УДК 004.342.75
В. В. КОЗЛОВСЬКИЙ, доктор техн. наук, професор;
А. В. МІЩЕНКО, канд. техн. наук, професор;
О. І. ВАРЧЕНКО, доцент;
Г. С. ЛЕВІНСОН, студент,
Національний авіаційний університет, Київ

Метод оперативного управління комплексною системою захисту інформації авіатранспортного комплексу

Розглянуто метод оперативного управління комплексною системою захисту інформації авіатранспортного комплексу, що відрізняється від відомих економічно обґрунтованим підходом до розв'язання оптимізаційних задач розміщення та управління ресурсами.

Ключові слова: інформаційна безпека; авіатранспортний комплекс; авіатранспортна інфраструктура; комплексні системи зв'язку; захищеність інформаційних систем.

Вступ

В авіатранспортному комплексі (АТК) України ще й досі функціонують аналогові вузли спецслужб захисту інформації, які виробили свій ресурс і найближчим часом мають бути демонтовані. Новітня цифрова комутаційна техніка і комп'ютерні технології дозволяють значно розширити можливості вузлів, упровадити на локальних телефонних мережах інтелектуальні послуги й організувати додаткові служби — довідкові, інформаційні й замовні, зробивши їх більш привабливими для користувачів і більш надійними з погляду інформаційної безпеки. Зрештою цифрові вузли зазначених спецслужб в авіатранспортній сфері стануть міцним фундаментом в забезпеченні інформаційної безпеки АТК.

Основна частина

Фундамент оперативного управління комплексною системою захисту інформації в АТК складається з двох компонентів: *інформаційного* та *програмного*.

Інформаційне забезпечення як найважливіший компонент Центру обробки викликів (ЦОВ), або Call Center, має реалізовуватися у вигляді відповідних баз даних (БД) сучасної архітектури. Більшість ЦОВ використовують архітектуру реляційних БД.

При створенні та експлуатації інформаційного забезпечення необхідно:

- вибрати систему керування базою даних (СКБД) і програмно-апаратну платформу для її розгортання;
- розробити і створити БД;
- виконати адміністрування БД;
- здійснити первісне введення інформації з неелектронних носіїв;
- конвертувати отриманий масив даних у структури відповідної БД;
- оперативно коригувати зміст БД для підтримки актуальності збереженої інформації;
- організувати доступ до запису нової та читання і зміни збереженої інформації.

При виборі СКБД варто враховувати:

- вид служби, для якої створюється БД, і кількість робочих місць (РМ) у ній;
- структуру (локальна чи розподілена) створюваної мережі;
- зміст інформації, яку передбачається зберігати;
- показники вартості;
- необхідну продуктивність, час відповіді системи на еталонне запитання;
- вимоги щодо надійності.

Для невеликих локальних мереж можна рекомендувати MS SQL Server у середовищі OS Windows XP Professional, а для більших мереж є сенс застосувати Oracle у середовищі OS Windows XP Professional чи в середовищі OS Unix. Для розподілених мереж можливе застосування DB2 у середовищі OS Windows XP Professional чи в середовищі OS Unix. Остаточний вибір варіанта реалізації СКБД має відбуватися на стадії проектування конкретного ЦОВ.

При розробці та створенні БД необхідно проаналізувати зміст інформації, яку передбачається зберігати (інформація предметної області, довідкова інформація, описи абонентів і т. д.). На підставі такого аналізу варто розробити:

- схему БД з урахуванням усіх збережених сутностей і їхніх взаємозв'язків;
- індекси для пошуку інформації зі змісту;
- екранні подання та форми;
- збережені процедури та тригери;
- процедури резервного копіювання та відновлення;
- процедури архівування;
- різні SQL-сценарії для взаємодії з БД (запити, адміністрування, збір статистики тощо);
- групи користувачів;
- заходи із забезпечення безпеки через надання різним групам користувачів різних прав доступу до БД.

