Напрямок 7.
Комплексні системи захисту інформації

УДК 004.342.75:004.352.65

Методика розподілу доступу до ресурсів системи управління авіатранспортним комплексом з забезпеченням захисту інформації

Козловський В.В., д-р техн. наук, професор,
Міщенко А.В., канд. техн. наук, професор,
Васянович В.В., аспірант
Національний авіаційний університет, м. Київ

Вступ Сьогодні в авіатранспортному комплексі України функціонують аналогові вузли (ВСС). Дані вузли виробили свій ресурс і в найближчий час повинні бути демонтовані. Новітня цифрова комутаційна техніка і комп'ютерні технології дозволяють значно поширити можливості вузлів, ввести на локальних телефонних мережах інтелектуальні послуги й організувати додаткові довідкові, інформаційні і замовні служби, зробити їх більш привабливими для користувачів і більш надійними з точки зору інформаційної безпеки. Дані вузли спецслужб захисту інформації в авіатранспортній сфері стануть міцним фундаментом в забезпеченні інформаційної безпеки авіатранспортного комплексу.

Бурхливий розвиток мережі Інтернет і технології пакетної передачі даних вчинив безпосередній вплив на структуру розподілу доступу до ресурсів інформаційних систем. У підсумку з'явився мультимедійний Центр обслуговування інформаційних систем (ММ ЦОІС). Сучасний ММ ЦОІС – це інтегроване прикладне середовище, на базі якої здійснюється управління всіма видами електронної взаємодії з користувачами через телефонну мережу та мережу Інтернет. В ЦОІС відбувається конвергенція традиційної технології комутації каналів і нової технології пакетної передачі інформації. Обмін повідомленнями з абонентами ЦОІС здійснюється через телефонну мережу (мовні і факсимільні повідомлення) та через Інтернет (текстові повідомлення чат, текстові, музичні і мовні повідомлення електронної пошти, мовні повідомлення IP-телефонії).

Основна частина

Фундамент оперативного управління комплексною системою захисту інформації в АТК складається з двох компонентів: інформаційної та програмної складової.

Інформаційне забезпечення – найважливіший компонент ЦОВ (ClCn). Воно повинне реалізовуватися у виді відповідних баз даних (БД) сучасної архітектури. Більшість ЦОВ (ClCn) використовують архітектуру реляційних БД.

При виборі СКБД для рішення визначеної задачі варто враховувати:

– вид служби, для якої створюється база даних, і число РМ в службі;

– локальна чи розподілена структура створюваної мережі;

– зміст інформації, що передбачається зберігати;

– показники вартості;

– необхідну продуктивність, час відповіді системи на еталонне питання;

– вимоги надійності.

Для невеликих локальних мереж можна рекомендувати MS SQL Server у середовищі OS Windows XP Professional, для більш великих мереж краще 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 повинний відбуватися на стадії проектування конкретного ЦОВ (ClCn). При розробці і створенні бази даних необхідно провести аналіз змісту інформації, що передбачається зберігати: інформація предметної області, довідкова інформація, описи абонентів і т.д. На підставі аналізу варто розробити:

– схему бази даних, враховуючі всі збережені сутності і їхні взаємозв'язки;

– індекси для пошуку інформації зі змісту;

– екранні представлення і форми;

– збережені процедури і тригери;

– процедури резервного копіювання і відновлення;

– процедури архівації;

– різні SQL-сценарії для взаємодії з базою даних (запити, адміністрування, збір статистики і т.д.);

– групи користувачів;

– міри забезпечення безпеки шляхом надання різним групам користувачів різних прав доступу до бази даних.

Для нормального функціонування створена база даних вимагає постійного адміністрування і рішення наступних задач:

– створення облікових записів користувачів і керування ними;

– створення ролей, сервісних правил, прав доступу;

– забезпечення захисту даних у мережі;

– навчання і підтримка користувачів;

– модернізація існуючого програмного забезпечення й установка нового;

– архівація даних;

– імпорт і експорт даних;

– попередження втрат даних;

– моніторинг вільного простору для збереження даних на сервері;

– настроювання продуктивності й оптимізація;

– протоколювання бази даних;

– резервне копіювання даних;

– відновлення даних після аварії;

– захист мережі від вірусів;

– діагностика;

– модернізація і заміна компонентів мережі;

– додавання в мережу нових робочих станцій.

Для первісного введення інформації з неелектронних носіїв повинні бути передбачені сучасні системи оптичного розпізнавання тексту (OCR). Отриману в електронному виді вихідну інформацію необхідно перетворити в структури обраної бази даних. Для цього необхідна розробка відповідного програмного забезпечення, що враховує предметну область БД. Сформована база даних повинна бути перевірена на несуперечність програмним способом, відповідна програма також повинна бути розроблена.

Для пошуку інформації зі змістом необхідно створити повнотекстовий індекс – алфавітний покажчик слів, що зустрічаються в тексті. Для роботи з документами на

російській або українській мові повинний бути спеціально адаптований сервіс повнотекстового індексу англомовної універсальної СКБД. Важливим для ефективної роботи пошукової системи є створення словника стоп-слів.

