УДК 004.5

**Д. В. Ланде**
Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

# Методи підвищення живучості інформаційної складової корпоративних інформаційно-аналітичних систем підтримки прийняття рішень

*Розглянуто інформаційну компоненту корпоративної інформаційно-аналітичної системи підтримки прийняття рішень як змістовну складову її інформаційного забезпечення. Інформаційна складова відноситься до баз даних, інформаційних сховищ, інформаційних масивів, окремих документів, наведених у будь-яких можливих форматах. Наведено основні методи підвищення живучості інформаційної складової корпоративних інформаційно-аналітичних систем. Ці методи спрямовано на зменшення рівня вразливості цих систем у межах інформаційної інфраструктури.*

***Ключові слова:*** *живучість, інформаційна складова, інформаційно-аналітична система, інформаційна інфраструктура, інформаційна безпека.*

Поняття живучості інформаційної складової корпоративної інформаційно-аналітичної системи (КІАС) підтримки прийняття рішень відповідає її здатності своєчасно виконувати свої функції в умовах дії дестабілізуючих чинників (фізичне руйнування, часткова втрата ресурсів, відмови і збої елементів, несанкціоноване втручання в контур управління) [1]. При цьому живучість інформаційної складової має велике значення для живучості системи в цілому [2] її інформаційної безпеки. КІАС повинна містити такі засоби, які дозволили би певним чином відреагувати на виникнення ситуації, що призводить до погіршення якості інформаційної складової, і забезпечити збереження її функціональної спроможності.

Методи підвищення живучості інформаційної складової КІАС спрямовані на зменшення рівня її вразливості в мережах і системах інформаційної інфраструктури. Живучість інформаційної складової КІАС цілком відповідає новій мережецентричній (network-centric) [3] парадигмі інформаційної безпеки, яка як концептуальна схема (модель) постановки і вирішення проблеми витікає передусім з підвищених вимог до живучості інформаційних систем, які характеризуються висо-

кою мірою розподілу ресурсів (обслуговуванням, логікою, програмним і апаратним забезпеченням, телекомунікаціями) і майже повною відсутністю централізованого управління [4]. Поняття живучості включає поняття надійності, безпеки, відмовостійкості тощо. Тому методи забезпечення живучості КІАС включають до свого складу також методи забезпечення цих характеристик, але не обмежуються ними.

Складність надання інформаційній складовій КІАС властивості живучості пояснюється багато в чому ще і складністю процесів і, як наслідок, складністю інформаційно-аналітичних систем, які призначені для автоматизації цих процесів.

Забезпечення живучості доповнюється ще однією важливою властивістю — сучасна інформаційно-аналітична система може сама породжувати нові функції, які не були в неї закладені спочатку, а з'явились у результаті самонавчання.

Методи підвищення живучості складних систем можуть бути активними і пасивними відносно до зовнішніх шкідливих дій, що прикладені до системи. При активному методі відмови виявляються за допомогою засобів контролю, локалізуються діагностуванням й усуваються автоматичною реконфігурацією системи, яка полягає в перебудові структури системи з метою відключення вузлів, що відмовили. Пасивні методи засновані на функціональному резервуванні, при якому ті ж самі елементи за необхідності можуть виконувати різні функції у системі, а також резервування одних елементів іншими, в основу принципу дії яких покладені різні фізичні процеси. При цьому можливе погіршення показників якості функціонування системи.

Метою засобів забезпечення живучості інформаційної компоненти КІАС є захист інформації, що зберігається і оброблюється в системі, і забезпечення безпеки КІАС та її зовнішнього середовища при роботі з цією інформацією.

Інформаційна компонента КІАС — це змістовна складова її інформаційного забезпечення. Інформаційна складова відноситься до баз даних, інформаційних сховищ, інформаційних масивів, окремих документів, наведених у будь-яких можливих форматах. Живучість інформаційної складової має безпосереднє відношення до живучості інформаційного забезпечення, можливості його відновлення, виконання їм свого функціонального призначення у разі здійснення шкідливих впливів, як на інформаційне забезпечення, так і на всю КІАС взагалі.

