, сполучення централізованого й децентралізованого адміністративного керування, відсутність єдиної політики безпеки. У необмежених мережних середовищах відсутня глобальна спостережуваність, тому кількість і тип вузлів (апаратно-програмних комплексів), що підключені до таких мереж, не завжди можуть бути визначені.

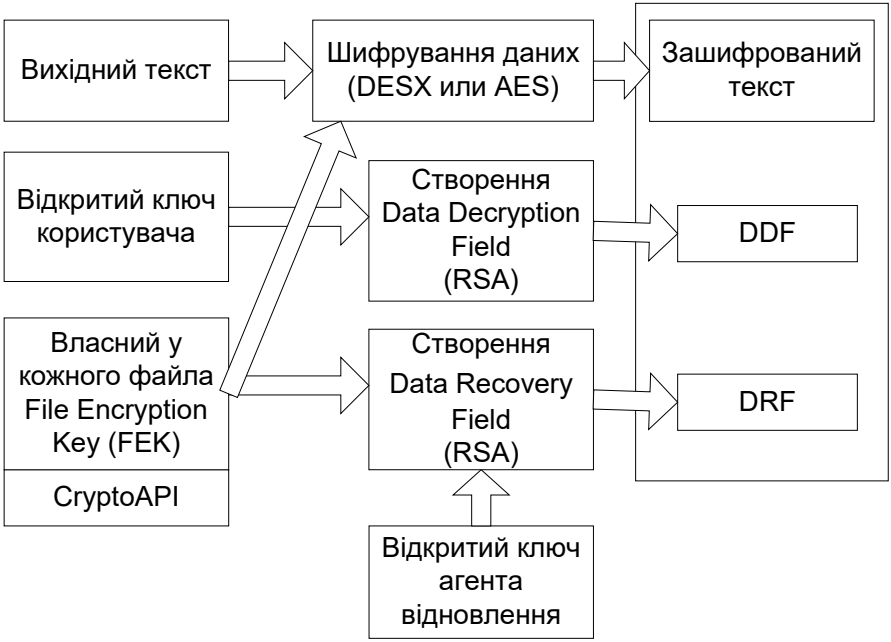

Рис. 5.54. Алгоритм шифрування файла з вихідним текстом

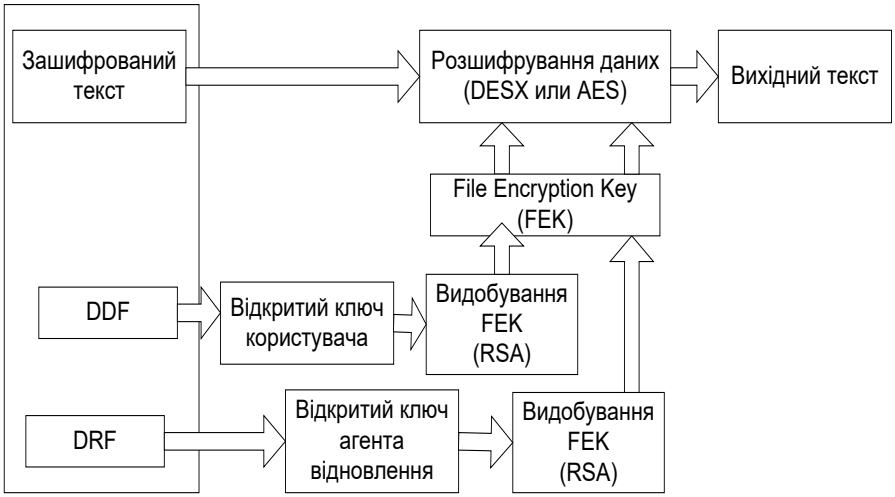

Рис. 5.55. Алгоритм розшифрування зашифрованого файла

Класичні методи захисту інформації не можуть гарантувати невразливість ІС, яка підключена до такого необмеженого середовища, оскільки базуються на моделі «фортеці», а засобів жорсткого розмежування вузлів, що заслуговують довіри, і вузлів, які потенційно можуть бути порушниками, не існує. Украй складним є визначення довірчих відносин між компонентами відкритих систем, а це послаблює цінність використання моделі «фортеці», де система захищена настільки, наскільки захищена її найслабкіша ланка.

У той же час механізми забезпечення живучості дозволяють виконувати у відкритих системах цілеспрямовану зміну конфігурації системи з метою покращання її захисту й ускладнення організації атак на систему.

Живучість систем — це властивість складних систем адаптуватися до непередбачених ситуацій, протистояти небажаним впливам і виконувати ціль функціонування за рахунок зміни поведінки і структури системи [180].

Поняттям «небажані впливи» визначають можливі відмови, збої і порушення в роботі апаратного і програмного забезпечення, різноманітні атаки на систему, катастрофічні впливи природного чи техногенного походження, але важлива не природа впливу, а його наслідки для системи [181, 182]. Традиційно безпека інформаційних систем базується на посиленні захисту системи та її компонентів. Наявність властивості живучості дозволяє системі функціонувати при наявності небажаних впливів і їх накопиченні, зберігатися як ціле в екстремальних для неї умовах.

Для розподілених інформаційних систем розрізняють функціональну, структурну та інформаційну живучість. Під *функціональною живучістю* розуміють здатність системи виконувати ціль функціонування із заданою якістю в умовах наявності небажаних впливів за рахунок механізмів зміни (редукції) цілі. *Структурна живучість* — це здатність системи виконувати ціль функціонування із заданою якістю в умовах наявності небажаних впливів за рахунок механізмів підтримки необхідної системної структури. *Інформаційна живучість* — здатність системи підтримувати доступність, цілісність і конфіденційність інформації на рівні, що дозволить виконувати ціль функціонування із заданою якістю незалежно від інформаційних впливів і порушень у користуванні інформаційними ресурсами.

Впровадження тих чи інших механізмів забезпечення живучості у комп'ютерні системи обґрунтовується аналізом ризиків, врахуванням

специфіки і цілі функціонування кожної конкретної системи. Механізми живучості дозволяють ще до проведення аналізу причин події (порушення безпеки) зреагувати на небажаний вплив і забезпечити перехід системи в безпечний для неї стан. Отже, спираючись на механізми забезпечення живучості можна будувати системи захисту на схемах «що, якщо», а не на класичних схемах «захист від».

На завершення як приклад доцільно навести рішення з інформаційної безпеки в ЄДАПС. Ураховуючи призначення системи, це питання є одним з найважливіших. Воно забезпечується як стандартними системними, так і спеціалізованими засобами захисту інформації, а також організаційними заходами. Для всіх приміщень, де експлуатуватиметься ЄДАПС, установлюється режим обмеженого і підконтрольного доступу. Співробітники паспортної служби працюють в обмежених їхніми службовими обов'язками зонах. Розроблено спеціальні інструкції на випадок пожежі, несправності системи енергозабезпечення, нападу, терористичного акту, стихійного лиха, аварії, катастрофи, іншої надзвичайної ситуації.

Працездатність системи в цілому не повинна залежати від стану працездатності будь-якого суб'єкта місцевого чи регіонального рівня. Тому всі суб'єкти місцевого рівня постійно контролюються відповідними суб'єктами регіонального рівня, а суб'єкти регіонального рівня разом із суб'єктами місцевого рівня — головним центром паспортизації. Підсистема контролю доступу і захисту інформації автоматично виявляє несанкціоноване чи нерегламентоване проникнення в систему, фіксує фізичні аномалії або несправність апаратних засобів і надає можливість адміністраторам системи вживати всіх необхідних заходів. У критичних випадках окремі вузли або підсистеми можуть бути заблоковані чи ізольовані.

Багаторівнева комбінація фізичних, технічних, математичних і організаційних методів захисту інформації має підтримувати їхню повну цілісність і секретність одночасно. На всіх рівнях мережа обміну інформацією захищена від несанкціонованого доступу. Рівень захисту інформації не залежить від місця її проходження і визначається лише її змістом.

Програмні засоби захисту мережі від несанкціонованого доступу повинні забезпечувати запобігання втратам, крадіжкам, несанкціонованому знищенню, викривленню, підробленню, несанкціонованому копіюванню інформації користувачами, що є зовнішніми стосовно захищеної мережі.

Підсумки розділу

Враховуючи сучасні умови державного управління, зорієнтовані на «клієнтське обслуговування» громадян, певні інформаційні технології автоматизованого управління підприємствами, що добре опрацьовані та апробовані, можуть бути застосовані і в АІАС.

Методологічні підходи до використання інформаційних технологій в АІАС мають базуватися також на підтримці парадигми адаптивного органу влади, який спроможний, завдяки застосуванню ІКТ, в умовах постійних змін і невизначеності оперативно пристосовуватись до таких обставин і забезпечувати прийняття ефективних рішень і взаємодію з населенням.

Ці парадигми є основою вимог до видів забезпечення АІАС як комплексних корпоративних систем на базі апробованих рішень та інформаційно-телекомунікаційних платформ, у першу чергу, інформаційного забезпечення, до підходів щодо побудови апаратного та програмного забезпечення основних складових АІАС, методології надання онлайнових послуг за допомогою веб-порталів, Інтернет-приймалень.

Найважливішою передумовою формування системи інформаційних ресурсів органів державної влади (СІРВ), яка має неабияке значення для забезпечення функціонування АІАС, а також для забезпечення інтеграції цих систем в ІІАС, є розвиток системи національних інформаційних ресурсів (СНІР). Побудова системи інформаційних ресурсів органу державної влади як інтегрованого інформаційного середовища має відбуватись на базі концепції сховища даних, спільного використання технологій OLAP і геоінформаційних систем (ГІС), а також реєстру інформаційних ресурсів, має використовуватись загальні джерела інформації, єдина технологія інтеграції різнорідних баз даних, наступного аналізу інформації й візуалізації його результатів.

