Заключение

Реализация средств защиты информации на основе механизма адаптивного управления безопасностью позволяет гибко определять требуемый в данный момент времени уровень защищенности компьютерной сети, что обеспечивает снижение усредненных потерь производительности компьютерных сетей по обработке пользовательских данных. Повышение эффективности функционирования средств защиты информации с адаптивным механизмом управления безопасностью компьютерных сетей достигается за счет применения аппарата нечеткой логики, позволяющего, в частности, формализовать функциональные критерии уровня защищенности компьютерных сетей.

Список литературы

1. *А.А. Жданов, А.В. Рядовиков.* Нейронные модели в средствах адаптивного управления// Оптическая память и нейронные сети, Т. 9, N 2, 2000. – с. 115-132.

2. Guide for Production of Protection Profiles and Security Targets: N2449 Draft v0.9. – ISO/JTC1/ SC27, 2000.

3. *A. Lee.* Certificate Issuing and Management Components Family of Protection Profiles. Version 1.0. – U.S. National Security Agency, October 31, 2001.

4. Standard ISO 15408: "The common criteria for information technology security evaluation". – ISO Standards Bookshop.

5. *G. Stoneburner.* CSPP-OS: COTS Security Protection Profile – Operating Systems: Draft Version 0.4. – U.S. Department of Commerce, NIST, February 5, 2001.

6. *M. Sheridan, E. Sohmer, R. Varnum.* A Goal VPN Protection Profile For Protecting Sensitive Information. Release 2.0. – U.S. National Security Agency, 10 July, 2000.

7. *А. Ротштейн, Д. Катефников.* Идентификация нелинейных объектов на основе нечетких знаний.// Кибернетика и системный анализ, N 5 (34), 1998. – с. 67 -78.

8. *M. Negnevitsky.* Artificial intelligence: a guide to intelligent systems. Addison-Wesley, NY, 2002. – 325 p.

9. *Г.Ф. Нестерук, М.С. Куприянов.* Нейронные системы с нечеткими связями// сб. трудов VI-ой междунар. конференции SCM'2003. – С.Пб, Т.1., 2003. – с. 341-344.

10. *А.В. Спесивцев.* Управление рисками чрезвычайных ситуаций на основе формализации экспертной информации. СПб., Изд-во Политехнического университета, 2004. – 238 с.

Поступила 18.05.2007 г.

УДК 681.327.8

Клименко В.О.

КОНЦЕПТУАЛЬНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ ОРГАНІЗАЦІЇ ПОВІТРЯНОГО РУХУ

Постановка задачі

Звісно [1-7], що проблема безпеки послуг організації повітряного руху (ОрПР) розглядається у двох площинах – як забезпечення *безпеки (safety)* функціонування систем ОрПР у нормальних умовах експлуатації і як *захист (security)* систем ОрПР в умовах зростаючої агресивності середовища експлуатації.

Безпека системи ОрПР досягається за умови забезпечення безпеки всіх ресурсів, які використовуються при наданні послуг ОрПР. Тому до переліку задач захисту системи ОрПР повинні входити задачі забезпечення захисту інформаційних ресурсів системи ОрПР [8]. Проте, незважаючи на вельми високу актуальність, проблема захисту інформаційних

ресурсів системи ОрПР до цих пір залишається недостатньо вирішеною й ні знайшла адекватного відображення, наприклад, у стандартах безпеки Евроконтролю [7].

Аналіз показує [5, 6, 8], що вимоги Євроконтролю [3, 7] та ІКАО [4] у сфері безпеки ОрПР не враховують потрібною мірою всі аспекти захисту інформаційних ресурсів системи ОрПР. Перш за все, це стосується специфікацій із захисту АС ОрПР на всіх етапах їхнього життєвого циклу та конкретизації задач, які повинні вирішуватися розробниками, експлуатаційниками та оцінювальниками подібних систем для забезпечення їх захисту. Розвиток системи подібних стандартів повинен ґрунтуватися на розробках Міжнародної організації із стандартизації (МОС) у галузі безпеки інформаційних технологій (ІТ) [9,10].

Стандарти МОС стосуються як програмно-технічних, так і організаційних (адміністративних, процедурних) заходів захисту, описують методологію розбудови систем захисту, класифікують загрози, функціонали захисту, міри довіри до захисту. Методології та довідники стандартів МОС можна використовувати при розробці "завдань з безпеки" для АС ОрПР. Вони дозволяють врахувати інтереси у сфері безпеки всіх груп спеціалістів, які мають справу з автоматизованими системами ОрПР.

Стандарти МОС не містять конкретних вимог до конкретних автоматизованих системам [10], тому характерною особливістю робіт із захисту будь-якої АС ОрПР є те, що така робота повинна починатися з етапу здійснення специфічних досліджень, які стосуються розробки інформаційно-функціональної моделі АС ОрПР, політики формування режиму безпеки АС ОрПР, а також заходів підтримки, оцінки та гарантування безпеки АС ОрПР.