Шкідливі впливи на інформаційну складову, як випадкові, так і навмисні, можуть бути двох типів — знищення елементів інформаційної складової та їхнього спотворення. Якщо знищення або спотворення метаданих в КІАС виправляється їх повторною генерацією, то знищення або спотворення первинних даних веде зазвичай до невиправних наслідків, якщо ця інформація не дублюється.

Уся інформація, що знаходиться в системі, може бути розділена на так звану «корисну» (знання, що отримуються, оброблюються і такі, що зберігаються в системі) і «технологічну» (інформація, що керує, внутрішні таблиці маршрутизації і тому подібне).

Методи та засоби забезпечення/підвищення живучості інформаційної складової необхідно застосовувати на всіх етапах її проходження в КІАС, а саме на етапах:

— генерування інформації;

— передачі інформації до КІАС;

— формування сховища інформаційних ресурсів КІАС (баз даних, інформаційних масивів, окремих документів тощо);

— безпосереднього використання інформаційної складової;

— утилізації (архівування) інформації.

Завдання із забезпечення живучості підрозділяються на дві групи:

1) запобігання виникненню нештатних ситуацій (тип 1);

2) забезпечення виходу з нештатних ситуацій (тип 2).

До першої групи відносяться завдання аналізу і, у разі потреби, корекції функціонування/використання інформаційної компоненти КІАС з метою забезпечення стабільної роботи. Друга група завдань — це забезпечення виходу з нештатної ситуації, якщо така все ж сталася, на основі методів реконфігурації, реконструкції, реорганізації і адаптації [5].

Нижче наведено основні методи, які застосовуються для підвищення живучості інформаційної складової КІАС.

1. Регулярна перебудова метаданих та індексів інформаційних ресурсів КІАС. Хешування інформаційних документів, зберігання хешів і їхня періодична перевірка.

У системі організації інформаційних ресурсів одним із ключових чинників є метадані (класифікації, переліки об’єктів, термінологічні словники, тезауруси, уніфіковані форми представлення даних, стандарти, патенти й інші форми нормативних і правових документів).

Переіндексування інформаційних ресурсів здійснюється для усунення помилок в індексах баз даних. Тому в багатьох корпоративних інформаційно-аналітичних системах передбачається проведення переіндексування баз даних у складі штатних регламентних робіт поряд з тестуванням, архівуванням, стискуванням даних тощо.

Для забезпечення живучості інформаційної складової корпоративної системи цей величезний масив метаданих необхідно підтримувати в актуалізованому стані, мати семантично еквівалентні переклади усіх задіяних видів документів державною мовою, здійснювати гармонізацію взаємопов’язаних документів і забезпечувати доступ користувачів до даної інформації.

2. Багатократне дублювання даних (реалізація надмірності даних). Надмірність вводиться штучно при проектуванні баз даних з метою підвищення надійності системи в умовах роботи зі збоями. При цьому передбачається регулярне здійснення реплікації дублюючих блоків інформації з перевіркою ідентичності.

Раніше вважалося, що надмірність даних необхідно обов’язково мінімізувати. З погляду живучості інформаційної складової КІАС, навпаки, надмірність несе ряд переваг. Так при застосуванні MySQL-серверів, підлеглий сервер (Slave-сервер) з визначеною періодичністю опитуватиме головний сервер (Master-сервер) на предмет змін у базі. Таким чином, усі зміни в master-сервері повторюватимуться на slave-сервері. Отже створюється надмірність даних на двох серверах і тим самим досягається висока доступність, надійність, живучість інформаційної складової.