Для підтримки інформації бази даних в актуальному стані вона повинна постійно коректуватися. Можливі наступні способи внесення коректур у БД:

– операторами служби, локально чи дистанційно;

– власником інформації, локально чи дистанційно;

– автоматично програмним забезпеченням ЦОВ (ClCn) на підставі аналізу зовнішніх джерел інформації;

– комбінованим способом, що охоплює перераховані вище способи.

Доступ до інформації бази даних повинні мати система інтерактивної мовної відповіді IVR, оператори, начальник зміни, адміністратор служби, адміністратор ЦОВ. Для роботи оператора необхідно розробити зручні екранні форми для видачі запитів до БД і відображення на екрані отриманої інформації. Повинна також передбачатися можливість віддаленого доступу до бази даних.

Програмне забезпечення разом з апаратними засобами повинне забезпечити функціональні вимоги, пропоновані до ЦОВ (ClCn) у дійсних технічних вимогах, з урахуванням загальних вимог.Програмне забезпечення ЦОВ (ClCn) повинне містити наступні компоненти прикладного і сервісного програмного забезпечення:

– програмне забезпечення для керування системою ACD;

– програмне забезпечення для керування системою IVR;

– інформаційне програмне забезпечення;

– програмне забезпечення системи контролю і реєстрації;

– програмні засоби розробки додатків.

Програмне забезпечення для керування системою ACD призначено для спостереження за роботою системи, оскільки сама система лише керує розподілом викликів між операторами за встановленими правилами і не показує, як вона функціонує. Дане ПО повинно мати наступні можливості:

– 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.д.);

– 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.

Висновки

Аргументовано подальший розвиток методу оперативного управління комплексної системи захисту інформації авіатранспортного комплексу, що відрізняється від відомих економічно обґрунтованим підходом до вирішення оптимізаційних задач розміщення та управління ресурсами та дозволяє в загальному аналізувати і здійснювати управління інформаційною безпекою авіатранспортного комплексу. Удосконалено методику розподілу доступу до ресурсів обробки і управління запитами в комп'ютеризованих інформаційних системах авіатранспортного комплексу, яка відрізняється від відомих комплексним

використанням контактних сценаріїв управління інформаційними ресурсами підприємства, що дозволяє контролювати процес обміну даними і підвищити безпеку інформаційних ресурсів систем обробки та управління запитами.

Список літератури

1. Качинський А.Б. Безпека, загрози, ризик. Наукові концепції та математичні методи. Інститут проблем національної безпеки. Національна академія служби безпеки України. Київ, 2004. – 470 с.

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

3. Самарский А.А. Гулин А.В. Численные методы. М: "Наука" 1989г. – 432с.

4. Кулинич, А. А. Субъектно-ориентированная сис-тема концептуального моделирования «Канва» [Текст]: матер. 1-й межд. конф. / А. А. Кулинич // Когнитивный ана-лиз и управление развитием ситуаций. – Москва, 2001. – С. 348.

5. Томас, Р. В., Френд Д. Х., ДаСильва Л. А., МакКензи А.Б. Когнитивные сети: адаптация и обучение для достижения конечных запланированных показателей [Текст] / Р. В. Томас, Д. Х. Френд, Л. А. ДаСильва, А. Б. МакКензи //Журнал IEEE Communications.3. – 2006. –No 12, Вип. 44. – С. 21. 2001.

6. Цибульский В. Р., Фомин В. В. Когнитология. Основные понятия когнитивного управления // Вестник кибернетики. Вып. 1.– Тюмень: Изд-во ИПОС СО РАН, 2002.– С. 34 – 37.

УДК 681.322.067

Етапи та принципи створення комплексної системи захисту інформації

Куницька С.Ю., канд. техн. наук, доцент
Черкаський державний технологічний університет, м. Черкаси

Система захисту інформації повинна створюватися спільно із створюваною комп'ютерною системою. При побудові системи захисту можуть використовуватися існуючі засоби захисту або ж вони розробляються спеціально для конкретної КС. Залежно від особливостей комп'ютерної системи, умов її експлуатації і вимог до захисту інформації процес створення КСЗІ може не містити окремих етапів, а також утримання їх може дещо відрізнятися від загальноприйнятих норм при розробці складних апаратно-програмних систем. Розробка систем включає наступні етапи:

- розробка технічного завдання;
- ескізне проектування;
- технічне проектування;
- робоче проектування;
- виробництво дослідного зразка.

Процес розробки систем, що закінчується виробленням технічного завдання, називають науково-дослідною розробкою, а іншу частину роботи по створенню складної системи називають дослідно-конструкторською розробкою. Дослідно-конструкторська розробка апаратно-програмних засобів ведеться із застосуванням систем автоматизації проектування, алгоритми проектування добре вивчені і відпрацьовані. Тому особливий інтерес представляє розгляд процесу науково-дослідного проектування.

Науково-дослідна розробка КСЗІ

Метою цього етапу є розробка технічного завдання для проектування КСЗІ, яке містить основні технічні вимоги до КСЗІ, а також узгоджені взаємні зобов'язання замовника і