Для розв'язання проблем систематизації, обробки і безпечного збереження значних обсягів документальної інформації в органі влади необхідне застосування сучасних систем електронного документообігу з використанням єдиного файлового формату офісних документів на базі мови XML та електронного цифрового підпису.

Основою аналітичної діяльності в АІАС повинні стати спеціалізовані СППР на базі багатовимірних сховищ даних (OLAP-технології) та DataMining.

Підходи до створення телекомунікаційного середовища АІАС повинні мати за основу побудову спеціалізованої закритої корпоративної

мережі за технологіями Інтернет/Інтранет на базі веб-сервісів шляхом побудови віртуальних приватних мереж.

З метою забезпечення вирішення проблем використання не ліцензійного програмного забезпечення, суттєвої економії при придбанні технічних і програмних засобів, а також інформаційної безпеки основні засади застосування апаратного та програмного забезпечення в АІАС мають полягати в організації АРМів фахівців на багатотермінальних комплексах із застосуванням операційного середовища на базі систем з відкритими кодами (системи Linux).

Відповідно до принципів інформаційної безпеки при створенні та функціонуванні АІАС повинна створюватися комплексна система захисту інформації (КСЗІ АІАС), що має забезпечити конфіденційність, цілісність, доступність інформації та спостережуваність за технологічним процесом її обробки. При цьому необхідно використовувати засоби шифрування на базі інфраструктури відкритих ключів і враховувати механізми забезпечення живучості АІАС.

ПІСЛЯМОВА

У сучасних умовах рівень розвитку інформаційно-аналітичного забезпечення державної управлінської діяльності з використанням нових інформаційних технологій, які дозволяють кардинально змінити взаємовідносини влади та суспільства, набуває важливого, а можливо і вирішального значення. Разом з тим, обумовлена цими обставинами відкритість, взаємозалежність технологій та сфер діяльності веде до потенційної уразливості та небезпеки. Водночас досліджень щодо питань вдосконалення інформаційно-аналітичної діяльності в органах влади на базі ІКТ, зокрема, з урахуванням вирішення проблем інформаційної безпеки державної влади, вкрай недостатньо. Переважна кількість публікацій присвячена лише окремим питанням створення конкретних автоматизованих інформаційно-аналітичних систем, засобів захисту інформації в них, не розкриваючи загальних тенденцій, підходів, положень і методологій.

Ще не існує ані методів інтеграції елементів інформатизації органу державної влади в єдину систему, ані концептуальних чи інформаційних моделей таких АІАС. Аналіз та оцінка існуючих підходів засвідчують, що нині відсутні не тільки строга теорія проектування подібних АІАС, а й чітке визначення самого цього терміна. У зв'язку з цим постає задача не лише розробки вказаних моделей, а й розробки на базі запропонованих моделей парадигми, що містила б сукупність архітектурних рішень та методологію формування як окремих АІАС органів влади, так і міжвідомчих інформаційно-аналітичних систем. Останні забезпечували б належний рівень захищеності інформаційної інфраструктури та в цілому інформаційної безпеки державної влади. У книзі вперше зроблено спробу вирішити ці важливі науково-прикладні проблеми та отримати практичні рекомендації для забезпечення створення АІАС у різних органах влади.

На відміну від відомих підходів та рішень запропоновано розглядати проблему побудови АІАС згідно, по-перше, з двома парадигмами — відкритості влади та адаптивного органу влади, а, по-друге, з позицій необхідності подальшої інтеграції АІАС в єдину державну систему. При цьому враховується необхідність забезпечення ефективної інформаційної взаємодії АІАС як з системами інших органів влади, так і з підприємствами та громадянами в рамках системи «електронного урядування». Ураховуючи сучасні умови державного управління, зорієнтовані на «клієнтське обслуговування» громадян, певні інформаційні технології автоматизованого управління підприємствами, що добре

опрацьовані та апробовані, можуть бути застосовані і в АІАС. Об'єднуючим принципом є урахування проблематики безпеки інформаційної інфраструктури державної влади.

Також визначено необхідні передумови побудови АІАС, що мають створюватись за активною підтримкою держави. Вони полягають у тому, що АІАС повинні стати елементами загальної електронної інфраструктури країни, а вирішення проблем формування та розвитку інформаційного забезпечення органів влади неможливе поза створенням системи національних інформаційних ресурсів, без широкого застосування Інтернет-технологій та належного розвитку національного сегменту Інтернету.

Принциповою відмінністю запропонованих підходів від наявних досліджень є й те, що вони дозволяють забезпечувати адаптування АІАС згідно з тенденціями в перебудові системи державного управління, відкритості відносин суспільства і держструктур, забезпечення ефективності та безпечності інформаційної взаємодії органів влади між собою та з суб'єктами суспільства в умовах наявності складних випадкових та навмисних загроз, що має визначальне значення для ефективного функціонування органів влади.

У рамках подальшого розвитку концепції інформаційного менеджменту визначено, обґрунтовано та досліджено питання ефективності АІАС, яке зводиться до вирішення завдання забезпечення інформаційною підтримкою сформульовану в органі влади політику виконавчої обов'язковості, запропоновано відповідні методи, що враховують аспекти інформаційного навантаження в системі.

У процесі вирішення проблем інформатизації органів влади доведено, що визначальним для побудови АІАС є розроблення структури інформаційного середовища органу влади, основ інформаційної взаємодії органів державної влади, створення системи інформаційних ресурсів органів влади та забезпечення їх доступності для громадян. При цьому значна увага має приділятися створенню основ побудови спеціалізованих підсистем АІАС для інформаційної підтримки прийняття рішень і забезпечення аналітичної діяльності із забезпеченням необхідного рівня інформаційної безпеки.

У зв'язку з цим запропоновані рішення щодо створення та забезпечення управління системами інформаційних ресурсів органів влади, їх інтеграції на основі використання геоінформаційних технологій, набули подальшого розвитку основні засади регламенту інформаційної взаємодії з урахуванням питань інформаційної безпеки.

Розглядаючи методологію дослідження специфіки інформаційного навантаження в АІАС, запропоновано основи нової теорії ситуаційного регулювання технологічних процесів в органі влади при автоматизованій обробці окремих інформаційних (документальних) потоків з використанням оцінок інтенсивностей надходження потоків документів, а також з урахуванням особливостей пріоритетності та дисципліни їхнього обслуговування, що дає можливість визначити особливості інформаційного навантаження.

Для вирішення проблеми структурування інформаційних потоків, що циркулюють між органами державної влади, застосовано теорію логіко-лінгвістичних інформаційних моделей, що реалізується методологією формування понять на основі методології зростаючих пірамідальних мереж. Нарешті, визначено відповідні архітектурні рішення з підвищеною ефективністю функціонування, запропоновано методологію формування видів забезпечень та технологічних підсистем АІАС.

Проведений системний аналіз органа державної влади, розгляд його цілей, задач і функцій, класифікація АІАС органів влади і на основі цих результатів визначення базових архітектур і їхніх структурних елементів можуть мати теоретичне і практичне значення для концептуального синтезу конкретних АІАС органів влади, при вирішенні проблем вибору комплексу програмно-технічних засобів АІАС, оцінки інтенсивності інформаційного обміну, а також при розв'язанні інших задач, пов'язаних із формуванням і розвитком зазначених систем, що дозволяє проектувати, впроваджувати та розвивати АІАС для органів державної влади, які забезпечують необхідний рівень інформаційної безпеки, а також інтегрувати їх до єдиної системи.

Запропоновані рішення та подані рекомендації стали основою для створення архітектурних рішень АІАС у різних органах влади України, а саме при побудові ІАС Держкомзв'язку, Автоматизованої системи експортного контролю (АСЕК), Єдиної Державної автоматизованої паспортної системи (ЄДАПС), Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій (УІАС НС), ІАС Національної комісії з питань регулювання зв'язку України, а також при розробці типової системи інформаційно-аналітичного забезпечення місцевих державних адміністрацій та органів місцевого самоврядування, складові якої впроваджено в кількох облдержадміністраціях.

Незважаючи на те, що вказані системи призначені для вирішення зовсім різних завдань, завдяки виявленню спільних характеристик і функцій, що виконуються, стало можливим застосувати розроблені підхо-

ди до їх побудови. Усі системи організовано за рівневою територіально-розподіленою архітектурою, мають центральну систему (центральний вузол), у них забезпечується повний цикл обробки інформації, а також створення та ведення інформаційної бази, практично безпаперова технологія, підтримується значний обсяг аналітичних обчислень, системи відповідають вимогам щодо захисту інформації тощо. Таким чином, організаційно-функціональна структура систем, принципи інформаційної взаємодії структурних елементів, технологічні рішення відповідають розробленим основним архітектурним рішенням.

Проблема синтезу та проектування АІАС із необхідним рівнем інформаційної безпеки як нового класу складних соціотехнічних систем державного рівня, вирішення якої дає інструмент для створення систем у вигляді єдиного комплексу науково-методологічних положень, проблемно-орієнтованої методології, математичних моделей, алгоритмів, програм і інформаційних технологій — це проблема, що потребує широкого фронту наукових досліджень. Автор сподівається, що ця книга дасть поштовх у напряму істотнішої інтенсифікації таких досліджень і приверне увагу відповідних державних органів до їхньої підтримки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Авер'янов В.Б.* Державне управління: теорія і практика / В.Б. Авер'янов, В.В. Цвєтков, В. М. Шаповал [та ін.]; за ред. В.Б. Авер'янова; НАН України; Інститут держави і права ім. В.М. Корецького. — К.: Юрінком Інтер, 1998. — 431 с.