3. Реалізація резервного та архівного копіювання інформаційних ресурсів КІАС. Резервне копіювання (англ. backup) — процес створення копії даних на но-

сії (жорсткому диску, флеш-пам'яті і т.д.), призначеному для відновлення даних в оригінальному місці їх розташування в разі їхнього пошкодження або руйнування, відповідними програмами — резервними дублікаторами даних. Резервне копіювання необхідне для можливості швидкого й недорогого відновлення інформації (документів, програм, налаштувань і т.д.) у разі втрати робочої копії інформації з будь якої причини. Крім цього вирішуються суміжні проблеми:

— дублювання даних;

— передача даних і робота із загальними документами.

Вимоги до системи резервного копіювання:

— надійність зберігання інформації — забезпечується застосуванням відмовостійкого обладнання систем зберігання, дублюванням інформації і заміною втраченої копії іншою у разі знищення однієї з копій (у тому числі як частина відмовостійкості);

— простота в експлуатації — автоматизація (за можливості мінімізувати участь людини: як користувача, так і адміністратора);

— швидке впровадження — прості установка і настроювання програм, швидке навчання користувачів.

Види резервного копіювання:

— повне резервування (Full backup) зазвичай зачіпає всю систему і всі файли. Щотижневе резервування повинне бути повним, як правило, виконується по п'ятницях або впродовж вихідних, коли копіюються всі бажані файли. Наступні резервування до наступного повного резервування, можуть бути додатковими або диференціальними, головним чином для того, щоб зберегти час і місце на носії. Повне резервування слід проводити, принаймні, щотижня;

— диференційне резервування (Differential backup) — кожен файл, який був змінений з моменту останнього повного резервування, копіюється щоразу заново. Диференціальне резервування прискорює процес відновлення. Все, що необхідно, це остання повна і остання диференціальна резервна копія. Популярність диференціального резервування росте, оскільки всі копії файлів робляться в певні моменти часу, що, наприклад, дуже важливо при зараженні вірусами;

— додаткове резервування (Incremental backup, інкрементальне) — здійнюється копіювання тільки тих файлів, які були змінені з тих пір, як в останній раз виконувалося повне або додаткове резервне копіювання. Подальше додаткове резервування додає тільки файли, які були змінені з моменту попереднього додаткового резервування. У середньому, додаткове резервування займає менше часу, оскільки копіюється меншу кількість файлів. Проте, процес відновлення даних займає більше часу, тому що повинні бути відновлені дані останнього повного резервування, плюс дані всіх наступних додаткових резервувань. При цьому, на відміну від диференціального резервування, файли, що змінилися або нові файли не заміщають старі, а додаються на носій незалежно;

— пофайловий метод резервування запитує кожен індивідуальний файл і записує його на носій. При цьому завжди слід використовувати опцію верифікації. При верифікації, все копійовані з диска дані перечитуються з джерела і перевіряються або побайтово порівнюються з даними на носії. Так як фрагментовані файли на диску через велику кількість виконуваних операцій пошуку уповільнюють

процес резервування, то продуктивність можна зазвичай збільшити здійснюючи регулярну дефрагментацію диска. При дефрагментації блоки даних розташовуються один за одним так, щоб вони були доступні в кеші попереднього читання;

— блочне інкрементальне копіювання (Block level incremental).

Для резервного копіювання дуже важливим питанням є вибір відповідної схеми ротації носіїв. Найчастіше використовують такі схеми:

— одноразове копіювання (custom) — найпростіша схема, що не передбачає ротації носіїв. Всі операції проводяться вручну. Перед копіюванням адміністратор задає час початку резервування, перераховує файлові системи або каталоги, які потрібно копіювати. Цю інформацію можна зберегти в базі, щоб її можна було використовувати знову. При одноразовому копіюванні найчастіше застосовується повне копіювання, проста ротація, ротація типу «дід, батько, син», «ханойська вежа», «10 наборів» тощо.