Ціль роботи - надати загальні концептуальні міркування щодо вирішення зазначених питань.

Інформаційно-функціональна модель АС ОрПР

Перехід авіаційної спільноти до парадигми ОрПР "gate-to-gate" вимагає інтенсивного впровадження та інтеграції широкого кола автоматизованих систем (АС) організації повітряного руху (ОрПР). До подібних автоматизованих систем відноситься низка наземних інформаційних систем (ІС) ергатичного типу: системи КПР; системи збору, обробки та розповсюдження даних спостереження; системи зв'язку, навігації, системи обробки метеорологічних даних; системи моніторингу та управління рухом об'єктів на аеродромі; системи інформування користувачів повітряного простору про стан повітряного трафіку тощо.

Автоматизовані системи ОрПР по своїй природі складні, вони включають ряд підсистем, частина з яких унікальні і є результатом власних розробок провайдерів, інші ж утворені типовими продуктами загального призначення від різних виробників (COTS). Підсистема – структурний компонент АС, здатний функціонувати окремо від решти частин АС ОрПР. Системні інтегратори АС ОрПР забезпечують взаємозв'язок і конфігурування автоматизованих підсистем у рамках загальної АС ОрПР.

АС ОрПР – це інформаційні системи, які окрім засобів ІТ включають персонал та інші нетехнічні ресурси, необхідні для їх номінальної роботи в контексті вимог операційного застосування та умов експлуатації в середовищі національної системи ОрПР.

Забезпечення безпеки АС ОрПР досягається завдяки використанню спеціальних регуляторів безпеки, тобто адміністративних, процедурних і програмно-технічних захисних заходів, призначених для усунення загроз і вразливостей, забезпечення конфіденційності, цілісності та доступності послуг АС ОрПР та оброблюваної нею інформації. Регулятори безпеки визначаються вибраною політикою безпеки ОрПР. Прийняття цієї політики ОрПР провайдером передбачається рекомендаціями ІКАО та Євроконтролем [4, 7]. Домен безпеки АС ОрПР – частина АС ОрПР, що реалізує єдиний набір технічних та організаційних політик безпеки.

При аналізі безпеки АС ОрПР слід виходити з її призначення, структурної внутрішньої взаємодії, взаємодії з різноманітними зовнішніми системами, а також враховувати всілякі загрози та вразливості. Уразливість – це дефект або слабке місце в проекті або в конкретній

реалізації АС (включаючи регулятори безпеки), які можуть бути навмисно або ненавмисно використані для шкідливої дії на ресурси та техніко-тактичні характеристики АС ОрПР. Верифікація захисних заходів – це процес оцінки, покликаний підтвердити, що регулятори безпеки АС ОрПР реалізовані коректно та ефективно відіграють відведену їм роль.

Забезпечення безпеки АС ОрПР та її компонентів може досягатися різноманітними способами - як технічними, так і організаційними.

Зазвичай, АС ОрПР:

– перебуває під контролем одного провайдера ОрПР;

– призначена для забезпечення безпеки, захисту, продуктивності, економічної ефективності, екологічності послуг ОрПР і для підтримки нових операційних процедур;

– включає як персонал, процедури, правила, норми, технічні засоби, включаючи ІТ-засоби, так і їхнє експлуатаційне середовище. Межа АС ОрПР пролягає там, де кінчається безпосередній внутрішній контроль у системі, а все інше розглядається як зовнішнє експлуатаційне середовище АС ОрПР;

– описується сукупністю ОрПР функцій, що реалізуються нею, зовнішніми інтерфейсами, а також внутрішньою структурою та внутрішніми інтерфейсами. Кожний компонент АС ОрПР може надавати одну або декілька функцій і бути реалізованим на базі одного або декількох засобів ІТ;

– зазнає істотних змін в плані процедурних, технічних та експлуатаційних нововведень по мірі еволюції у напрямі регіональної ОрПР інтеграції у Європі;

– містить дуже велику кількість ІТ-компонентів, включаючи COTS-продукти, з численними можливими варіантами конфігурування;

– містить ІТ-компоненти з різними рівнями та типами довіри до безпеки;

– включає низку доменів безпеки з різними функціональними вимогами та вимогами довіри до безпеки. Для вирішення проблеми безпеки АС ОрПР потрібно визначити загальну політику безпеки АС, загальну мету та вимоги безпеки, загальну документацію. Крім цього, можливе існування аналогічного набору для кожного домена безпеки, що містить специфічну для домена інформацію;

– залишає за провайдером вибір балансу між технічними і нетехнічними (адміністративними, процедурними) заходами забезпечення безпеки та захисту послуг ОрПР. Програмне забезпечення АС ОрПР включає прикладне і базове програмне забезпечення, а також ПЗ проміжного шару. Базове ПЗ може бути заздалегідь сертифікованим (наприклад, відповідно до вимог стандарту ISO/IEC 15408), а для інших компонентів можлива потреба в окремих свідоцтвах довіри до безпеки. Для деяких компонентів отримання подібних свідоцтв проблематичне, тому оцінювач повинен підходити до них як до "чорного ящика". Це ще один аспект різнорідності системних об'єктів оцінки в рамках АС ОрПР.