Для нормального функціонування створеної БД необхідне постійне адміністрування та розв'язання низки завдань:

- створення облікових записів користувачів і керування ними;
- визначення ролей, сервісних правил, прав доступу;
- забезпечення захисту даних у мережі;
- навчання та підтримка користувачів;
- модернізація існуючого програмного забезпечення (ПЗ) та встановлення нового;
- архівування даних;
- імпорт і експорт даних;
- запобігання втратам даних;
- моніторинг вільного простору для збереження даних на сервері;

- настроювання продуктивності та її оптимізація;
- протоколювання БД;
- резервне копіювання даних;
- відновлення даних після аварії;
- захист мережі від вірусів;
- діагностика;
- модернізація та заміна компонентів мережі;
- додавання в мережу нових робочих станцій.

Для первісного введення інформації з неелектронних носіїв має бути передбачено сучасні системи оптичного розпізнавання тексту (OCR).

Отриману в електронному вигляді вихідну інформацію потрібно перетворити в структури обраної БД. Для цього необхідна розробка відповідного ПЗ, що враховує предметну область БД. Сформована БД має бути перевірена на несуперечливість програмним способом. Відповідну програму також слід розробити.

Для пошуку інформації зі змістом необхідно створити повнотекстовий індекс — алфавітний покажчик слів, що трапляються в тексті. Для роботи з документами російською або українською мовою має бути спеціально адаптований сервіс повнотекстового індексу англомовної універсальної СКБД. Важливим для ефективної роботи пошукової системи є створення словника стопслів. Це особливий список слів російської або української мови, що не несуть самостійного змістового навантаження (прийменники, сполучники, займенники тощо). Наявність ієрархічного словника синонімів дозволить створити складні запити на основі синонімів і родовидових зв'язків.

Для підтримання інформації БД в актуальному стані її слід постійно коригувати. Внесення коректур у БД може здійснюватись:

- операторами служби (локально чи дистанційно);
- власником інформації (локально чи дистанційно);
- автоматично програмним забезпеченням ЦОВ на підставі аналізу зовнішніх джерел інформації;
- комбінованим способом, що охоплює перелічені прийоми.

Для коригування необхідна розробка спеціального ПЗ, що дозволяє конкретному користувачеві змінювати інформацію БД тільки згідно з його повноваженнями та за допомогою індивідуальних (для класу користувачів) зручних прийомів.

Доступ до інформації БД повинні мати системи інтерактивної мовної відповіді IVR, оператори, начальник зміни, адміністратор служби, адміністратор ЦОВ. Для роботи оператора необхідно розробити зручні екранні форми, що уможливлюють видачу запитів до БД і відображення на екрані отриманої інформації. Має також передбачатися можливість вилученого доступу до БД.

Програмне забезпечення разом з апаратними засобами має задовольняти функціональні вимоги, які висуваються до ЦОВ у чинних технічних вимогах, з урахуванням загальних вимог.

Програмне забезпечення ЦОВ має містити такі компоненти прикладного і сервісного ПЗ:

- програмне забезпечення для керування системою ACD;
- програмне забезпечення для керування системою IVR;
- інформаційне ПЗ;
- програмне забезпечення системи контролю і реєстрації;
- програмні засоби розробки додатків.

Програмне забезпечення для керування системою ACD призначено для спостереження за її роботою, оскільки сама система лише керує розподілом викликів між операторами за встановленими правилами і не показує, як вона функціонує.

Така ПЗ має:

- видавати звіти про якість обслуговування викликів, що надходять, і про роботу операторів у реальному масштабі часу і за задані проміжки часу;
- мати модульну структуру і дозволяти швидке нарощування системи ACD;
- інтегруватися з іншими додатками (облік викликів, розподіл витрат, визначення послідовності робіт і т. ін.);
- забезпечувати гнучкість системи, підтримуючи важливі для користувача параметри.