4. Застосування децентралізованих систем зберігання інформації поряд із дублюванням критичних блоків інформації передбачає надлишкове дублювання інформаційних ресурсів. Децентралізоване зберігання даних потребує встановлення компонент системи в кожній частині корпорації: головному офісі, філіях, окремих установах тощо. Децентралізація у цих випадках підвищує живучість при реалізації надмірності даних, але суттєво збільшує терміни введення системи та проведення доопрацювань (оновлень) у майбутньому;

5. Резервне дублювання не тільки інформації, але й цілих апаратно-програмних комплексів. Так у багатьох сучасних КІАС (наприклад, у системі Quest InTrust, виробник Quest Software, яка призначена для аналізу дій користувачів і підтримки відповідності корпоративній політиці безпеки) передбачено автоматине резервне дублювання сервера, що відмовив. Це дозволяє оперативно і в автоматичному режимі перемістити всі налаштування та завдання з сервера, що відмовив, на резервний, який потім приймає на себе функції того, що відмовив. Ця функція знижує ризик утрати системних журналів при відмові сервера.

6. Застосування сертифікованого антивірусного захисту. Оцінювання вхідної інформації повинно здійснюватися на базі внутрішньої адміністративної політики КІАС, сигнатур шкідливого програмного забезпечення, шаблонів поведінки шкідливого програмного забезпечення і т.п. Наприклад, аналізуючи існуючий у Міністерстві оборони США порядок організації антивірусного захисту, можна виділити декілька ключових моментів:

— для антивірусного захисту використовуються програми декількох провідних національних розробників у галузі захисту від шкідливих програм;

— тестується кожна нова версія антивірусних програм на сумісність і безпомилковість;

— оперативне постачання нових версій та оновлень антивірусних програм здійснюється з надійних джерел;

— антивірусні програми регулярно (щодобово або щотижнево) оновлюються з надійних джерел;

— існують конкретні та однозначні нормативні вимоги до налаштувань антивірусів;

— здійснюється оперативне реагування на всі випадки виявлення комп'ютерних вірусів.

Цей ефективний порядок організації антивірусного захисту може застосовуватися при побудові систем антивірусного захисту КІАС міністерств, відомств і великих компаній, банків тощо.

7. Застосування засобів електронного цифрового підпису, хешування даних (як засіб проти спотворення даних). Найбільш простий спосіб перевірки цілісності даних, які передаються в цифровому представленні, — це метод контрольних сум. Недолік цього методу полягає в тому, що хоча розбіжність значень цих сум служить вірним доказом, що даний документ зазнав зміни, рівність порівнюваних значень ще не дає гарантії, що інформація залишилася незмінною. Більш досконалий спосіб цифрової ідентифікації деякої послідовності даних — це обчислення контрольного значення її циклічного надмірного коду (cyclic redundancy check — CRC). Більш високу надійність, ніж при контролі CRC, можна досягти при використанні односторонніх алгоритмів хешування; результатом їхньої роботи є особливі значення хешу. Серед односторонніх алгоритмів хешування найбільшою популярністю користуються два з них: алгоритм MD5 (message digest) і алгоритм Secure Hash Algorithm (SHA). Результат аналізу послідовності вхідних даних за допомогою алгоритму MD5 — 128-розрядний цифровий ідентифікатор, а при використанні алгоритму SHA — 160-розрядне значення. Якщо використовувати алгоритми хешування разом з криптосистемами з ключем загального користування, то можна створити цифровий підпис, що гарантує справжність отриманого набору даних, аналогічно тому, як рукописний підпис, підтверджує автентичність надрукованого документа. Для забезпечення живучості КІАС має здійснюватися зберігання критичної інформації в закодованому вигляді, застосування електронних цифрових підписів. Таким чином, системи забезпечення живучості інформаційної складової КІАС мають забезпечувати контроль хешових значень та електронних цифрових підписів як документів, так і окремих програмних модулів.