Формування режиму безпеки АС ОрПР

Процес формування режиму інформаційної безпеки АС ОрПР (або її ІТ-компоненту) включає заходи, показані на рис. 4. Перший етап полягає в ідентифікації, аналізі та оцінці ризиків, на які наражається система. Другий етап – зменшення (або ліквідація) ризиків шляхом вибору, застосування та оцінки регуляторів безпеки. На третьому етапі здійснюється акредитація АС, яка підтверджує допустимість залишкових ризиків для системи, що експлуатується в конкретному реальному середовищі.

Як засіб досягнення мети другого етапу може використовуватися оцінка безпеки, заснована на моделі оцінювання технічних регуляторів, що прийнята в стандарті ISO/IEC 15408, але поширюється на регулятори всіх видів, а не тільки на регулятори безпеки програмно-технічних засобів.

Процес оцінювання ризиків повинен бути задокументованим, оскільки його результати є початковими даними для розробки *системного завдання з безпеки (СЗБ)*.

Для формування режиму безпеки АС ОрПР слід:

– ідентифікувати ризики, які потрібно зменшити або ліквідувати;

– сформулювати мету безпеки для технічних, процедурних і адміністративних регуляторів безпеки, покликаних знизити всі ризики до прийнятного рівня;

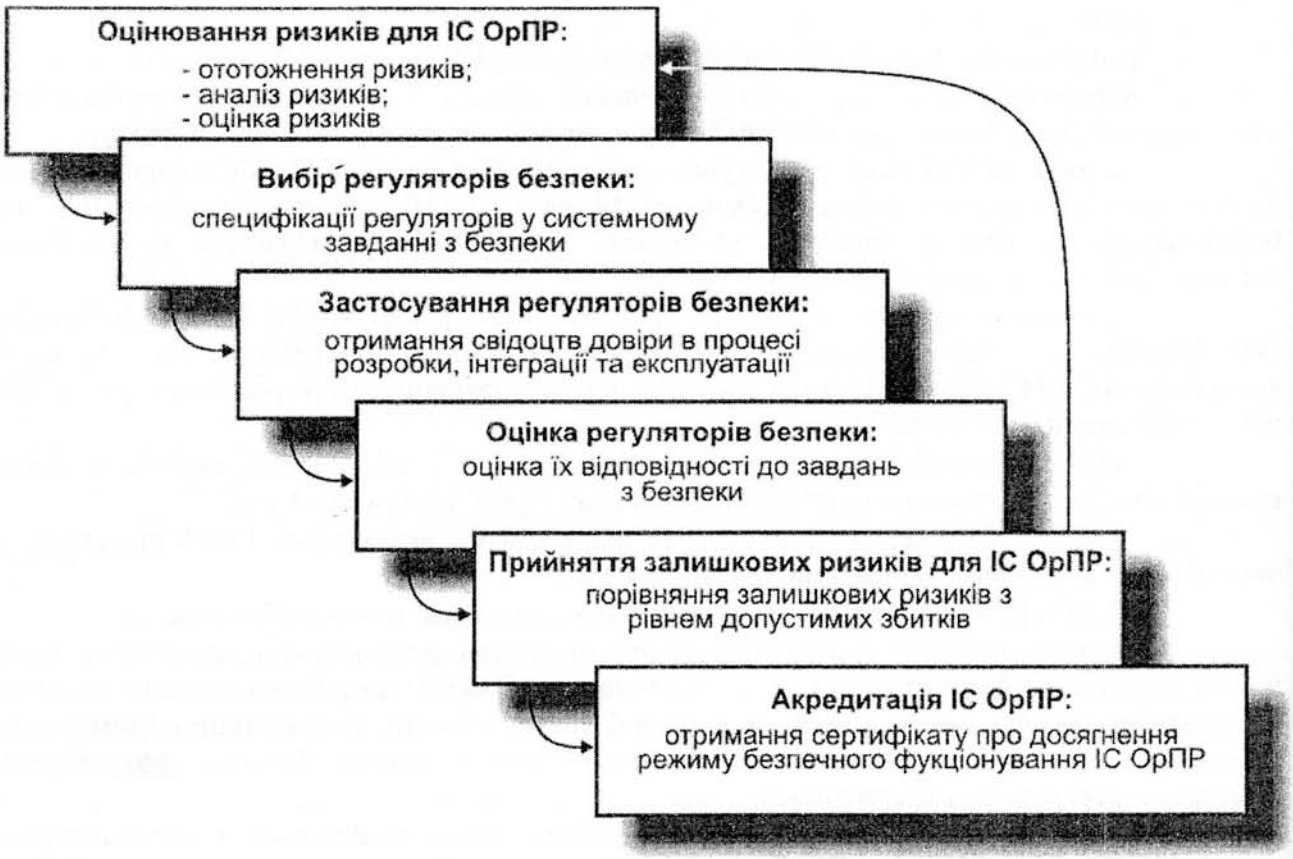


Рис. 4. Процес формування режиму інформаційної безпеки інформаційних систем ОрПР

– вибрати функціональні регулятори, що відповідають меті безпеки АС ОрПР;