Інформаційне програмне забезпечення призначене для одержання з інформаційного сховища ЦОВ (ClCn) даних, необхідних для обслуговування абонента. Воно повинне включати мережну інформаційну базу даних (NID) і сервісні логічні програми (SLP), що відповідають за виконання різних видів обслуговування. Інформаційна база даних повинна містити параметри маршрутів установлення з'єднання, історію звертань кожного абонента (при необхідності), довідкову інформацію, статистичну інформацію про роботу ЦОВ.

Інформаційне ПЗ разом із системою IVR має брати участь в інтелектуальному керуванні потоком вхідних викликів. За запитом IVR воно має підготувати набір відомостей із БД ЦОВ, на підставі яких на екран оператора буде виводитися попередня інформація про виклик, що надійшов, і сценарій його обслуговування.

До комплекту ПЗ ЦОВ мають входити програмні засоби розробки додатків, що забезпечують функціональну розширюваність наданих програмних продуктів. Має бути можливість доробки і модифікації готового ПЗ силами персоналу ЦОВ. Оператор чи адміністратор повинні мати можливість самостійно змінювати правила керування обробкою викликів з урахуванням зміни специфіки чи особливостей ЦОВ.

При спілкуванні оператора з абонентом основні складові комплекту ПЗ ЦОВ реалізують усі необхідні функції через інтерфейс оператора. Засоби розробки додатків мають слугувати саме для модифікації інтерфейсу та адаптації його до конкретних вимог. Використовуються такі стандарти розробки додатків: Java, Active, DCOM, TAPI. Застосовуючи кожний із цих механізмів, можна створювати власні додатки для використання в різних службах сервісу і з будь-якою інформацією з БД.

Мультимедійний центр обслуговування абонентів (ММ ЦОА), або Contact Center, — це сукупність апаратно-програмних засобів, інформаційних баз, операторських ресурсів і систем доступу, призначена:

- для прийому й обробки вхідних звернень абонентів до ресурсів ЦОА;
- для генерації вихідних звернень ЦОА до абонентів за списками, заздалегідь підготовленими чи створюваними відповідно до заданого алгоритму.

Обмін повідомленнями між абонентами і ЦОА має здійснюватися через телефонну мережу (мовні і факсимільні повідомлення) і через інтернет (текстові повідомлення чат, текстові, мовні і музичні повідомлення електронної пошти, мовні повідомлення IP-телефонії). На базі інтегрованого прикладного середовища ЦОА має відбуватися керування всіма видами електронної взаємодії з абонентами по телефонній мережі і через інтернет.

Центр обслуговування абонентів має підтримувати стандартні протоколи взаємодії з телефонними мережами загального користування, цифровою мережею з інтеграцією послуг (ISDN), інтелектуальною мережею (IN), мережею мобільного зв'язку (MN) і мережею Інтернет (IP-телефонія, електронна пошта, чат).

Мультимедійний центр обслуговування абонентів порівняно з центром обслуговування викликів має додатково підтримувати такі технології спілкування з абонентами:

- інтернет-взаємодію, що дозволяє оператору та абоненту автоматично синхронізувати свої браузери й одночасно переміщувати по інтернет-сторінках телефонної компанії. При цьому оператор може допомогти абоненту знайти необхідну інформацію і навчити користуватися можливостями інтернет-сайту;
- голосовий зв'язок по IP-мережі, який дозволяє відвідувачу інтернет-сайту телефонної компанії поговорити з оператором безпосередньо зі свого ПК за допомогою стандартних програмних засобів IP-телефонії;
- електронну пошту, що дозволяє абоненту відправляти й одержувати з ЦОА текстові, мовні й музичні повідомлення, тоді як ЦОА має автоматично відповідати на пошту, котра прибуває, чи пропонувати оператору практично готові відповіді;
- інтерактивний текстовий зв'язок, який дозволяє абоненту, що відвідав інтернет сайт телефонної компанії, набрати на екрані питання і відразу одержати на нього текстову відповідь оператора ЦОА;
- факсимільний зв'язок, що повинен мати можливість перетворення вхідних і вихідних факсимільних повідомлень у повідомлення електронної пошти та автоматичної відповіді на факси за правилами, встановленими для електронної пошти;
- доступ через мобільні мережі до всіх послуг ЦОА з мобільного телефону на основі стандартних протоколів передавання даних WAP і служби коротких повідомлень SMS;
- обробка паперових документів із можливістю сканування документів на паперових носіях, отриманих від абонентів, і розпізнавання інформації, що міститься в них. Після перетворення в електронний формат документи можуть передаватися подібно до звичайної електронної пошти для підготовки відповіді абоненту і вжиття відповідних заходів.