8. Постійна перевірка валідності джерел інформації. Обґрунтованість (валідність) інформації визначається перед усім характеристиками методу дослідження, що застосовується, та полягає у його здібності вимірювати саме ті властивості об’єкта досліджень, які цікавлять дослідника. При цьому валідність джерел не може досягатися за рахунок достовірності (надійності) джерел інформації. Дієвим методом при цьому є створення засобів цензурування інформації, що потрапляє до зовнішнього інформаційного середовища. Причому правила цензурування повинні постійно доповнюватися на основі реакції зовнішнього середовища на вихідну інформацію. Таким чином, здійснюється фільтрація інформації, що входить, з метою відсіювання інформації, що не задовольняє вимогам інтерфейсу (ця інформація накопичується для подальшого аналізу).

9. Видалення (архівування) зайвої, непотрібної інформації, інформаційного шуму з КІАС. Інформаційний шум — це непотрібна, несвоєчасна інформація, що заважає споживачеві сприймати іншу, яка відповідає його запитам. Інформаційний шум може бути ненавмисним (фактичні, технічні, механічні, помилки тощо) та навмисним (пропаганда, дезінформація тощо). Для забезпечення живучості інформаційної компоненти КІАС необхідно усунути інформаційне забруднення електронної інформації (спам, миттєві повідомлення, небажаний контент вебсайтів).

10. При здійсненні процедур обробки даних з можливою втратою інформації (автоматичне реферування, переклад, JPEG-перетворення зображень) необхідно зберігати першоджерела документів у інформаційному сховищі (депозитарії). Зберігати інформацію в різних форматах: як у внутрішньому системному, так і зовнішньому вихідному. На цей час існує багато програмних систем (наприклад, Navicat), які застосовуються для одночасного підключення до декількох баз даних у різних форматах, що реалізують надійне та зручне керування базами даних MySQL, Oracle, PostgreSQL, SQLite і SQL Server. Необхідно забезпечувати супроводження аналітично узагальнюючих документів першоджерелами з метою автоматизованої або автоматичної перевірки достовірності.

11. Забезпечення доступу аналітиків (аналітичних програмних модулів) до будь-якого фрагмента інформаційного репозитарію КІАС з метою оперативного виявлення впливу на інформаційну складову, здійснення регулярного цілеспрямованого аналізу, контролю і коригування стану програмного та інформаційного забезпечень КІАС. Організація розподіленої бази даних КІАС надає такі переваги: зменшується час відгуку системи, підвищується надійність зберігання даних, зменшується вартість апаратної частини за рахунок зниження обсягів даних, які зберігаються на одному сервері. Ефективність такої інформаційної системи безпосередньо залежить від можливостей доступу аналітиків до інформаційної складової: чим він більш ефективний, тим швидше окупаються кошти, що вкладені в його побудову. Ключем до успішної реалізації інформаційної складової КІАС є оптимальна організація розподілу та зберігання інформації.

12. Ранжирування інформації. Інформація, що зберігається в КІАС, має бути ранжирувана за ступенем важливості, рівнем конфіденційності та приналежності підрозділам корпорації. До умов зберігання та обробки найбільш важливої інформації мають бути пред'явлені особливі вимоги. Крім того, інформація може бути ранжирувана за максимальним часом доступу до неї в різних ситуаціях; необхідно виділити деяку множину критичної інформації, яка має бути доступна в будь-якій ситуації. Для іншої інформації необхідно задати максимальний час доступу, який може залежати від поточної ситуації (штатна, нештатна і т.п.) виділення зв'язків між даними дозволить сформувати вимоги до зберігання різних блоків інформації, запобігти можливим «непрямим» утратам інформації, виробити раціональний підхід до внесення надмірності при зберіганні даних у КІАС.

13. Розподіл прав доступу до інформації. Реалізація визнаних політик безпеки. Політика безпеки — це організаційно-правовий та технічний документ одночасно. При її складанні треба завжди спиратися на принцип розумної достатності. Значну увагу в політиці безпеки приділяється питанням забезпечення безпеки інформації при її обробці в автоматизованих системах: автономно працюючих комп'ютерах і локальних мережах. Необхідно встановити, як повинні бути захищені сервери, маршрутизатори та інші пристрої мережі, порядок використання змінних носіїв інформації, їхнє маркування, зберігання, порядок внесення змін до програмного забезпечення. При спільній роботі користувачів у КІАС необхідний поділ їхніх прав доступу відповідно до повноважень, а також аудит подій доступу до системи.