– визначити конкретні, вимірні вимоги довіри для технічних, процедурних і адміністративних регуляторів безпеки, щоб отримати необхідний ступінь упевненості в здатності АС ОрПР досягти поставленої мети безпеки;

– зафіксувати ухвалені рішення в *системному завданні з безпеки (СЗБ)* для АС ОрПР;

– оцінити відповідність реальної АС ОрПР системному ЗБ;

– періодично проводити переоцінку ризиків і здатності АС ОрПР цим ризикам протистояти.

Украй важливо, що процес формування режиму безпеки АС ОрПР повинен поновлюватися при внесенні будь-яких змін в її компоненти, включаючи ІТ компоненти ОрПР.

Безпека в життєвому циклі АС ОрПР

Регулятори безпеки АС ОрПР (або її компонентів) повинні оцінюватися протягом усього її життєвого циклу. Для АС ОрПР пропонується виділити чотири етапи життєвого циклу:

1. Розробка/інтеграція.
2. Введення в експлуатацію.
3. Виробнича експлуатація.
4. Супровід.

Першим кроком першого етапу вказана ідентифікація ризиків для АС ОрПР. Після того, як виявлені неприпустимо високі ризики, що підлягають зменшенню або ліквідації засобами безпеки АС ОрПР, уповноважений посадовець розглядає очікувані залишкові ризики та підтверджує їх прийнятність.

Другий крок – проектування АС ОрПР, включаючи визначення апаратних і програмних продуктів, підтримуючої інфраструктури, прикладного програмного забезпечення і необхідних технічних регуляторів безпеки, що використовуються. Паралельно розробляється системне завдання з безпеки (СЗБ), до якого включається опис системних вимог безпеки, у тому числі перелік ризиків, яким необхідно протистояти, і цілей безпеки, яких потрібно досягти за допомогою технічних, процедурних і адміністративних регуляторів. Зафіксований в СЗБ список регуляторів може розглядатися як форма представлення системних цілей безпеки.

Вже на першому, вихідному, етапі життєвого циклу АС ОрПР слід розпочати здійснення оцінки її безпеки. Це полегшить оцінювачам розуміння системи та її передбачуваного експлуатаційного середовища, аналіз проектної документації та керівництв, отримання свідоцтв довіри до безпеки. В ідеалі слід оцінити все СЗБ, щоб переконатися у відсутності невідповідностей та упущень у вимогах безпеки і пропонованих регуляторах.

Третій крок першого етапу – розробка або закупівля базового і прикладного ПЗ, включаючи технічні регулятори безпеки, а також системна інтеграція, конфігурування та тестування розробником/інтегратором. Паралельно створюється інфраструктура безпеки для адміністративного та процедурного рівнів, документуються політики, правила та процедури безпеки, що інтегруються в системний контекст.

Якщо відбувається перебудова існуючої АС ОрПР, то виконується заміна регуляторів безпеки відповідно до середовища, що змінилося. Верифікаційна діяльність при цьому повинна бути пов'язаною з масштабом і характером змін.

За інтеграційним тестуванням розробник/інтегратор здійснює *тестування безпеки* АС ОрПР, щоб переконатися у виконанні системних вимог, що пред'являються. Зазвичай, специфічні для провайдера ОрПР параметри безпеки (технічні, адміністративні та процедурні) можуть бути визначеними до розгортання АС у виробничому середовищі, тому розробник/інтегратор може виконати верифікацію регуляторів безпеки вже на першому етапі, до початку етапу введення в експлуатацію. Верифікація повинна підтвердити силу механізмів безпеки та коректність функціонування регуляторів.

Наступний крок – оцінка автоматизованої системи. Це дасть власнику АС ОрПР незалежне підтвердження того, що всі ризики, що фігурують в СЗБ, завдяки застосуванню регуляторів безпеки зменшені до прийнятного рівня. У сертифікаційній доповіді перераховуються всі знайдені вразливості та описуються дії, що рекомендуються для їх усунення. Власник АС ОрПР готує план усунення недоліків. Результати сертифікації системи представляються уповноваженому посадовцю, що визначає допустимість реальних залишкових ризиків для системних активів і процесу функціонування.

Підсумок першого етапу – отримання офіційного дозволу на введення АС ОрПР в експлуатацію.

На другому етапі система встановлюється, розгортається і готується до використання.