Наведений перелік послуг має бути доповнений розглянутими далі послугами, наданими абонентам ММ ЦОА за допомогою мережі Інтернет.

♦ Послуга ***електронної пошти*** забезпечує прийом повідомлень електронної пошти на загальну адресу і маршрутизацію повідомлення на оператора відповідного рівня кваліфікації, що звільнився першим. Для відповіді оператор може скористатися одним зі стандартних, заздалегідь підготовлених текстових, мовних чи музичних повідомлень або скласти свій варіант повідомлення. Центр повинен мати набір інструментальних засобів обробки вхідних повідомлень електронної пошти, включаючи їхню маршрутизацію і контроль поштових скриньок, що використовують різні системи електронної пошти: Microsoft Exchange, Lotus Notes, Novell GroupWise, iPlanet Messaging Server і т. ін.

♦ Послуга ***IP-телефонії*** дозволяє передавання мови по IP-мережах, включаючи мережу Інтернет. При перегляді інтернет-сайту телефонної компанії абонент повинен мати можливість викликати оператора щигликом миші по кнопці «Телефонуйте нам». На ПК абонента має завантажитися спеціальне прикладне ПЗ «контроль виклику», написане мовою Java, і засвітитися вікно «контроль виклику». Абонент отримує можливість стежити за ходом установлення з'єднання, а також доступ до таких функцій, як «текстовий чат», «напрямлений перегляд» і «спільне заповнення HTML форм». Виклик, що надійшов у ЦОА, залежно від оперативної обстановки має бути спрямований до першого вільного оператора відповідного рівня кваліфікації, на автоінформатор чи поставлений у чергу.

При надходженні виклику на термінал оператора на дисплеї в нього має засвітитися інтернет-сторінка, з якої прийшов запит. Під час сеансу зв'язку оператор і абонент можуть синхронно переглядати ті самі сторінки. При перегляді різних сторінок можна натиснути кнопку «переслати сторінку» (функція «напрямлений перегляд») і сторінки на екранах стануть ідентичними.

♦ Послуга ***«текстовий чат»*** надає абоненту можливість текстової бесіди з оператором ЦОА при перегляді інтернет-сайту телефонної компанії. Це зручно для абонентів, що не мають програмно-апаратного забезпечення для мовних переговорів через інтернет. Текстовий діалог, як і мовний, забезпечується ПЗ «контроль виклику». За необхідності вони можуть доповнювати один одного.

♦ Послуга ***«зворотний виклик»*** може виконуватися з виходом з мережі Інтернет і без такого виходу. Якщо в абонента немає другої телефонної лінії для розмови з оператором, йому доведеться перервати сеанс зв'язку з мережею Інтернет. Коли абонент має дві телефонні лінії чи цифрову лінію ISDN, він може залишитися в мережі Інтернет, а по другій лінії прийняти виклик оператора. У цьому разі він може скористатися також послугами «текстовий чат», «напрямлений перегляд» і «спільне заповнення HTML форм».