14. Фільтрація вихідної інформації, яка поступає з КІАС безпосередньо для прийняття рішень шляхом цензурування з метою відсіювання несприятливої для

зовнішнього світу інформації. Поряд з вимогами до кількості і якості одержуваної інформації не менше значення мають її склад і показність. Надмірність інформації інколи настільки ж шкідлива, як і її недостатність. Ще більш важливо володіти потрібною інформацією, що безпосередньо відноситься до справи, до досліджуваної проблеми; таку інформацію в теорії управління називають релевантною. Для отримання релевантної інформації доводиться вдаватися до процесів фільтрації всіх отриманих даних на предмет відбору тільки тих, які безпосередньо пов'язані з виникненням і суттю аналізованої проблеми.

15. Розподіл частин КІАС («відкритої», корпоративної тощо) можливо реалізувати на різних рівнях (паролі, файрволи, фізичне роз'єднання). Типова КІАС може ґрунтуватися на трирівневій моделі:

— відкрита частина або презентаційний рівень, що забезпечує інтерфейси, необхідні для управління і настроювання інформаційних розділів і сервісів КІАС. Структура інформаційних розділів повинна ґрунтуватися на специфіці використання інформаційних матеріалів у корпорації;

— закрита частина КІАС або рівень бізнес-логіки, що містить програмні об'єкти та програмний код, який реалізує логіку роботи систем, і модулі, що реалізують інформаційні та інтерактивні сервіси. Закрита частина повинна регулюватися на рівні прав доступу до розділів підсистем і модулів КІАС для кожного з адміністраторів;

— рівень зберігання даних КІАС, що включає в себе СУБД і компоненти для доступу до даних. Для зберігання інформації повинна використовуватися файлова система і СУБД.

16. Обмеження доступу до інформації. Цей метод припускає наявність розвиненого периметра безпеки, що має як централізоване, так і децентралізоване керування, який був би в змозі оцінювати вхідну інформацію («службову» і «корисну»), і виключати інформацію небезпечного змісту. При цьому повне обмеження доступу до інформації передбачає неможливість отримання всієї інформації користувачами, для яких явно не встановлено відповідний дозвіл. Часткове обмеження доступу до інформації передбачає обмеження доступу на читання та/або зміну частини властивостей інформації користувачами, для яких явно не встановлено відповідний дозвіл.

17. Протоколювання подій у системі, ведення системних журналів з метою виявлення можливих фрагментів даних, які зазнали втручання. Аналіз, контроль і коригування стану КІАС з погляду можливого відхилення від штатного режиму функціонування за різними напрямами, у тому числі за журналами подій, що сталися в КІАС, протоколами роботи програмного забезпечення; статистикою завантаження каналів зв'язку, завантаження та збоїв апаратного забезпечення. При цьому необхідно визначити і активізувати наявні в додатках і операційних системах механізми протоколювання скрізь, де це необхідно, а також протоколювати «необхідний мінімум» подій, а саме:

— активізувати базові журнали безпеки;

— активізувати протоколювання подій мережі;

— протоколювати випадки невдалої автентифікації;

— протоколювати порушення доступу;

— протоколювати спроби імплантації вірусів або іншого «недружнього» коду;

— протоколювати будь-які нестандартні дії/події. Наприклад, великі скачки в трафіку можуть бути як свідченням атаки, так і ознакою дуже успішної маркетингової кампанії (приміром, якщо в десять разів піднялася відвідуваність).

18. Забезпечення працездатності апаратних засобів, коректне відключення носіїв даних при зупинці системи, окремих блоків і модулів. Обслуговування програмного забезпечення, баз даних і технічної підтримки обладнання спеціалізованих інформаційних комплексів і технологій. Використання надійної системи енергопостачання, що забезпечує безперебійне енергопостачання апаратних засобів інформаційної системи, взаємодіючих систем і мереж зв'язку відповідно до документів, що регламентують режим умови їхньої експлуатації.