На етапі виробничої експлуатації здійснюється протоколювання, безперервне відстежування роботи технічних, процедурних і адміністративних регуляторів безпеки, забезпечується зворотний зв'язок для коригуючих дій після внесення змін в АС ОрПР. Звичайно, здійснюється моніторинг не всіх регуляторів, а тільки їх критично важливої підмножини. Крім того, власник АС ОрПР повинен мати у своєму розпорядженні засоби управління конфігурацією, адміністрування та аудиту, які дозволяють отримати поточну

картину ресурсів АС ОрПР та їх конфігурації.

На етапі супроводу розглядаються та аналізуються всі запропоновані або зроблені зміни до АС ОрПР, включаючи зміни політик, правил і процедур. За потреби, виконується регресійне тестування. Якщо можлива значна зміна залишкових ризиків, то може знадобитися переоцінка АС ОрПР.

Супровід завершується виведенням системи з експлуатації, архівацією, ліквідацією або переміщенням даних на інші системи. Уповноважений посадовець повинен завірити факт успішного завершення роботи АС ОрПР.

Довіра до безпеки АС ОрПР

Довіра до безпеки АС ОрПР по своїй природі складніше за довіру до безпеки ІТ-продуктів, досягнуту в результаті здійснення оцінки за стандартом ISO/IEC 15408. Довіра повинна бути поширеною як на технічні, так і на процедурні та адміністративні регулятори безпеки, для її формування можуть знадобитися дії на всіх етапах життєвого циклу АС ОрПР, а не тільки на етапі розробки/інтеграції. АС ОрПР може складатися з багатьох доменів безпеки з різними вимогами довіри.

Поєднання всіх згаданих чинників змушує передбачити нові (порівняно із стандартом ISO/IEC 15408) дії для оцінки довіри до безпеки.

Для АС ОрПР пропонується ввести два аспекти довіри до безпеки: коректність і ефективність. Коректність означає правильну реалізацію механізмів безпеки, функціонування відповідно до документації, відстежування постійної доступності сервісів безпеки. Ефективність означає, що механізми безпеки протистоять загрозам і вразливостям і запобігають неавторизованим діям, такі як обхід захисних засобів або втручання в їх роботу. І коректність, і ефективність повинні підтримуватися на всіх етапах життєвого циклу АС ОрПР.

На етапі розробки/інтеграції АС ОрПР для перевірки коректності необхідно, перш за все, перевірити відповідність між ризиками та вимогами безпеки, а також між вимогами та контрзаходами. Вимоги повинні охоплювати всі неприпустимо високі ризики, а контрзаходи – всі вимоги безпеки. Необхідно переконатися в коректності управління конфігурацією контрзаходів. Наступний крок – перевірка коректності реалізації контрзаходів та їх включення до системи без неавторизованих модифікацій. Нарешті, слід перевірити, чи коректно відображена функціональність контрзаходів у документації на систему.

Для перевірки ефективності на етапі розробки/інтеграції АС ОрПР слід переконатися, що вимоги безпеки, включені до СЗБ, дозволяють зменшити ризики до прийнятного рівня. Потім необхідно проаналізувати проекти архітектури системи в цілому, її підсистем і компонентів, а також уявлення про реалізацію та концепцію безпеки на предмет узгодженості контрзаходів, розподілених між різними підсистемами та компонентами, і переконатися, що у сукупності ці контрзаходи забезпечують потрібні властивості безпеки АС ОрПР. Нарешті, слід перевірити, чи володіють механізми безпеки достатньою стійкістю і чи забезпечують вони захист від атак зловмисників з передбачуваним потенціалом. Для цього потрібно здійснити аналіз вразливостей і організувати тестування шляхом реальних намагань подолання захисту.

На етапі введення АС ОрПР в експлуатацію для перевірки коректності слід переконатися, що адміністративні та процедурні регулятори відповідають вимогам безпеки, а їх введення в дію санкціоновано уповноваженим посадовцем. Ефективність полягає в доведенні до відома користувачів АС ОрПР правил і процедур безпеки і в проведенні навчань. Необхідно проконтролювати формальні та змістовні результати навчання.

Для перевірки коректності на етапі експлуатації АС ОрПР слід здійснювати аудит реєстраційної інформації, перевіряти дані про доступ і використання ресурсів, щоб переконатися в коректній роботі контрзаходів. Ефективність контролюється аналогічним чином, можливо, з додатковим здійсненням опитів користувачів. Слід переконатися у відсутності несанкціонованих дій і неприпустимо високих ризиків, у відновленні безпечних

станів з небезпечних за потрібний час.

На етапі супроводу потрібно контролювати своєчасне виявлення проблем, доведення їх до відома посадовців, здійснення аналізу та внесення змін. Регресійне тестування та тестування шляхом подолання захисту повинне підтвердити, що змінені регулятори безпеки функціонують відповідно до специфікацій й ефективно протистоять ризикам.