2. *Рижих В.М.* Державне управління науково-технічним прогресом: економічні аспекти: автореф. дис. на здобуття наук. ступеня д-ра наук з держ. управління: спец. 25.00.05 «Державне управління» / В.М. Рижих; Укр. академія держ. управління при Президентові України. — К., 1999. — 36 с., включ. обкл.: іл.

3. *Леслі А. Пал.* Аналіз державної політики / Пал Леслі А. — К.: Основи, 1999. — 422 с.

4. *Баранчук В.* Роль місцевого самоврядування в становленні та реформуванні системи територіальної організації державної влади в Україні / В. Баранчук // Державне управління, державна служба і місцеве самоврядування [за ред. О. Оболенського]. — Хмельницький: Поділля, 1999. — С. 330–352.

5. *Комунальне* самоврядування // Баварська школа управління. Федеральна академія державного управління. — 1998. — Серія V. — Т. 2. — 210 с.

6. *Корнієнко М.* Концептуальні основи місцевого самоврядування України / М.Корнієнко // Місцеве та регіональне самоврядування України. — 1992. — Вип. 2. — С. 15.

7. *Котюк В.О.* Загальна теорія держави і права: навч. посіб. / В.О. Котюк. — К.: Атіка, 2005. — 592 с.

8. *Соловйова І.В.* До питання про визначення поняття державної влади в Україні / І.В. Соловйова // Правова держава. — 1998. — Вип. 9. — С. 329–332.

9. *Прохожев А.А.* Теория развития и безопасности человека и об-щества / А.А. Прохожев. — М.: Ин-октаво, 2006. — 288 с.

10. *Оболенський О.* Державне управління і державна служба України: реформування у світлі світового досвіду / О. Оболенський // Досвід стажування державних службовців у США та ЄС і його роль у становленні демократичного державного управління в Україні: наук.-практич. семінар за міжнародною участю, 11–12 берез. 2002 р.: матеріали семинару / Видавн. УАДУ. — К., 2002. — С. 9–33.

11. *Цвєтков В.В.* Державне управління: основні фактори ефективності: Політико-правовий аспект / В.В. Цвєтков; НАН України; Інститут держави і права ім. В.М.Корецького; Академія правових наук України. — Х.: Право, 1996. — 164 с.

12. *Леліков Г.* Основні напрямки розвитку і удосконалення державної служби / Г. Леліков // Державна служба в Україні: організаційно-правові основи і шляхи розвитку [за заг. ред. В. Авер'янова]. — К.: ВД «Ін-Юре». — 1999. — С. 23–36.

13. *Атаманчук Г.В.* Теория государственного управления / Г.В. Атаманчук. — М.: Изд-во ОМЕГА-Л, 2005. — 584 с.

14. *Контроль* в органах виконавчої влади в сучасних умовах: пер. з англ. / [збірка]. — Видавн. «К.І.С», 2006. — 274 с.

15. *Гриценко О.М.* Суспільство, держава, інформація / О.М. Гриценко. — К.: Ін-т журналістики, 2001. — 165 с.

16. *Відкритість* суспільства і роль державного управління // Урядовий кур'єр. — 2002, 19 липн. — № 130. — С. 4–5.

17. *Права* людини та підзвітність органів влади в Україні (результати дослідження) / Є. Герасименко, Т. Коноплицька, Ю. Привалов [та ін]; [ред. Ю. Саєнко]; НАН України; Інститут соціології; Центр соціальних експертиз. — К.: ПЦ «Фоліант», 2003. — 184 с.

18. *Державне* управління та адміністративне право в сучасній Україні: актуальні проблеми реформування / [В.Б. Авер'янов (гол. ред.), В.Б. Авер'янов (підгот.), І.Б. Коліушко (ред.)]; Укр. академія держ. управління при Президентові України; Ін-т держави і права ім. В.М.Корецького НАН України. — К., 1999. — 50 с.

19. *Дмитрук Н.* Виконавча влада в інформаційному полі України: соціологічний аналіз / Н. Дмитрук, Ю. Привалов // Вісник державної служби України. — 1999. — № 4. — С. 6–9.

20. *Луцкий Г.М.* Информационные системы и общественное единство / Г.М. Луцкий, А.В. Нестеренко, В.Р. Сафонов // Інформація і ринок. — 1996. — № 2. — С. 11–14.

21. *Нестеренко О.В.* Інформаційно-аналітичні системи органів державної влади як основа забезпечення відкритості влади / О.В. Нестеренко // Інформатизація та відкритість влади як засоби демократизації суспільства: круглий стіл, 17 груд. 2002 р. / Національний інститут стратегічних досліджень. — К.: Альтерпрес, 2003. — С. 132–138.

22. *Петров В.В.* Автоматизированные системы массового распространения информации. / Вячеслав Васильевич Петров, Александр Васильевич Нестеренко. — К.: Наук. думка, 1993. — 132 с.

23. *Горбулін В.П.* Засади національної безпеки України: підручн. / В.П. Горбулін, А.Б. Качинський. — К.: Інтертехнологія, 2009. — 272 с. — ISBN 978-966-1648-08-0.

24. *Горбулін В.П.* Національна безпека: український вимір / В.П. Горбулін, О.В. Литвиненко; Ін-т проблем національної безпеки Ради національної безпеки і оборони України. — К.: ПІІ «Інтертехнологія», 2008. — 104 с. — ISBN 978-966-1648-03-5.

25. *Міжнародна* інформаційна безпека: сучасні виклики та загрози / Макаренко Є.А., Рижиков М.М., Ожеван М.А. [та ін.]. — К.: Центр вільної преси, 2006. — 916 с.

26. *Данільян О.Г.* Національна безпека України: сутність, структура та напрямки реалізації: навч. посіб. / О.Г. Данільян, О.П. Дзьобань, М.І. Панов. — Х.: Фоліо, 2002. — 285 с.

27. *Биченок М.М.* Основи інформатизації управління регіональною безпекою / М.М. Биченок. — К.: Ін–т проблем національної безпеки Ради національної безпеки і оборони України, 2005. — 196 с.

28. *Ігнатенко П.П.* Особливості інформатизації суб'єктів економічної та громадської діяльності в контексті формування «Електронної України» / П.П. Ігнатенко, С.Є. Захаренко, О.В. Нестеренко [та ін.] // Зв'язок. — 2003. — № 1. — С. 31–35.

29. *Нестеренко А.В.* Информационно-аналитические системы органов государственной власти в информационном обществе / А.В. Нестеренко // Построение информационного общества: ресурсы и технологии: XI международная науч.-практич. конференция, 2–3 июня 2005 г.: тезисы докл. / УкрИНТЭИ. — К., 2005. — С. 4–5.

30. *Нестеренко О.* Інформатизація владних структур / Олександр Нестеренко // ДК-зв'язок. — 2002. — № 10. — С. 1, 5.

31. *Нестеренко О.В.* Від інформатизації освіти до інформаційного суспільства / О.В. Нестеренко // Нова педагогічна думка. Тематичний спецвипуск «Стратегія управління закладами освіти в умовах формування інформаційного суспільства». — 2002. — № 3–4 (31–32). — С. 214–221.

32. *Нестеренко О.В.* Інформаційне суспільство і масова інформаційна просвіта / О.В. Нестеренко // Комп'ютер в школі та сім'ї. — 2004. — № 4. — С. 3–5.

33. *Кристальный Б.В.* Электронное правительство. Опыт США / Б.В. Кристальный, Ю.В. Травкин; [под ред. В.И. Дрожжинова]. — М.: Эко-трендз, 2003. — 224 с.

34. *Электронная* Европа: планы на ближайшие 3 года / http://www.b2b.ibs.ru

35. *«Электронное правительство»* становится частью европейской действительности [Электронный ресурс]: По материалам журнала «Европа» // Подробности. — 26 марта 2004 г. — Режим доступу до газети: http://podrobnosti.com.ua/power/2004/03/26/109844.html

36. *Данилин А.* Электронные государственные услуги и административные регламенты: от политической задачи к архитектуре «электронного правительства» / А. Данилин. — М.: ИНФРА-М, 2004. — 336 с.

37. *Петров А.В.* Информационные технологии в органах государственной власти: [Электронный ресурс] / А.В. Петров // Информационное общество. — 1999. — Вып. 2. — С. 9–13. — Режим доступу до журн.: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/ 385bcf2af6ade85dc32568bd00394dcb

38. *Федеральная* целевая программа «Электронная Россия» (2002–2010 годы). — Режим доступу: http://www.erussia.minsvyaaz.ru

39. *Шубина Н.В.* Основные положения Концепции государственной поддержки развития и реформирования местного самоуправления в Санкт-Петербурге [Электронный ресурс] / Н.В. Шубина, Л.В. Желонкина, Шевцов П.И. — Режим доступа: http://www.infokniga.ru/ellibr/municipal/d_shubin.html

40. *Государство* в XXI веке [Электронный ресурс] / [Информационный бюллетень]. — Режим доступу: http://www.microsoft.com/rus/government

41. *Основні* аспекти створення «електронного уряду» в Україні / П.П. Ігнатенко, О.В. Нестеренко, І.П. Синицин, В.Ю. Суслов // Зв'язок. — 2002. — № 3. — С. 36–41.

42. *Бебік В.* Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка, паблік рилейшнз / В. Бебік. — К.: Академія, 2005. — 236 с.