В абонента після замовлення послуги «зворотний виклик» на екрані має з'явитися повідомлення виду «Ми передзвонимо Вам протягом декількох хвилин». Запит на «зворотний виклик» надходить у чергу до операторів і маршрутизирується у звичайний спосіб. В обраного оператора на екрані «спливає» вікно з номером телефону абонента, оператор натискає кнопку «зворотний виклик», і з'єднання автоматично встановлюється.

♦ Послуга ***спільного перегляду*** додатків дозволяє оператору супроводжувати абонента при перегляді інтернет-сайту телефонної компанії і допомогти знайти необхідну інформацію. Для одночасного перегляду інтернет-сторінок необхідні додатки типу Microsoft NetMeeting чи Netscape Collabra.

♦ Послуга ***передавання запиту*** через мережу Інтернет. Інтерфейс забезпечує прийом запиту електронною поштою і зворотне з'єднання оператора з абонентом через телефонну мережу.

♦ Послуга ***уніфікованих повідомлень*** дозволяє запис і збереження в кожній поштовій скриньці на рівних правах голосових, текстових і факсимільних повідомлень та файлових включень будь-якого виду. При роботі з голосовими повідомленнями мають забезпечуватися стандартні послуги голосової пошти. Обслуговування факсимільних повідомлень має дозволяти їх переадресацію, відправлення кільком абонентам, присвоєння статусу (приватне чи пріоритетне повідомлення), прикріплення до нього мовного коментаря чи використання факсимільного повідомлення як коментар до голосового повідомлення. Одержувач факсимільного повідомлення повинен мати можливість витягти його

з поштової скриньки, вивести на екран монітора або відправити на принтер.

При реалізації послуги уніфікованих повідомлень зручно використовувати спеціальні функції перетворення тексту в мову (Text-to-Speech) і тексту у факс (Text-to-Fax). Перша функція дозволяє абоненту прослухати адресовані йому повідомлення електронної пошти, а друга — роздрукувати ці повідомлення на факсимільному апараті.

Логічна структура ММ ЦОА має включати в себе такі функціональні підсистеми (рис. 1):

- інтерфейс користувачів — кінцеві пристрої абонентів (телефон, факс, ПК), що забезпечує передавання їхніх запитів за допомогою інтернету і телефонної мережі загального користування;
- інфраструктура взаємодії, яка містить систему доступу, апаратно-програмні засоби, сервери та БД ЦОА і активізується при надходженні звертання абонента, а також координує процес обслуговування абонента і контролює рівень його обслуговування;
- адміністративне керування, котре складається з пристроїв контролю, реєстрації, тарифікації, статистики й аналізу, допомагаючи адміністрації керувати роботою ЦОА і контролювати показники його функціонування;
- інтерфейс операторів, що містить устаткування РМ операторів та відповідне ПЗ і використовується операторами для відповіді на запити абонента незалежно від способу передавання запиту;
- керування інфраструктурою взаємодії, яке містить систему керування ЦОА і забезпечує надійне його функціонування.

До складу типової схеми побудови ЦОА мають входити (рис. 2):

- система автоматичного розподілу викликів (ACD), які забезпечує розподіл звернень абонентів, що надходять, по робочих місцях операторів і відправляє їх до системи інтерактивної мовної взаємодії (IVR), підімкненої до телефонної мережі, РМ операторів, сервера CTI і шлюзу IP-телефонії для зв'язку через мережу Ethernet з Web-сервером і маршрутизатором мережі Інтернет;
- система інтерактивної мовної взаємодії (IVR), яка забезпечує можливість автоматичної відповіді на запит і маршрутизацію виклику до оператора та підімкнена до системи ACD і до мережі Ethernet;
- система керування і статистики, яка керує маршрутизацією запитів, що надійшли по мережі Інтернет, збирає статистики про роботу ЦОА, та підімкнена до мережі Ethernet;
- шлюз IP-телефонії, що забезпечує сполучення ЦОА з мережею IP-телефонії (Інтернет), підімкнений до мережі Ethernet і може виконуватися у вигляді окремого пристрою чи пристрою, інтегрованого в комутаційну систему;
- сервер комп'ютерної телефонії (CTI), що забезпечує сполучення телефонної й обчислювальної систем ЦОА, підімкнений до мережі Ethernet;
- засоби доступу до мережі Інтернет, що містять Web-сервер, маршрутизатори, комутатори тощо;
- обчислювальна система, яка містить сервери E-mail, Fax для обробки інтернет-запитів і збереження баз даних, а також захисні екрани Firewall і локальну мережу Ethernet;
- робочі місця операторів і адміністраторів ЦОА, обладнані ПК і телефонною гарнітурою та включені в комутаційну й обчислювальну системи.