Здійснення оцінки безпеки АС ОрПР

Процес оцінки безпеки АС ОрПР в пропонується поділити на три етапи:

– формування свідоцтв для оцінювання, включаючи результати оцінки ризиків, специфікацію системного об'єкту оцінки, дані та документацію з розробки, інтеграції, експлуатації та моніторингу АС ОрПР;

– оцінювання, включаючи сертифікацію результатів оцінки;

– акредитація АС ОрПР.

Усі зазначені дії повинні виконуватися певними посадовцями. Їхні ролі та обов'язки полягають у наступному.

На першому етапі той керівник провайдера послуг ОрПР (організації-власника АС ОрПР), який несе загальну відповідальність за ІБ, визначає допустимий рівень ризиків і санкціонує дії уповноваженого посадовця, який оцінює та визначає допустимість залишкових ризиків.

Відділ ІБ провайдера послуг ОрПР розробляє політику безпеки організації, визначає обов'язкові регулятори, які повинні бути реалізованими в усіх автоматизованих системах підприємства.

Провайдер ОрПР здійснює оцінку ризиків, визначає задачу безпеки, вирішувану АС ОрПР, готує системні профілі захисту з урахуванням вимог ІКАО та Євроконтролю, санкціонує повторне здійснення оцінки, виходячи із змін, що відбулися в системі і/або експлуатаційному середовищі, відстежує стан системи за даними протоколювання/аудиту, що безперервно надходять.

Проектувальник/розробник/інтегратор АС ОрПР створює або бере участь у формуванні СЗБ, виходячи з задачі безпеки, сформульованої провайдером послуг ОрПР; породжує свідоцтва етапу розробки; допомагає власнику системи зменшити або усунути вразливості, виявлені в процесі оцінювання.

Фахівці, що займаються адмініструванням, експлуатацією та супроводом АС ОрПР, допомагають розробити СЗБ; породжують свідоцтва етапу експлуатації; допомагають власнику системи зменшити або усунути вразливості, виявлені в процесі оцінювання.

На етапі здійснення оцінки оцінювач/представник сертифікаційного відомства оцінює АС ОрПР, виходячи з вимог безпеки, що фігурують в СЗБ, і робить висновок щодо здатності АС задовольняти ці вимоги у даний момент часу; дає незалежну оцінку безпеки діючої системи; у міру необхідності здійснює переоцінку АС ОрПР після внесення змін до системи або експлуатаційного середовища; сертифікує результати оцінки; готує доповідь за результатами оцінки і сертифікації та надає її власнику системи разом з рекомендаціями, щоб підтримати акредитацію АС ОрПР.

На етапі акредитації представник державної авіаційної адміністрації санкціонує використання АС ОрПР або підтверджує, що очікувані залишкові ризики перебувають у допустимих межах.

АС ОрПР повинна вирішувати певну задачу безпеки. У формулюванні цієї задачі повинні бути відображені два аспекти:

– результати аналізу ризиків і, зокрема, ризики, які потрібно зменшити або усунути;

– політики безпеки провайдера послуг ОрПР, які система повинна реалізовувати.

– Запропоноване рішення задачі безпеки починається з вибору мети безпеки. У контексті оцінювання АС ОрПР слід розрізняти три типи мети безпеки:

– мета, що досягається за допомогою технічних регуляторів, які реалізуються в рамках системної функціональності;

– мета, що досягається за допомогою адміністративних і/або процедурних регуляторів (політик, процедур і т.п.), які реалізуються в експлуатаційному середовищі АС ОрПР;

– мета, що досягається за допомогою заходів довіри (таких, як діяльність з верифікації).

При постановці задачі інформаційної безпеки АС ОрПР, як і в стандарті ISO/IEC 15408, вимоги безпеки поділяються на функціональні та вимоги довіри. У свою чергу, *системна функціональність безпеки (СФБ)* включає *технічні функції безпеки (ТФБ)* та *організаційні функції безпеки (ОФБ)*. Після того, як визначені вимоги безпеки, власник АС ОрПР може вибрати баланс між технічними та організаційними регуляторами безпеки. Технічні регулятори вибираються з арсеналу стандарту ISO/IEC 15408. Вимоги до організаційних (адміністративних, процедурних) регуляторів специфіковані (за сімома функціональними класами) у технічній доповіді ISO/IEC PDTR 19791.

Організаційні вимоги безпеки повинні пред'являтися до адміністративних та експлуатаційних процесів і процедур. Вони повинні бути описаними в експлуатаційному керівництві, призначеному для користувачів і операторів АС ОрПР. У процесі оцінювання перевіряється, чи надаються вибраними організаційними функціями безпеки необхідні можливості. Застосування організаційних регуляторів повинне супроводжуватися протоколюванням, що допускає подальший аудит.