43. *Рыжков В.И.* Информационные технологии в государственном и муниципальном управлении: учеб. пособие / В.И. Рыжков. — Хабаровск: Изд-во ДВАГС, 2004. — 220 с.

44. *Введение* в архитектонику информационного пространства: Модели. Проблемы развития / В.И. Гриценко, М.И. Вовк, А.Б. Котова; [ред. С.Е. Ноткина]; НАН Украины ; Междунар. науч.-учеб. центр информ. технологий и систем. — К.: Наук. думка, 2003. — 167 с.

45. *Нестеренко О.В.* Методологія ситуаційного регулювання в автоматизованих системах для забезпечення необхідного рівня інформаційної безпеки державної влади / О.В. Нестеренко // Реєстрація, зберігання і оброб. даних. — 2008. — Т. 10, № 4. — С. 25–36.

46. *Нестеренко О.В.* Засади забезпечення необхідного рівня інформаційної безпеки державної влади / О.В. Нестеренко // Національна безпека: український вимір: щокв. наук. зб. / Рада нац. безпеки і оборони України; Ін-т пробл. нац. безпеки; [редкол.: В.П. Горбулін (голов. ред.) та ін.]. — К., 2009. — Вип. 3 (22). — С. 58–67.

47. *Організаційні* та правові засади створення національного інформаційного простору / А.О. Морозов, В.Л. Косолапов, В.О. Ковтун [та ін.] // Наука та наукознавство. — 2000. — № 3. — С. 29–37.

48. *Тесля Ю.Н.* Основы теории информационного взаимодействия / Ю.Н. Тесля; НАН Украины; Ин-т кибернетики им. В.М.Глушкова. — К., 1995. — 44 с.

49. *Бургин М.С.* Информация как природный и технологический феномен / М.С. Бургин // Інформатизация та нові технології. — 1996. — № 1. — С. 2–5.

50. *Нестеренко О.* Інформаційно-аналітична система органів держав-ної влади / О.Нестеренко // Реєстрація, зберігання і оброб. даних. — 1999. — Т. 1, № 2. — С. 43–50.

51. *Головні* передумови створення інтегрованої інформаційно-аналітичної системи органів державної влади в Україні / Л.І. Куцаченко, О.В. Нестеренко, І.П. Синицин [та ін.] // Зв'язок. — 2001. — № 3. — С. 40–41.

52. *Айвазян С.А.* Информационно-аналитическая поддержка социально-экономических исследований / С.А. Айвазян, А.В. Маракуев, В.Л. Ушкова. —

М., 2001. — 30 с.

53. *Интеллектуальная* информационная система мониторинга политических конфликтов: концепция создания / Бабынин И.В., Кретов В.С., Потапенко Ф.И. [и др.] // НТИ. — 1995. — № 10. — С. 56–75.

54. *Государственная* навигационно-гидрографическая информационная система. Концепция. Реализация / В.И. Грищенко, В.Н. Никулин, А.А. Урсатьев; НАН Украины; Междунар. центр инф. технологий и систем. — К.: Наук. думка, 1999. — 122 с.

55. *Дегтяр А.* Інформаційно-аналітична діяльність як засіб підвищення якості державно-управлінських рішень / А. Дегтяр // Актуальні проблеми державного управління. — Одеса, 2003. — Вип. 2(14). — С. 223–228.

56. *Дорофиенко В.В.* Опыт разработки информационно-управляющих систем в регионе / В.В. Дорофиенко. — Донецк, 1993. — 17 с. (Препринт / Донецкий региональный научный центр УкрАИН).

57. *Дорофиенко В.В.* Управление научно-техническим потенциалом региона (организационно-информационные аспекты) / В.В. Дорофиенко. — К.: УкрИНТЭИ, 1995. — 216 с.

58. *Інформаційно-аналітична* діяльність в міжнародних відносинах // Актуальні проблеми міжнародних відносин. — К., 2002. — Вип. 36. — Ч. 1. — С. 3–61.

59. *Косолапов В.Л.* Автоматизированная система обработки информации и экспертных оценок при анализе общественно-политических процессов / В.Л. Косолапов // Управл. системы и машины. — 1998. — № 1. — С. 25–32.

60. *Косолапов В.Л.* Информационно-аналитическая технология поддержки избирательной компании / В.Л. Косолапов // Мат. машины и системы. — 1998. — № 2. — С. 92–101.

61. *Морозов А.О.* Інформаційно-аналітичні технології підтримки прийняття рішень на основі регіонального соціально-економічного моніторингу / А.О. Морозов, В.Л. Косолапов. — К.: Наук. думка, 2002. — 229 с.

62. *Чичелов Ю.В.* Информационно-аналитическая работа в федеральных органах налоговой полиции: учеб. пособие / Ю.В. Чичелов, К.В. Сомик. — М.: ЧеРо, 2000. — 383 с.

63. *Нестеренко О.В.* Інформаційна інфраструктура органів державної влади для забезпечення електронного урядування / О.В. Нестеренко // Зв'язок. — 2004. — № 2. — С. 28–30.

64. *ДеКонти Л.* Информационные системы для управления государственным сектором [Электронный ресурс]. Раздел 4. Положительный опыт по созданию сайтов: анализ сайтов правительств штатов США / Л. ДеКонти. — 1998. — Режим доступа: http://www.man.ac.uk/idpm

65. *Додонов О.Г.* Архітектура автоматизованих інформаційно-аналітичних систем органів державної влади / О.Г. Додонов, О.В. Нестеренко, М.М. Будько // Мат. машини і системи. — 2003. — № 3, 4. — С. 138–146.

66. *Каныгин Ю.М.* Основы когнитивного обществознания: (Информ. Теория соц. систем) / Ю.М. Каныгин. — К.: Укр. акад. информатики, 1993. — 236 с.

67. *Каныгин Ю.М.* Информатизация управления: социальные аспекты / Ю.М. Каныгин. — К.: Наук. думка, 1991. — 163 с.

68. *Азаров С.С.* Мифы и реальность информатизации посткоммунистического общества / С.С. Азаров, А.А. Стогний // Управл. системы и машины. — 1994. — № 6. — С. 26–37.

69. *Згуровский М.В.* Исследование социальных процессов на основе методологии системного анализа / М.В. Згуровский, А.В. Доброногов, Т.Н. Померанцева. — К.: Наук. думка, 1997. — 221 с.

70. *Винарик Л.С.* Информационная культура: эволюция, проблемы / Л.С. Винарик, А.Н. Щедрин; НАН Украины; Ин-т экономики промышленности. — Донецк, 1999. — 144 с.

71. *Информационная* технология и информационная политика: Научно-информационное исследование (Информация, наука, общество) / РАН; Ин-т научной информации по общественным наукам. — М., 1994. — 208 с.

72. *Луцкий Г.М.* Информационный резонанс и реализация идей / Г.М. Луцкий, А.В. Нестеренко, В.Р. Сафонов // Информационные ресурсы: создание, интеграция и использование: III междунар. науч.-практич. конф., 25 февр. – 1 марта 1996 г.: тезисы докл. / Гута, Ивано-Франковская обл. — К.: УкрИНТЭИ. — 1996. — Ч. 2. — С. 4–8.

73. *Рубан В.Я.* Глобальные проблемы современности и нформатизация / В.Я. Рубан // Состояние и перспективы информатизации в республике. — Киев, 1990. — С. 21–40.

74. *Рубан В.Я.* Проблемы и перспективы информатизации / В.Я. Рубан, М.Т. Матвеев. — К.: Об-во «Знание» УССР, 1991. — 16 с.

75. *Смолян Г.Л.* Национальная информационная инфраструктура — объект действия администрации США / Г.Л. Смолян // Межотрасл. инф. служба. — 1994. — № 2. — С. 29–33.

76. *Kazuhiso M.* Information superhighway: japanese style / M. Kazuhiso // J. Jap. Trade and Ind. — 1993. — Vol. 12, N 4. — P. 40–42.

77. *Матов О.* Інформаційна основа прийняття рішень / О. Матов // Урядовий кур'єр. — 1997, 2 груд., — № 224. — С. 6.

78. *Петров В.В.* Інтеграція інформаційних ресурсів — необхідна умова побудови інформаційного суспільства в Україні / В.В. Петров, Б.О. Березін // Інформаційне суспільство в Україні — стан, проблеми, перспективи : міжнар. конгрес, 25–27 верес. 2000 р. — С. 235—238.

79. *Баранов О.А.* Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. — К.: ВД «Софтпрес», 2005. — 316 с.

80. *Інформатизація* управління соціальними системами: Орг.-правові питання теорії і практики: навч. посіб. / В.Д. Павловський, Р.А. Калюжний, В.С. Цимбалюк [та ін.]; [за заг. ред. М.Я. Швеця, Р.А. Калюжного]. — К.: МАУП, 2003. — 336 с.

81. *Інформатизація* законотворчої, нормотворчої, правозастосовної та правоосвітньої діяльності: посібн. / Л.Є. Горьовий (підгот.). — Секретаріат Верховної Ради України; Академія правових наук України. — К.: Парламентське вид-во, 1999. — 199 с.

82. *Глушков В.М.* Введение в АСУ / В.М. Глушков. — К.: Техніка, 1972. — 312 с.

83. *Глушков В.М.* Что такое ОГАС? / В.М. Глушков, В.Я. Валах. — М.: Наука, 1981. — 160 с.

84. *Глушков В.М.* Основы безбумажной информатики / В.М. Глушков. — Изд. 2-е, испр. — М.: Наука, 1987. — 552 с.