ММ ЦОА може додатково містити такі додатки, що розширюють пропоновані послуги:

- систему голосової пошти, що інтегрована з локальною мережею і дозволяє створити універсальну поштову скриньку, яка включає в себе електронні листи, факсимільні та голосові повідомлення;

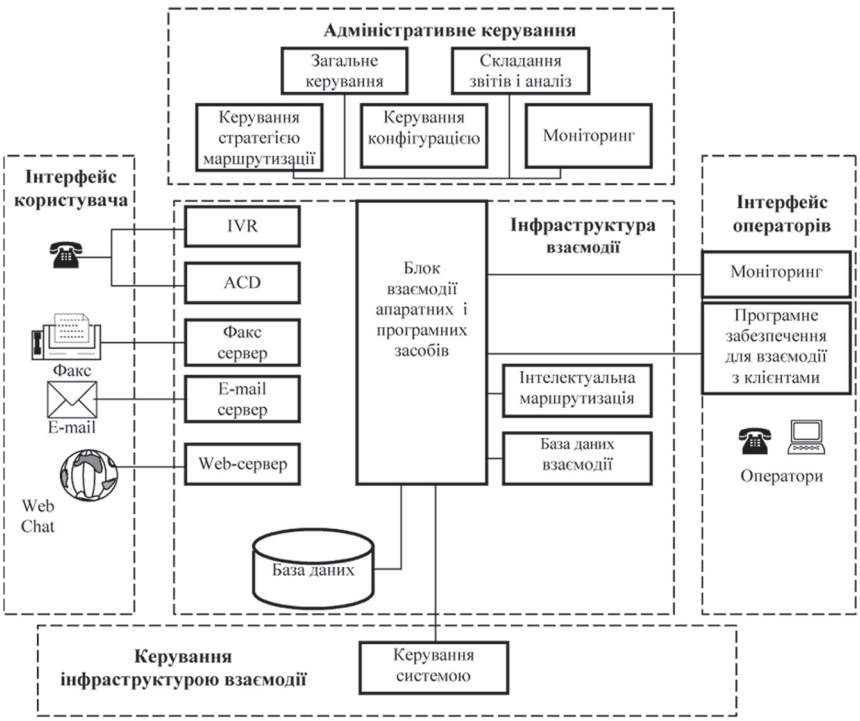

Рис. 1. Логічна структура ММ ЦОА

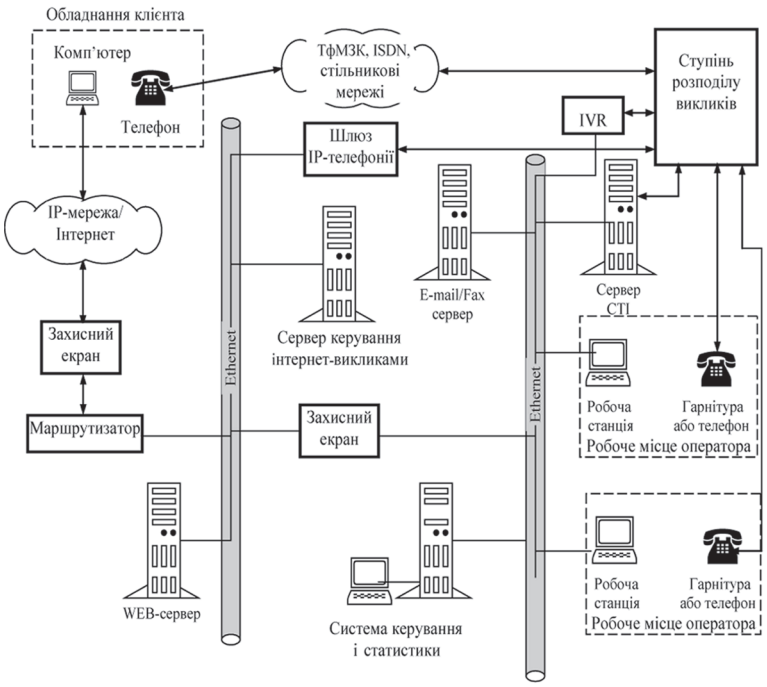

Рис. 2. Типова схема ММ ЦОА

• систему інтелектуального голосового обслуговування, що дозволяє організувати інтелектуальні автовідповідачі, які розпізнають прості голосові команди, імпульсний набір і перетворюють текст у мову (Text-to-Speech);

• систему домашнього офісу (Home Office), що дозволяє створити розподілений Центр обслуговування абонентів, в якому частина операторів буде розташована в себе вдома. Основне завдання системи — забезпечити передавання інформації, необхідної для нормальної роботи оператора вдома;

• систему голосового повідомлення, що дозволяє робити телефонне опитування абонентів, забезпечує відповідну маршрутизацію викликів, дає оцінку відповіді кожного абонента та готує загальний звіт.

Висновок

Набув подальшого розвитку метод оперативного управління комплексною системою захисту інформації авіатранспортного комплексу, що вигідно відрізняється від відомих економічно обґрунтованим підходом до розв'язання оптимізаційних задач розміщення та управління ресурсами, що дозволяє загалом аналізувати та здійснювати управління інформаційною безпекою авіатранспортного комплексу.

Література

1. ***Качинський, А. Б.*** *Безпека, загрози, ризик. Наукові концепції та математичні методи / А. Б. Качинський.— К.: Нац. академія СБУ, 2004.— 470 с.*