19. Зберігання в системі різних версій програм обробки/візуалізації, що допоможе запобігти помилок при реалізації принципу «наслідування». Іноді оновлення продуктів породжують різного роду технічні проблеми, і буває доцільним відкотитися на попередню версію програми, яку розробники, як правило, дбайливо прибирають з сайту. Сучасні сховища програм дозволяють зберігати всі програми в одному місці, з якого і відбувається їхній запуск. Сховище спрощує процедуру адміністрування версій програм, поділу прав на запуск, відстеження змін, спрощує настройку робочих станцій користувачів і зменшує розмір базового образу операційної системи.

20. Наявність конверторів форматів даних і підсистем інтеграції ПЗ (підсистеми імпорту, експорту і синхронізації даних між різними додатками) для забезпечення використання вихідних даних у різних форматах. Конвертори даних відповідають за перетворення файлів різної структури (текстові, бінарні) в універсальні формати для подальшого завантаження даних у бази даних.

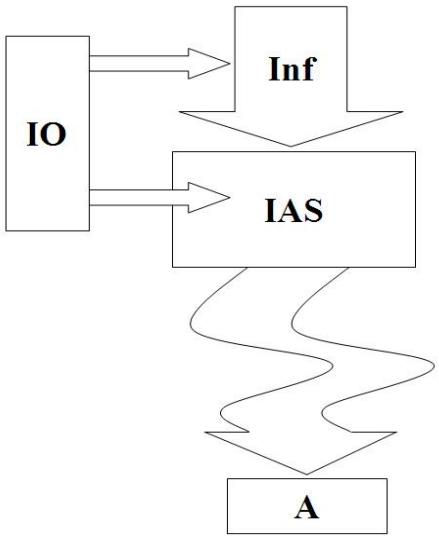
21. Застосування засобів термінового зберігання критично важливих документів, доступних у режимі «тільки читання», резервне зберігання інформації на знімних носіях, розміщення у захищених приміщеннях. Задовольнити новим вимогам можна, використовуючи декілька підходів. Виробники реляційних СУБД сьогодні розширюють функціональність своїх продуктів за рахунок додавання спеціального індексування, що орієнтоване на режим read-only.

22. Зберігання історії (версій) інформаційних документів. Майже всі сучасні документальні сховища підтримують версіонність інформаційних документів. Крім того, між документами формуються взаємозв'язки, які можуть бути класифіковані.

23. Використання надійних каналів передачі вхідних даних. Безпека має забезпечуватися шифруванням трафіка між серверами додатків і клієнтами. Використання декількох каналів інформації з подальшим порівнянням при занесенні в інформаційне сховище (реплікації).

24. Застосування систем виявлення зовнішнього впливу (вторгнення), за допомогою яких можна зафіксувати факт атак на інформаційну інфраструктуру, оцінити можливі збитки й виконати адекватні дії у відповідь. При цьому зовнішні впливи на інформаційну складову нині прийнято вважати інформаційними операціями [6], відповідно для забезпечення її живучості необхідно застосовувати методи моніторингу та протидії інформаційним операціям. Інформаційні операції по

боротьбі з системами контролю та керування КІАС стали дуже істотними елементами ведення різного роду протиборств (бізнесового, політичного, релігійного тощо). Особливою метою при здійсненні інформаційних операцій є інформаційно-аналітичні системи підтримки прийняття рішень суб'єкта впливу [7, 8]. Здійснюючи вплив на такі системи, можна домогтися того, що особи з табору супротивника, які приймають рішення, зроблять неадекватні висновки, і необхідний бізнес-процес змінить траєкторію в напрямку, необхідному для сторони, що впливає (див. рисунок).