85. *Сергієнко І.В.* Інформатика в Україні: становлення, розвиток, проблеми / І.В. Сергієнко; [Ю.В. Капітонова (відп.ред.), Т.Г. Лебедєва (відп.ред.)]; НАН України; Інститут кібернетики ім. В.М.Глушкова. — К.: Наук. думка, 1999. — 354 с.

86. *Сергієнко І.В.* Становлення і розвиток досліджень з інформатики / І.В. Сергієнко; НАН України; Інститут кібернетики ім. В.М.Глушкова. — К.: Наук. думка, 1998. — 205 с.

87. *Андон Ф.И.* Методы инженерии распределенных компьютерных приложений / Ф.И. Андон, Е.М. Лаврищева; НАН Украины; Институт программных систем. — К.: Наук. думка, 1997. — 228 с.

88. *Багаторівнева* телекомунікаційна мережа для накопичення та обміну інформації в Державному реєстрі фізичних осіб-платників податків та інших обов'язкових платежів / Звіт про науково-технічну роботу. — Інститут проблем реєстрації інформації НАН України. — 1995. — 321 с.

89. *Великий А.П.* Про підходи та принципи дослідження економічної безпеки та деякі результати їх практичного застосування / А.П. Великий, В.П. Горбулін, І.В. Сергієнко // Управл. системы и машины. — 1997. — № 4/5. — С. 5–16.

90. *Голышев Л.К.* Сложные системы с развитой функцией информационно-аналитической поддержки управления. Элементы теории, методологии, практики: монография / Л.К. Голышев. — К., 2001. — 253 с.

91. *Довгий С.О.* Засади регіональної інформатизації / С.О. Довгий, О.В. Копійка, Черепін Ю.Т. [за ред. С.О. Довгого]. — К.: ВПЦ «Тираж», 2004. — 304 с.

92. *Довгий С.О.* Міжнародне співробітництво України у сфері інформатизації і телекомунікацій / С.О. Довгий, В.Л. Банкет, А.В. Клікич [та ін.]; ред. С.О. Довгий; Відкрите акціонерне товариство «Укртелеком». — К.: Укртелеком, 2001. — 448 с.

93. *Єдина* інформаційно-аналітична система «Кадри державної служби зайнятості». Підсистема «Накази» / [уклад М.П. Панченко]; Державний центр зайнятості. — К.: Наук. світ, 2004. — 63 с.

94. *Іванов М.М.* Інформаційно-аналітична система моделювання формування доходної частини місцевого бюджету / М.М. Іванов // Економіка: проблеми теорії та практики. — Д., 2002. — Вип. 154. — С. 229–233.

95. *Кравченко С.* Щодо вибору стилів ухвалення управлінських рішень з використанням сучасних інформаційних технологій / С. Кравченко // Вісник УАДУ. —1998. — № 1/98. — С. 176.

96. *Кривонос Ю.Г.* Некоторые информационные технологии экомониторинга, актуальные для задач экологического права / Ю.Г. Кривонос, В.Г. Писаренко, О.И. Чайковский. — К., 2003. — 36 с. — (Препринт / НАН Украины, Институт кибернетики им. В.М. Глушкова; 2003-1). — С. 33–34.

97. *Математическое* моделирование техногенных воздействий на качество воды в каскаде водохранилищ / В.С. Михалевич, А.А. Морозов, М.И. Железняк, В.В. Михайлов // Актуальные проблемы вычислительной и прикладной математики. — Новосибирск: ВЦ СО АН СССР, 1987. — С. 124–135.

98. *Орлов П.И.* Кадровая информационно-аналитическая система МВД Украины. Описание локальной версии: науч.-практ. пособие / П.И. Орлов, А.М. Луганский, Е.С. Замыслов [та ін.]. — Х.: Изд. Национального ун-та внутренних дел, 2001. — 88 с.

99. *Сидоренко В.* Проблеми зміни мотивацій у необхідності інформатизації при реорганізації органів державного управління / В. Сидоренко, Г. Гажієнко // Вісник УАДУ. — 1998. — № 1/98. — С. 167.

100. *Шиндер В.С.* Методы и программные средства для разработки систем поддержки принятия решений в задачах с пространственной информацией / В.С. Шиндер // Мат. машины и системы. — 2000. — № 2, 3. — С. 64–75.

101. *Шмиголь Н.М.* Інформаційно-аналітична система підтримки прийняття рішень задачі реального інвестування / Н.М. Шмиголь // Економіка: проблеми теорії та практики. — 2004. — Вип. 190. — Т. 2. — С. 350–357.

102. *Морозов А.А.* Некоторые аспекты геополитического и экономического мониторинга / А.А. Морозов, В.Л. Косолапов // Управл. системы и машины. — 1993. — № 4. — С. 20–25.

103. *Морозов А.А.* Ситуационные центры — основа управления организационными системами большой размерности / А.А. Морозов // Мат. машины и системы. — 1997. — № 2. — С. 7–10.

104. *Андрук Г.В.* Актуальні проблеми застосування інформаційно-аналітичних технологій / Г.В. Андрук, В.О. Ковтун, В.Є. Колосов [та ін.] // Мат. машини і системи. — 1999. — № 1. — С. 146–154.

105. *Морозов А.А.* Новые информационные технологии в системах принятия решений / А.А. Морозов // Управл. системы и машины. — 1993. — № 3. — С. 13–22.

106. *Морозов А.О.* Методологія створення інформаційно-аналітичної системи обліку і контролю використання інтелектуальної власності / А.О. Морозов, В.Л. Косолапов, С.П. Козлова [та ін.] // Мат. машини і системи. — 2004. — № 2. — С. 114–133.

107. *Косолапов В.Л.* Автоматизированная система обработки информации и экспертных оценок при анализе общественно-политических процессов / В.Л. Косолапов // Управл. системы и машины. — 1998. — № 1. — С. 25–32.

108. *Косолапов В.Л.* Принципи і організація підтримки прийняття рішень на основі ситуаційних оцінок / В.Л. Косолапов // Наука і наукознавство. — 1997. — № 3–4. — С. 43–52.

109. *Kosolapov V.L.* The designing problems of information technology for comparative analysis of the actors impact in the society transformation / V.L. Kosolapov // Mathematical Machines and Systems. — 1997. — N 2. — P. 71–77.

110. *Косс В.А.* Варіант структури активного об'єкта з точки зору функцій підтримки прийняття рішень в системах типу «Ситуаційний центр» / В.А. Косс // Мат. машини і системи. — 2004. — № 2. — С. 73–78.

111. *Система* поддержки коллективного принятия решения в области охраны вод на базе центра ситуационного управления / А.А. Морозов, М.И. Железняк, В.М. Михайлов, А.Б. Тимофеев // Исследование процедур поддержки принятия решений в автоматических системах. — К.: ИК АН УССР, 1989. — С. 51–58.

112. *Баранов А.А.* Права человека и защита персональных данных: науч. изд. / А.А. Баранов, В.М. Брижко, Ю.К. Базанов // Госкомсвязи и информатизации Украины; Харьк. правозащ. группа. — Киев, 2000. — 280 с.

113. *Додонов О.* Державне регулювання інформатизації України / О. Додонов, О. Нестеренко // Реєстрація, зберігання і оброб. даних. — 1999. — Т. 1, № 6. — С. 43–50.

114. *Горбулін В.П.* Системно-концептуальні засади стратегії національної безпеки України / В.П. Горбулін, А.Б. Качинський. — К.: ДП «НВЦ «Євроатлантикінформ», 2007. — 592 с.

115. *Фомін В.О.* Сутність і співвідношення понять «інформаційна база», «інформаційна війна», «інформаційна боротьба» / В.О. Фомін, А.О. Рось // Наука і оборона. — 1999. — № 4. — С. 23–32.

116. *Качинський А.Б.* Безпека, загрози і ризик: наукові концепції та математичні методи / А.Б. Качинський; Інститут проблем національної безпеки; Національна академія Служби безпеки України. — К., 2004. — 472 с.

117. *Ходаков В.Е.* Управління розвитком підприємства в умовах ризику / В.Е. Ходаков, Д.В. Ходаков // Зб. наук. праць ІФДТУНТ, 1998. — В. 35(7). — С. 156–162.

118. *Бурый А.С.* Структурная сложность распределенных информационно-управляющих систем / А.С. Бурый // Изв. РАН. Техн. кибернетика. — 1994. — № 5. — С. 160–207.

119. *Петров Э.Г.* Методы и средства принятия решений в социально-экономических и технических системах / Э.Г. Петров, М.В. Новожилова, И.В. Гребенюк, Н.А. Соколова. — Херсон: Олді-плюс, 2003. — 380 с.

120. *Венделин А.Г.* Подготовка и принятие управленческого решения / А.Г. Венделин. — М.: Экономика, 1994. — 176 с.

121. *Емельянов С.В.* Многокритериальные методы принятия решений / С.В. Емельянов, О.Н. Ларичев. — М.: Знание, 1985. — 32 с.

122. *Евланов Л.Г.* Теория и практика принятия решений / Л.Г. Евланов. — М.: Экономика, 1984. — 176 с.

123. *Амангильдиев Б.Р.* О некоторых вопросах многокритериальной оптимизации / Б.Р. Амангильдиев // Функциональный анализ и вычислительная математика. — Алма-Ата, 1981. — С. 16–36.

124. *Дубов Ю.А.* Многокритериальные модели выбора вариантов систем / Ю.А. Дубов, С.И. Травкин, Якимец В.Н. — М.: Наука, 1986. — 296 с.

125. *Жуковский В.И.* Многокритериальные задачи управления в условиях неопределенности / В.И. Жуковский, М.Б. Салуквадзе. — Тбилиси: Мецниереба, 1994. — 128 с.