Взагалі, вимоги довіри в тому вигляді, як вони сформульовані в стандарті ISO/IEC 15408 для технічних регуляторів, можуть бути застосованими буквально або легко адаптованими до адміністративних і процедурних регуляторів. Для оцінки ж АС ОрПР, яким властива складніша, порівняно з IT-продуктами, структура, потрібні додаткові вимоги довіри. Наприклад, у проектній документації та при тестуванні слід узяти до уваги загальну архітектуру АС ОрПР і специфіку доменів безпеки. Ще одна група вимог довіри необхідна для охоплення моніторингу роботи регуляторів безпеки на етапі експлуатації та для перевірки системних профілів захисту і завдань з безпеки. У технічній доповіді ISO/IEC PDTR 19791 описано десять нових класів вимог довіри стосовно автоматизованих систем.

У даній доповіді звертається увага на те, що при здійсненні оцінювання за стандартом ISO/IEC 15408 вимоги довіри зазвичай не виводяться із задачі безпеки, але просто постулюються чи вибираються "політичним рішенням". При оцінюванні автоматизованих систем доводиться враховувати відмінності в характері та об'ємі інформації про продукти IT, що використовуються, а також вибраний баланс між технічними та організаційними регуляторами безпеки і, відповідно, вибирати заходи довіри. З цього витікає те, що мета довіри повинна розглядатися як частина рішення задачі безпеки.

Ще один нюанс полягає в тому, що для АС ОрПР, які включають численні різноманітні продукти IT, доводиться враховувати існування численних середовищ розробки, принаймні одна з яких (для системної інтеграції та розробки організаційних регуляторів) співпадає з експлуатаційною. Це означає, що деякі вимоги довіри до безпеки середовища розробки виявляються нездійсненними, а застосування інших може бути відкладене до етапу введення системи в експлуатацію.

Задачі, мета і вимоги безпеки фіксуються ОрПР провайдером в системному завданні по безпеці (СЗБ). Структура СЗБ для автоматизованих систем ОрПР може ґрунтуватися на відповідних специфікаціях технічного проекту ISO/IEC PDTR 19791.

Якщо провайдер ОрПР прагне сформулювати вимоги до АС ОрПР способом, не залежним від реалізації, він може спочатку розробити *системний профіль захисту (СПЗ)*. Обов'язкові та необов'язкові частини СПЗ специфіковані в технічному докладі ISO/IEC PDTR 19791.

СЗБ є основою як документації щодо засобів безпеки АС ОрПР, так і оцінки цих засобів у межах *системного об'єкту оцінки (СОО)*. Як таке, системне ЗБ надає і свідоцтво, і інформацію, необхідну для здійснення оцінки. Як і звичне за стандартом ISO/IEC 15408 завдання з безпеки, СЗБ може бути перевірене на внутрішню несуперечність незалежно від

СОО.

Подальша оцінка СОО може виявити невідповідності між СЗБ і СОО. Наприклад: розбіжності між реальним і описаним в СЗБ експлуатаційним середовищем, між запланованою в СЗБ і реалізованою функціональністю безпеки, між реальними і запланованими інтерфейсами та їхньою поведінкою. Власник АС ОрПР повинен вирішити, що (завдання або система) є правильним, а що слід змінити. З цієї причини остаточного висновку про те, що СЗБ є коректним представленням задуманої автоматизованої системи, можна дійти лише після завершення оцінювання СОО.

Провайдер сервісу ОрПР повинен передбачити технічні і організаційні регулятори, які забезпечать його упевненість у тому, що результати оцінки автоматизованої системи зберігають свою придатність в процесі експлуатації. З цією метою він повинен:

– специфікувати адміністративні регулятори для здійснення періодичних перевірок супроводу технічних регуляторів і дієвості регуляторів організаційних;

– здійснювати періодичні переоцінки АС ОрПР з акцентом на аналіз впливу змін у вимогах безпеки організації на сукупність технічних і організаційних регуляторів і на збереження ефективності застосування організаційних заходів.

Висновки

У роботі наданий концептуальний підхід щодо формування режиму інформаційної безпеки автоматизованих систем організації повітряного руху. Міркування стосуються наступних аспектів захисту систем: розробки інформаційно-функціональної моделі, процесу формування режиму безпеки, змісту заходів щодо підтримання безпеки системи в її життєвих циклах, реалізації процесу оцінки безпеки системи та досягнення довіри до її засобів захисту.

Запропоновані концептуальні положення повністю відповідають стандартам ІКАО та Євроконтролю та документам Міжнародної організації із стандартизації у сфері захисту продуктів і систем інформаційних технологій. Вони можуть бути корисними провайдерам аеронавігаційного обслуговування щодо підвищення ефективності сервісу ОрПР, насамперед - безпеки польотів.

Практичне використання результатів потребує подальшого проведення низки додаткових досліджень, спрямованих на розробку політики інформаційної безпеки провайдерів ОрПР, критеріїв і методів категоріювання інформаційних ресурсів та оцінки можливих ризиків, створення регуляторів захисту ресурсів ОрПР та засобів оцінки обраного функціоналу захисту.