2. ***Косарів, О. Й.*** *Інформаційні системи на транспорті / О. Й. Косарів, А. М. Мержвинська. — К.: НАУ, 2001.*

3. ***Проект*** *Державної програми безпеки польотів [Електронний ресурс].— Режим доступу:*
http://www.avia.gov.ua/documents/

4. ***Самарский, А. А.*** *Численные методы / А. А. Самарский, А. В. Гулин.— М.: Наука, 1989.— 432 с.*

Рецензент: доктор техн. наук, професор **В. Л. Бурячок**, Державний університет телекомунікацій, Київ.

В. В. Козловский, А. В. Мищенко, О. И. Варченко, Г. С. Левинсон

МЕТОД ОПЕРАТИВНОГО УПРАВЛЕНИЯ КОМПЛЕКСНОЙ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ АВИАТРАНСПОРТНОГО КОМПЛЕКСА

Рассмотрен метод оперативного управления комплексной системой защиты информации авиатранспортного комплекса, отличающейся от известных экономически обоснованным подходом к решению оптимизационных задач размещения и управления ресурсами.

Ключевые слова: информационная безопасность; авиатранспортный комплекс; авиатранспортная инфраструктура; комплексные системы связи; защищенность информационных систем.

V. V. Kozlovskii, A. V. Mishchenko, O. I. Varchenko, H. S. Levinson

THE METHOD OF OPERATIVE MANAGEMENT OF COMPLEX INFORMATION SECURITY SYSTEM AIR TRANSPORT COMPLEX

In the article the method of surgical management of complex information security system air transport sector, which differs from the known economically reasonable approach to solving optimization problems placement and resource management.

Keywords: information security; air-traffic complex; air infrastructure; complex communication systems; information systems security.