126. *Канторович Л.В.* Оптимальное решение в экономике / Л.В. Канторович, Л.Д. Горстко. — М.: Наука, 1972. —230 с.

127. *Кини Р.Л.* Функции полезности многих альтернатив / Р.Л. Кини // Вопросы анализа и процедуры принятия решений: сб. — М., 1976. — С. 59–79.

128. *Ларичев О.И.* Оптимизация при перспективном планировании и проектировании / О.И. Ларичев. — М.: Экономика, 1984. — 222 с.

129. *Нестеренко О.В.* Основи побудови інформаційно-аналітичних систем органів державної влади / О.В. Нестеренко. — К.: Наук. думка, 2005. — 628 с.

130. *Access* to Information: Making it Work for Canadians / Report of the Access to Information Review Task Force. — Public Works and Government Services, Ottawa. — Catalogue Number BT22-83/2002-MRC. — 2002. — 225 p.

131. *Розробити* і впровадити першу чергу типової системи інформаційно-аналітичного забезпечення місцевого органу виконавчої влади. Методичні рекомендації зі структурного аналізу організацій для впровадження типової системи інформаційно-аналітичного забезпечення їхньої діяльності / Звіт про наук.-дослід. роботу. — К.: Ін-т телекомунікацій і глобального інформаційного простору НАН України. — 2004. — 98 с.

132. *Розробити* і впровадити першу чергу типової системи інформаційно-аналітичного забезпечення місцевого органу виконавчої влади. Алгоритми і задачі процесів управління / Звіт про наук.-дослід. роботу. — К.: Ін-т телекомунікацій і глобального інформаційного простору НАН України. — 2004. — 205 с.

133. *Розробити* і впровадити першу чергу типової системи інформаційно-аналітичного забезпечення місцевого органу виконавчої влади. Аналіз інформаційних потоків в обласній державній адміністрації / Звіт про наук.-дослід. роботу. — К.: Ін-т телекомунікацій і глобального інформаційного простору НАН України. — 2004. — 108 с.

134. *Урядова* інформаційно-аналітична система з надзвичайних ситуацій. Розробка системного проекту / Пояснюв. записка. — К.: ІПРІ НАН України. — 1997. — 169 с.

135. *Урядова* інформаційно-аналітична система з надзвичайних ситуацій. Регламент роботи групи експертної підтримки УІАС НС. — К.: ІПРІ НАН України. — 1998. — 22 с.

136. *Урядова* інформаційно-аналітична система з надзвичайних ситуацій. Створення системи адміністрування та управління УІАС НС / Звіт про наук.-дослід. роботу. — К.: ІПРІ НАН України. — 2001. — 45 с.

137. *Формування* банку даних центрального рівня Єдиної Державної автоматизованої паспортної системи (ЄДАПС) / Звіт про наук.-дослід. роботу. — К.: ВАТ «КП ОТІ». — 2002. — 68 с.

138. *Автоматизована* система експортного контролю / Техно-робо-чий проект. — К.: Ін-т системного аналізу та комп'ютерно-технологічних систем УАН. — 1999. — 187 с.

139. *Створити* першу чергу інформаційно-аналітичної системи Державного комітету зв'язку та інформатизації. Концепція створення та функціонування інформаційно-аналітичної системи Державного комітету зв'язку та інформатизації. — К.: ТОВ «Ер-Джі-Дейта Україна». — 2004. — 55 с.

140. *Інформаційно-аналітична* система Державного комітету зв'язку та інформатизації України (перша черга) / Звіт про НДДКР. — К.: ТОВ «Ер-Джі-Дейта Україна». — 2004. — 75 с.

141. *Нестеренко О.В.* Інформаційна інфраструктура сфери державного регулювання ринку телекомунікацій / О.В. Нестеренко // Зв'язок. — 2008. — № 7–8. — С. 21–27.

142. *Ескізний* проект інформаційно-аналітичної системи Національної комісії з питань регулювання зв'язку / Пояснюв. записка. — К.: БМС Консалтинг. — 2006. — 154 с.

143. *Нестеренко О.В.* Основні засади забезпечення інформаційної взаємодії автоматизованих інформаційно-аналітичних систем органів державної влади / О.В. Нестеренко // Зв'язок. — 2005. — № 5. — С. 2–6.

144. *Нестеренко О.В.* Електронна інфраструктура інформаційного суспільства України / О.В. Нестеренко // Моделювання та інформаційні технології: зб. наук. пр. [спец. випуск] / НАН України; Ін-т проблем моделювання в енергетиці ім. Г.Є. Пухова [редкол.: О.М. Богданов та ін.]. — К., 2005. — С. 15–23.

145. *Нестеренко О.В.* Інформаційно-аналітичні системи органів державної влади в системі «електронного уряду» [Електронний ресурс] / О.В. Нестеренко // Електронний уряд і електронна демократія: міжнар. конф. [в рамках Другої міжнар. конф. «e-Development» спеціалізованої акції «Електронна Україна»]. — 12 квіт. 2002 р. — К., 2002. — С. 16–18. — Режим доступу: http://gipi.internews.ua/rus/activity/initiatives/seminars/papers_WB_conference.pdf

146. *Нестеренко О.В.* Національна мережа обміну Інтернет-трафіком / О.В. Нестеренко, К.С. Синявський // Зв'язок. — 2003. — № 5. — С. 26–31.

147. *Нестеренко О.В.* Національна мережа обміну Інтернет-трафіком. Частина ІІ. Рішення щодо створення мережі / О.В. Нестеренко, К.С. Синявський // Зв'язок. — 2003. — № 6. — С. 20–24.

148. *Балашов В.А.* Обеспечение всеобщего доступа к инфокоммуникационным технологиям и услугам в сельских районах Украины / В.А. Балашов, С.Я. Зяблов, А.В. Нестеренко // Зв'язок. — 2004. — № 7. — С. 10–14.

149. *Створити* систему пунктів колективного доступу до мережі Інтернет / Звіт про наук.-дослід. роботу; Одеський наук.-дослід. ін-т зв'язку. — Одеса, 2004. — 105 с.

150. *Клыков Ю.И.* Семиотические основы ситуационного управления: учебн. пособие / Ю.И. Клыков. — М.: МИФИ, 1974. — 160 с.

151. *Разработка* методов моделирования задач оперативного управления на авиапредприятии / А.Г. Додонов, А.М. Щетинин, Ю.С. Боримский; ИПРИ АН Украины. — К., 1993. — 61 с.

152. *Поспелов Д.А.* Ситуационное управление: Теория и практика / Д.А. Поспелов. — М.: Наука, 1988. — 288 с.

153. *Згуровский М.З.* Системный анализ: Проблемы, методология, применение / М.З. Згуровский, Н.Д. Панкратова; НАН Украины; Ин–т прикладного системного анализа; Нац. техн. ун-т Украины «Киев. политехн. ин-т». — К.: Наук. думка, 2005. — 743 с.

154. *Рогожин М.В.* Побудова інформаційних технологій у системі управління регіонального рівня: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.06 «Автоматизовані системи управління та прогресивні інформаційні технології» / Рогожин М.В.; Ін-т проблем моделювання в енергетиці ім. Г.Є. Пухова. — К., 2002. — 16 с.

155. *Годлевский М.Д.* Задачи координации и управления развитием иерархических распределенных систем на основе государственных механизмов регулирования / М.Д. Годлевский, О.В. Пленис // Вестник национального технического университета «ХПИ». — Х.: НТУ «ХПИ», 2002. — № 3. — С. 57–64.

156. *Клебанова Т.С.* Модели и методы координации в крупномасштабных экономических системах / Т.С. Клебанова, Е.В. Молдовская, Хонгвен Чанг. — Х.: Бизнес Информ, 2002. — 148 с.

157. *Теория* телетрафика: учебн. для вузов / Б.С. Лившиц, А.П. Пшеничников, А.Д. Харкевич. — Изд. 2-е, перераб. и доп. — М.: Связь, 1979. — 224 с.

158. http://uis.kiev.ua/russian/win/~xyz/par_int.rus.html.

159. *Нестеренко О.В.* Інформаційний підхід до забезпечення керування в автоматизованих інформаційно-аналітичних системах органів влади / О.В. Нестеренко // Реєстрація, зберігання і оброб. даних. — 2008. — Т. 10, № 3. — С. 46–55.

160. *Акофф Р.* О целеустремленных системах / Р. Акофф, Ф. Эмери. — М.: Наука, 1974. — 269 с.

161. *Коваль В.Н.* Целенаправленные системы планирования решений / В.Н. Коваль, Ю.В. Кук // Искусственный интелект. — 1999. — № 2. — С. 158–165.

162. *Wooldridg M.* Agent theories, architecture and languages: a survey / M. Wooldridg, N. Jennings // Intelligent Agents: ECAI-94 Workshop on Agent theories, architecture and languages: august, 1994. — Amsterdam: Springer verlag, 1994. — P. 3–39.

163. *Гладун В.П.* Гипотетическое моделирование: методология и применение / В.П. Гладун // Кибернетика и системный анализ. — 1997. — № 1. — С. 10–20.

164. *Гладун В.П.* Партнерство с компьютером. Человеко-машинные целеустремленные системы / В.П. Гладун. — К.: Port-Royal. — 2000. — 128 с.

165. *Комашинский В.* Нейронные сети и их применение в системах управления и связи / В. Комашинский, Д. Смирнов. — М.: Горячая линия – Телеком, 2002. — 94 с.

166. *Осовский С.* Нейронные сети для обработки информации / С. Осовский. — М.: Финансы и статистика, 2003. — 336 с.