Список літератури

1. *EATMP Safety Policy*, SAF.ET1.STO1.1000-POL-01-00, Edition 2.0, 9 May 2001.

2. European Safety Program for ATM. http://www.eurocontrol.int/ esp/public/ standard_page/ 5_field_activity.html.

3. *Antonio Nogueras*, ATM security in Europe, Skyway 43 - Winter 2006.

4. Руководство по управлению безопасностью (РУБП), Документ. 9859 AN/460. ИКАО, 2006.

5. *Клименко В.А.* Анализ политики Евроконтроля в сфере организации безопасности полетов// Проблеми підвищення ефектиності інфраструктури, Збірник наукових праць, Випуск 8, Київ 2002.

6. *Клименко В.О., Поліщук К.А.* Шляхи вдосконалення безпеки польотів в умовах АТМ-інтеграції// Проблеми підвищення ефектиності інфраструктури, Збірник наукових праць, Збірник наукових праць, Випуск 9, Київ 2003.

7. EUROCONTROL Safety Regulation Commission (SRC), ESARR s, http://www.eurocontrol.int/src/public/subsite_homepage/homepage.html.

8. *Дем'янчук В.С., Клименко В.О.* Доцільність захисту інформації в автоматизованих системах управління повітряним рухом. Проблеми підвищення ефективності

інфраструктури. Зб. науков. праць, вип. 11, Київ, 2005. с. 244-245.

9. *Бетелин В.Б., Галатенко В.А., Кобзарь М.Т. и др.* Профили защиты на основе «общих критериев». Аналитический обзор, Jet Info №3(118)/2003.

10. *Галатенко В.А.* Оценка безопасности автоматизированных систем. JetInfo, N 7, 2005, http://www.jetinfo.ru/2005/7/2005.7.pdf.

Надійшла 23.04.2007 р.

УДК 621.375

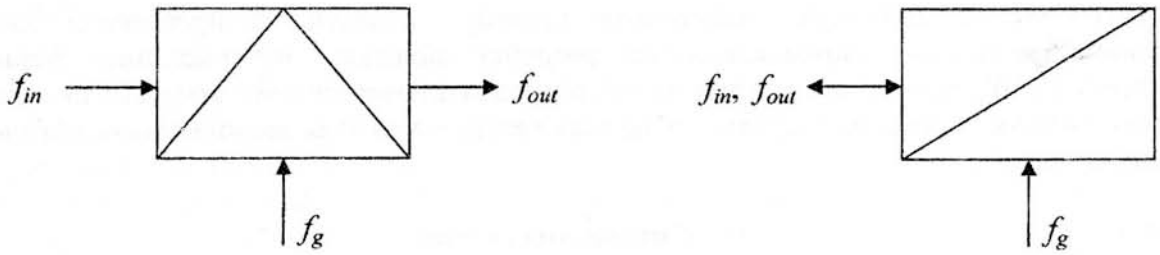
Форощук І.В.

СТРУКТУРНІ СХЕМИ ПЕРЕТВОРЮВАЧІВ ЧАСТОТИ З ПОЄДНАНИМИ ВХОДОМ І ВИХОДОМ

Вступ

Висока інтенсивність впровадження інформаційно-телекомунікаційних систем (ІТС) у різноманітні галузі людської діяльності зумовлює зростання актуальності та складності задач розробки, практичної реалізації або модифікації відповідного електронного устаткування.

Так, наприклад, стрімкий розвиток засобів радіозв'язку зумовлює значні зміни діапазонів виділених частот, що призводить до необхідності розробки нових радіоприймачів, які входять до складу комплексних систем захисту інформації, або розширення діапазону робочих частот існуючих застосуванням відповідних конверторів. Для реалізації конверторів застосовують різноманітні схеми перетворювачів частоти. На рис. 1, *а* наведений класичний перетворювач з окремими входом і виходом, де f_{in} – частота сигналу на вході перетворювача, f_g – частота сигналу гетеродину (опорного генератора), f_{out} – частота виділеного сигналу, утвореного внаслідок частотного перетворення.



а) *б)*

Рис. 1. Перетворювачі частоти:
а – з окремими входом і виходом; *б* – з поєднаними входом і виходом

Частотні конвертори знайшли широкого вжитку у сучасній схемотехніці, але складність дообладнання радіоприймача зазначеним перетворювачем частоти полягає в необхідності безпосереднього втручання у вхідний високочастотний тракт.

Альтернативою перетворювачу частоти з окремими входом і виходом є перетворювач частоти з поєднаними входом і виходом (далі – однобічний перетворювач частоти) (рис. 1, *б*). Його застосування полягає в простому паралельному приєднанні до входу радіоприймача. Подальший матеріал присвячений розробці структурної схеми однобічного перетворювача частоти (ОПЧ) та оцінці ефективності ОПЧ за обраними показниками.