Вплив на інформаційно-аналітичну систему супротивника: Inf — інформаційний простір; IAS — інформаційно-аналітична система; A — абонент системи (особа, що приймає рішення); IO — інформаційні впливи

У процесі зростання масштаби інфраструктури, кількість інформаційних процесів і складність взаємозв'язків інколи перевищують рубіж, коли можливо контролювати всю інфраструктуру, бачити взаємозв'язки бізнес-процесів і роль елементів інфраструктури в кожному процесі, внаслідок чого:

— знижується рівень готовності усієї інформаційної інфраструктури;

— знижується якість обслуговування, яку, крім того, важко оцінювати;

— при змінах процесів виникають нові проблеми в інфраструктурі;

— збільшується питома вартість володіння інфраструктурою;

— виникають труднощі в плануванні розвитку всієї інфраструктури.

Інформація, що може використовуватися для підтримки прийняття рішень, розглядається вже на новому рівні — як аналітична інформація. Базою для створення аналітичної інформації є інформаційні потоки, а також спеціальні нормативно-довідкові бази даних. Ця інформація обробляється аналітиками, які й готують аналітичну інформацію (проекти рішень, довідки, прогнози тощо) для осіб, що приймають рішення.

Забезпечення живучості аналітичної складової охоплює усі ланки процесу створення та використання аналітичної інформації, а саме:

— отримання аналітиками вихідної інформації;

— аналіз інформації за визначеною проблемою, що зібрана;

— обробка інформації;

— підготовка документів (аналітичних звітів);

— верифікація аналітичної інформації;

— використання аналітичної інформації.

Відповідно до цього, забезпечення живучості аналітичної складової включає забезпечення живучості окремих ланок, а саме:

— вхідних інформаційних потоків і баз даних, що досягається використанням різних каналів надходження інформації, поступовим збільшенням кількості джерел інформації в аналітичній системі, захистом, резервним копіюванням і дублюванням баз даних, які використовуються для створення аналітичної інформації;

— програмного забезпечення, яке застосовується аналітичною службою. Рекомендується використовувати програмне забезпечення декількох (бажано конкуруючих) виробників, наприклад, систем контент-моніторингу InfoStream поряд із системою Integrum; систем рівня глибинного аналізу текстової інформації Галактика Zoom поряд із системою PolyAnalyst; захист програмного забезпечення;

— людського фактору — залучення колективу взаємозамінних фахівців-аналітиків;

— аналітичної інформації, що створюється аналітичними підрозділами та надається особам, що приймають рішення — верифікація інформації різними фахівцями, використання захищених каналів зв'язку, корпоративних мереж без підключення (з обмеженим підключенням) до Інтернету, протоколювання дій з аналітичною інформацією, резервне копіювання, архівування аналітичної інформації.

1. *Survivable* Network Systems: An Emerging Discipline CMU/SEI-97-TR-013 ESC-TR-97-013 Software Engineering Institute Carnegie Mellon University Pittsburgh. — May 1999.

2. *On the* Definition of Survivability. — Department of Computer Science University of Virginia. — June 2001.

3. *Defense-in-Depth* Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations. — MILCOM-2001.

4. *Proceedings* of the DARPA Information Survivability Conf. and Exposition (DISCEX'2000). — Hilton Head Island, South Carolina. — January 25–27, 2000.

5. *Додонов А.Г.* Корпоративные информационные системы: обеспечение живучести / А.Г. Додонов, Д.В. Флейтман // Математичні машини і системи. — 2005, № 4. — С. 119–130.

6. *Горбулін В.П.* Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. — К.: Інтертехнологія, 2009. — 164 с.

7. *Burke M.M.* Knowledge Operations: Above and Beyond Information Operations. 6-th Internation. Command and Control Research and Technology. — June 19–21, 2001.

8. *Lasswell H.D.* The Structure and Function of Communication in Society / H.D. Lasswell // The Communication of Ideas / Ed.: L. Bryson. — New York: Harper and Brothers, 1948.

Надійшла до редакції 29.04.2012