167. *Грицик В.В.* Інформаційно-аналітична система оцінки складних зображень, процесів і прогнозування ситуацій на базі штучних нейронних мереж / В.В. Грицик // Вестник Харьковского гос. политехн. ун-та. — Х., 2000. — Вып. 121: Системный анализ, управление и информационные технологии. — С. 109–113.

168. *Теленик С.Ф.* Концепція, моделі, алгоритми та засоби адаптивної технології створення інформаційно-керуючих систем: автореф. дис. на здобуття наук. ступеня д-ра техн. наук: спец. 05.13.06 «Автоматизовані системи управління та прогресивні інформаційні технології» / Теленик С.Ф.; Національний технічний ун-т України «Київський політехнічний ін- т». — К., 2000. — 33 с.

169. *Нестеренко А.В.* Информационный менеджмент — значение и задачи / А.В. Нестеренко // Інформатизація та нові технології. — 1996. — № 3. — С. 20–23.

170. *Гладун В.П.* Локально-статистические методы формирования знаний / В.П. Гладун, Н.Д. Ващенко // Кибернетика и системный анализ. — 1995. — № 2. — С. 62–74.

171. *Ващенко Н.Д.* Формирование понятий в семантической сети / Н.Д. Ващенко // Кибернетика. — 1987. — № 2. — С. 101–107.

172. *Поспелов Д.А.* Логико-лингвистические модели в системах управления / Д.А. Поспелов. — М.: Энергоиздат. — 1981. — 231 с.

173. *Прогнозирование* неорганических соединений, перспективных для поиска новых электрооптических материалов / Киселева Н.Н., Ващенко Н.Д., Гладун В.П. и др. // Перспективные материалы. — 1998. — № 3. — С. 28–32.

174. *Ващенко Н.Д.* Инструментальный комплекс для решения задач обнаружения и анализа закономерностей CONFOR / Н.Д. Ващенко // конф. по искусств. интеллекту: сб. науч. тр. — Тверь, 1992. — Т. 2. — С. 109–113.

175. *Грушо А.А.* Теоретические основы защиты информации [Електронний ресурс] / А.А. Грушо, Е.Е. Тимонина. — Изд. агентства «Яхтсмен», 1996 г. — Режим доступу: http://kiev-security.org.ua

176. *Нестеренко А.В.* Методология классификации и структурирования автоматизированных информационно-аналитических систем органов государственной власти / А.В. Нестеренко // Искусственный интеллект. — 2005. — № 3. — С. 504–520.

177. *Treven S.* Main Function of Strategic Information system / S.Treven // Information Systems Development. — ISD'94. Method & Tools. Theor. & Practice: proc. of the 4-th Int. Conf, 20–22 Sept. 1994. — Bled (Slovenia). — P. 315–322.

178. *Нестеренко О.* Використання ГІС-технологій при організації даних в органах державної влади / О. Нестеренко // Реєстрація, зберігання і оброб. даних. — 2000. — Т. 2, № 1. — С. 60–66.

179. *Нестеренко О.В.* Технології інтеграції інформаційних ресурсів інформаційно-аналітичних систем органів державної влади / О.В. Нестеренко // Науково-технічна інформація. — 2001. — № 4. — С. 3–6.

180. *Network-Centric* Computing. Preparing the Enterprise for the Next Millennium. Computer Technology Research Corp. / http://www.itworks.be/reports

181. *Foster I.* The Anatomy of the Grid: Enabling Scalable Virtual Organizations [Електронний ресурс] / Ian Foster, Carl Kesselman, Steven Tuecke // International J. Supercomputer Applications. — 2001. — 15(3). — Режим доступу: http://www.globus.org/alliance/publications/papers/anatomy.pdf

182. *Bryan B.C.* ICSIS. The Intelligence Community System for Information Sharing / B.C. Bryan, T. Taylor, T. Minton // Military Communications Conference (MILCOM–2001), 28–31 oct. 2001. — http://www.milcom.org/2001/classified.htm

183. *Vickie R. Westmark.* A Definition for Information System Survivability / Proceedings of the 37th Hawaii International Conference on System Sciences — 2004. — http://www2.computer.org/portal/web/csdl/doi/10.1109/HICSS.2004.1265710

184. *Ellison R.J.* Survivable Network Systems: An Emerging Discipline / R.J. Ellison, D.A. Fisher, R.C. Linger H and Ind. // Survivable Systems Engineering project CMU/SEI-97-TR-013 ESC-TR-97-013: may, 1999. — Software Engineering Institute Carnegie Mellon University Pittsburgh. — www.cert.org/research/97tr013.pdf

185. *Додонов А.Г.* Введение в теорию живучести вычислительных систем / А.Г. Додонов, М.Г. Кузнецова, Е.С. Горбачик. — К.: Наук. думка, 1990. — 184 с.

186. *Stoneburner G.* Information System Security Engineering Principles — Initial Draft Outline [Електронний ресурс] / G. Stoneburner. — NIST, 2000. — Режим доступу: http://csrc.nist.gov/publications/drafts/epits-draft

187. *Survivable* Network Systems: An Emerging Discipline [Електронний ресурс] / J. Robert Ellison, David A. Fisher, Richard C. Linger and at. — Режим доступу: http://www.cert.org/research/97tr013.pdf

188. *Нестеренко О.В.* Концептуальна модель інформаційно-аналітичної системи органа державної влади / О.В. Нестеренко // Інформаційні техно-логії і системи. — 2003. — № 1–2. — С. 46–53.

189. *Мейор Т.* Методологии оценки ИТ [Електронний ресурс] / Трэйси Мейор // Директор ИС. — 2002. — № 9. — Режим доступу: http://www.osp.ru/cio/2002/09/172287

190. *Эффективность* внедрения ЭВМ на предприятии // Д.И. Агейкин, Э.Л. Ицкович, Ю.Л. Клоков и др. — М.: Финансы и статистика, 1981.

191. *Матвеев М.Т.* Эффективность АСУ / М.Т. Матвеев, А.А. Гаца, А.А. Якунин. — К.: Тэхника, 1989.

192. *Верников Г.* Основы систем класса MRP-MRPII / Г. Верников. — www.cfin.ru/vernikov

193. *Кинг Дэвид Р.* Продолжая начинания ERP / Дэвид Р Кинг. — http://www.citforum.ru/consulting/ERP/ERP_1/

194. *Руководство* по ГИС-анализу. Часть 1: Пространственные модели и взаимосвязи: пер. с англ. / [Andy Mitchell. ESRI Guide to GIS analysis. Vol. 1: Geographic Patterns&Relationships]. — К.: ECOMM, 2000. — 179 с.

195. *Интегрированное* управление производством*:* Организационные и технологические аспекты менеджмента предприятиями / В.И. Архангельский, И.И. Богаенко, Г.Г. Грабовский, Н.А. Рюмшин; [под. ред. В.И. Архангельского]. — К.: Техніка, 2005. — 328 с.

196. *Иванов П.* Управление информационными системами: базовые концепции и тенденции развития / П. Иванов // Открытые системы. — 1999. — № 4. — С. 37–43.

197. *Корнеев И.* Информационные технологии в управлении / И. Корнеев, В. Машурцев. — М.: Инфра-М, 2001. — 158 с.

198. *Волков И.* Архитектура современной информационноаналитической системы / И. Волков, И. Галахов. — http://www.citforum.ru/consulting/BI/ias/

199. *Еталонні* архітектури MSA / Майкрософт Україна. — К.: Видавнича група BHV, 2005. — 352 с.

200. *Колесников С.Н.* Как организовать проект внедрения / С.Н. Колесников. — http://www.citforum.ru/cfin/articles/organize.shtml

201. *Ермошкин Н.Н.* Стратегия информационных технологий предприятия: как Cisco Systems и ведущие компании мира используют Интернет решения для бизнеса / Н.Н. Ермошкин, А.А. Тарасов. — М.: Изд-во Московского гуманитарного университета, 2003. — 360 с.

202. *Нестеренко О.В.* Методологія використання сучасних інформаційних технологій в інформаційно-аналітичних системах органів державної влади / О.В. Нестеренко // Реєстрація, зберігання і оброб. даних. — 2004. — Т. 6, № 1. — С. 62–74.

203. *Петров В.В.* Національні інформаційні ресурси. Проблеми формування, розвитку, управління і використання / В.В. Петров, О.В. Нестеренко, М.Г. Монастирецький, В.Ю. Шагалов // Реєстрація, зберігання і оброб. даних. — 2001. — Т. 3, № 2. — С. 38–49.

204. *Нестеренко О.В.* Єдина державна система електронних інформаційних ресурсів / О.В. Нестеренко // Науково-технічна інформація. — 2003. — № 4. — С. 3–9.

205. *Додонов О.Г.* Формування, інтеграція та використання інформаційних ресурсів органів державної влади / О.Г. Додонов, О.В. Нестеренко, А.В. Бойченко, О.А. Бойченко // Реєстрація, зберігання і оброб. даних. — 2002. — Т. 4, № 3. — С. 69–75.

206. *Нестеренко О.В.* Реалізація шляхів доступу до системи електронних інформаційних ресурсів органів державної влади / О.В. Нестеренко // Науково-технічна інформація. — 2004. — № 3. — С. 3–10.

207. *Додонов О.Г.* Методологія створення Національного реєстру електронних інформаційних ресурсів / О.Г. Додонов, О.В. Нестеренко, А.В. Бойченко // Реєстрація, зберігання і оброб. даних. — 2005. — Т. 7, № 3. — С. 88–97.

208. *Willams B.* Document imaging in local government / B. Willams // Inf. Manag. and Technol. — 1994. — Vol. 27, N 6. — P. 241–245.

209. *Алишов Н.И.* Организация безопасности информационных ресурсов в корпоративных сетях компьютеров органов государственной власти / Н.И. Алишов, А.В. Нестеренко // Інформаційні технології та безпека. Зб. наук. пр. / НАН України; Ін-т проблем реєстрації інформації; [редкол.: Додонов О.Г. (голов.ред.) та ін.]. — К., 2002. — Вип. 1. — С. 9–17.

210. *Нестеренко О.В.* Геоінформаційні технології та інтеграція інформаційно-аналітичних систем органів державної влади України / О.В. Нестеренко // Вісник геодезії та картографії. — 2000. — № 2 (17). — С. 33–37.

211. *Жалковский Е.А.* Состояние и тенденции геоинформационного обеспечения органов государственной власти Российской Федерации / Е.А. Жалковский // Геодезия и картография. — 1998. — № 5. — С. 15–19.

212. *Нестеренко О.В.* Використання геоінформаційних технологій для забезпечення системи електронного уряду / О.В. Нестеренко // Ученые записки ТНУ. Серия: География; [редкол.: Н.В. Багров (голов.ред.) та ін.]. — Сімферополь, 2004. — Т. 17(56), № 2. — С. 99–104.

213. *Нестеренко О.В.* Геоінформаційне суспільство / О.В. Нестеренко // Ученые записки ТНУ. Серия: География; [редкол.: Н.В. Багров (голов.ред.) та ін.]. — Сімферополь, 2005. — Т. 18 (57), № 1. — С. 103–108.

214. *Тимкович Б.* Геоінформаційні системи і створення нормативно-правового поля для їх застосування у державному управлінні та місцевому самоврядуванні / Б.Тимкович // Вісник УДАУ. — 1998. — № 4/98. — С. 207.

215. *Баранов О.А.* Використання ГІС у проектах Національної прог-рами інформатизації України / О.А. Баранов, О.В. Нестеренко // Геоинформационные технологии в управлении территориальным развитием: IV междунар. конф., 28 мая – 1 июня 2001 г., К.: ECOMM. — 1 электрон. опт. диск (CD-ROM); 12 см.

216. *Круковський М.Ю.* Концепція побудови моделей композитного документообігу / М.Ю. Круковський // Мат. машини і системи. — 2004. — № 2. — С. 149–163.

217. *Кільчицкій Є.В.* Центральний засвідчувальний орган національної системи електронного цифрового підпису починає діяти! / Є.В. Кільчицкій, О.Л. Перевозчикова, Д.Ю. Савельєв // Зв'язок. — 2005. — № 5. — С. 18–21.

218. *Морозов А.А.* Базы знаний в системах ситуационного управления коллективного пользования / А.А. Морозов // УСиМ. — 1995. — № 4/5. — С. 1–5.

219. *Нестеренко О.В.* Використання Internet/Intranet-технологій в інформаційно-аналітичних системах органів державної влади / О.В. Нестеренко, Б.О. Березин // Вісник Державного університету інформаційно-комунікаційних технологій. — 2004. — 2, № 1. — С. 12–19.

220. *Business* Integration / Сторінка сайту корпорації Oracle. — http://www.oracle.com/technology/products/integration/index.html

221. *Современные* телекоммуникации. Технологии и экономика / В.Л. Банкет, О.В. Бондаренко, П.П. Воробиенко [та ін.]; общ. ред. С.А. Довгий. — М.: Эко-Трендз, 2003. — 319 с.

222. *Довгий С.О.* Стан та проблеми розвитку телекомукаційної мережі України: Розвиток телекомукаційної мережі в Україні та діяльність Укртеекому / С.О. Довгий // Наука та наукознавство. — 2000. — № 3. — С. 33–41.

223. *Широкополосные* мультисервисные сети — новая платформа телекоммуникационных магистралей и услуг: Аналит. обзор / [ред. В.В. Петров, ред. А.Е. Стрижак]. — К.: Нора-принт, 1999. — 134 с.

224. *Алішов Н.І.* Основні вимоги до телекомунікаційного середовища інформаційно-аналітичних систем органів державної влади / Н.І. Алішов, О.В. Нестеренко // Нові комп'ютерні засоби, обчислювальні машини та мережі. Зб. наук. пр.; НАН України; Ін-т кібернетики ім. В.М.Глушкова; Наук. рада НАН України з пробл. «Кібернетика»; [редкол.: В.О. Романов (відп.ред.) та ін.]. — Київ, 2001. — Т. 2. — С. 18–25.

225. *Олифер В.Г.* Новые технологии и оборудование IP-сетей / В.Г. Олифер, Н.А. Олифер. — СПб.: БХВ-Петербург, 2001. — 512 с.: ил.

226. *Дилип Н.* Стандарты и протоколы Интернета: пер. с англ. / Н. Дилип. — М.: Изд. отдел «Русская Редакция» ТОО «Channel Trading Ltd.», 1999. — 384 с.

227. *Дунаев С.Б.* Internet-технологии. WebDBC. CGI. CORBA 2.0. Netscape. Suite. Borland/InfraBuider. Java. JavaScript. Live Wire / С.Б. Дунаев. — М.: Диалог – МИФИ, 1997. — 288 с.

228. *Паркер Т.* Введение в TCP/IP (Internet в подинике) / Т. Паркер [под ред. М. Пайка]. — С.Пб.: Торг.-изд. бюро BHV, 1996. — 640 с.

229. *Построение* виртуальных частных сетей (VPN) на базе техно-логии MPLS. —Cisco Systems, 2001.

230. *Telecommunications* News / Информационный бюллетень СП «Инфоком». — 2001. — № 10; 2002. — № 11.

231. *Черников Ф.* Туннель для данных / Ф. Черников // Телеком. Коммуникации и сети. — 2002. — № 9.

232. *Шимми Бредли Ф.* Эффективное использование электронной почты: Ясные ответы на непростые вопросы: Передача файлов, безопасность, надежность обмена / Бредли Ф. Шимми. — Ростов н/Дону: Феникс, 1998. — 304 с.

233. *Робочий* проект багатотермінального комплексу на базі ОС Linux / Звіт про наук.-дослідну роботу. ВАТ «КП ОТІ». — 2002. — 12 с.

234. *Техніко-економічний* аналіз впровадження ОС Linux / Звіт про наук.-дослід. роботу. — К.: ВАТ «КП ОТІ». — 2002. — 13 с.

235. *Андон Ф.И.* Основы инженерии качества программных систем / Ф.И. Андон, Г.И. Коваль, Т.М. Коротун, В.Ю. Суслов; НАН Украины; Ин–т программных систем. — К.: Академпериодика, 2002. — 503 с.

236. *Нестеренко О.В.* Безпека інформаційно-аналітичних систем органів державної влади / О.В. Нестеренко // Інформаційні технології та безпека. Зб. наук. пр. / НАН України; Ін-т проблем реєстрації інформації; [редкол. О.Г. Додонов (голов.ред.) та ін.]. — Київ, 2003. — Вип. 5. — С. 37–44.

237. *Моделирование* безопасной обработки информации в компьютерных системах / А.М. Богданов, А.В. Корнейко, Г.С. Корхмазов [та ін.]; НАН Украины; Ин-т проблем моделирования в энергетике. — К.: Наук. думка, 2000. — 160 с.

238. *Домарев В.В.* Безопасность информационных технологий. Системный подход / В.В. Домарев. — К.; М.; СПб.: Торгово-изд. дом «DiaSoft», 2004. — 975 с.

239. *Мельников В.В.* Безопасность информации в автоматизированных системах / В.В. Мельников. — М.: Финансы и статистика, 2003. — 368 с.

240. *Зима В.М.* Безопасность глобальных сетевых технологий / В.М. Зима, А.А. Молдовян, Н.А. Молдовян. — Изд. 2-е. — СПб.: БХВ-Петербург, 2003. — 361 с.

241. *Безопасность* сети на основе Microsoft Windows 2000. Учебный курс MCSE: Официальное пособие Microsoft для самостоятельной подготовки: пер. с англ. — М.: Русская Редакция, 2001. — 912 с.

242. *Ярочкин В.И.* Информационная безопасность: Учебник для студентов вузов / В.И. Ярочкин. — М.: Академический Проект; фонд «Мир», 2003. — 640 с.

243. *Алишов Н.И.* Концепция создания высокоорганизованной системы безопасности информационных ресурсов в корпоративных сетях компьютеров органов государственной власти / Н.И. Алишов, А.В. Нестеренко // Актуальні проблеми економіки. — 2002. — № 9. — (Сучасні проблеми інформатики в управлінні, економіці, освіті: семінар, 8–13 лип. 2002 р.). — С. 5–11.

Наукове видання

Нестеренко Олександр Васильович

Безпека інформаційного простору державної влади Технологічні основи

Київ, Науково-виробниче підприємство
«Видавництво «Наукова думка» НАН України», 2009

Комп'ютерна верстка *М.Д.Рассоленко*

Підп. до друку 21.12.2009. Формат 60x84/16.
Гарнітура Futura Book. Папір офс. 1. Друк офс.
Обл.-вид. арк. 16,50. Ум.-друк. арк. 20,46.
Наклад 300 прим.

НВП «Видавництво «Наукова думка» НАН України»
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру — серія ДК № 2440 від 15.03.2006 р.
01601, Київ-1, вул. Терещенківська, 3

Видруковано у друкарні ТОВ «Інфодрук»
03113, м. Київ, вул. М. Шпака, 2