УДК 004.3.684:621.396.967.2

І.І. Обод, О.О. Стрельницький

Харківський національний університет радіоелектроніки, Харків

ІНФОРМАЦІЙНА БЕЗПЕКА ІНФОРМАЦІЙНОЇ МЕРЕЖІ СИСТЕМ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

У статті на основі аналізу функціональної архітектури та інфраструктури розповсюдження даних спостереження наводиться структура інформаційної безпеки інформаційної мережі систем спостереження повітряного простору.

Ключові слова: *інформаційна безпека, мережа систем спостереження повітряного простору.*

Вступ

Постановка проблеми й аналіз літератури. Досвід провідних країн світу свідчить, що в них вже досить тривалий термін існують національні єдині системи контролю використання повітряного простору (ПП) як військовий, так і цивільною авіацією. Очевидно, що при цьому досягається максимальна ефективність використання ПП при порівняно низьких матеріальних, технічних і людських витратах.

Основні елементи процедури контролю ПП [1, 2] це: аналіз повітряної обстановки й прийняття рішень. Рішення приймає особа на основі аналізу відповідним чином підготовленої інформації про стан повітряної обстановки. Правильне рішення може бути прийнято лише тоді, коли є досить повна, точна, достовірна й безперервна інформація про повітряну обстановку в зоні управління. Отже, якість прийняття рішень визначаються якістю й складом інформації, на основі якої особа приймає рішення.

Мережному принципу побудови інформаційних засобів приділяється значна увага. Зокрема, існуючі національні єдині системи контролю використання ПП, як правило, реалізовані на мережевому використанні окремих інформаційних засобів (програми 968Н, ACCS та ін.) [3]. Основними завданнями цих програм є об'єднання в загальну інформаційну мережу (ІМ) існуючих систем спостереження (СС) різних відомств і централізоване управління цією мережею вищестоящим органом. Інформація мережі видається споживачам. Однак такий принцип організації мережі збіднює інформаційне забезпечення (ІЗ) споживачів. Дійсно, споживачеві часто потрібна інформація конкретного джерела, а не об'єднана інформація мережі. Це стимулює пошук нових методів та технологій створення ІМ на базі СС ПП для цілей надійного ІЗ споживачів та вирішення проблем функціонування окремих інформаційних засобів. У [4, 5] розглянута ІМ СС у котрій вищезазначені недоліки вирішені. Однак створення, впровадження і експлуатація ІМ СС призводить до виникнення спектра нових проблем у сфері захисту інформації ІМ тобто інформаційної безпеки (ІБ).

Мета роботи – розробка структури інформаційної безпеки ІМ СС ПП.

Основна частина

Як показано у [5], ІМ складається з різноманітних СС як джерел інформації з відповідними етапами обробки інформації, каналів передачі інформації, засобів її отримання, аналізу, реєстрації, відображення, зберігання, операторів та користувачів інформації. Таким чином основою розглядаємої ІМ є СС.

Спостереження визначається як спосіб своєчасного виявлення ПО та визначення їхнього місцезнаходження (а за потреби й отримання додаткової інформації, що стосується ПО) і своєчасного надання цієї інформації користувачам.

Функціональна архітектура спостереження описує систему, яка могла б також слугувати основою для досягнення необхідних фізичних рівнів характеристик і задоволення вимог до безпеки, визначених необхідними характеристиками спостереження.

Головним об’єктом функції спостереження є повітряний об’єкт (ПО) та його таки атрибути:

- чотиривимірне (4D) місцезнаходження ПО після первинної, вторинної та третинної обробки з відповідними матрицями точності;
- ідентифікація за ознакою «свій-чужий»;
- інші атрибути (польотна інформація (ПІ)), що вважаються операційно суттєвими.

Все це входить до картини повітряного простору. Користувачам може надаватися повний або обмежений доступ до даних спостереження.

На інфраструктуру спостереження можуть впливати численні фактори, де-яки з котрих можуть призвести до перекручування інформації. Це стосується ідентифікаційних СС, котрі побудовані за принципами одноканальних відкритих систем масового обслуговування з відмовами, що призводить до їх низької завадозахищеності при наявності навмисних корельованих завад.

Таким чином формуляр ПО, що передається споживачам, може бути сформований при наявності первинної та двох запитальних (ідентифікаційної та вторинної) СС. Інтегральним показником якості (ІПЯ) ІЗ ІМ в цьому разі може бути ймовірність ІЗ, котру можливо записана як

$$P_{inf} = D_{11}, D_{12}, D_{13}, P_{ppi}, P_{obe}, P_{por1}, P_{por2},$$

де P_{ppi} - імовірність правильного прийому ПІ, P_{obe} - імовірність об'єднання координатної та польотної інформації вторинної СС, P_{por1} - імовірність порівняння координатної інформації первинної та вторинної СС, P_{por2} - імовірність порівняння координатної інформації первинної та ідентифікаційної СС.

Імовірності правильного виявлення ПО кожною СС $P_i = D_{1i}$, є функціями

$$D_{1i} = f(D_{0i}, F_{0i}, C_i, P_0) = f(q_{0i}, z_{0i}, C_i, P_0),$$

де $z_0(C)$ – аналоговий (цифровий) поріг виявлення сигналу (ПО), q_{0i} - відношення с/ш у каналі обробки, P_0 - коефіцієнт готовності (КГ) відповідача ПО, що є характерним для вторинної та ідентифікаційної СС.

Інфраструктура розповсюдження даних спостереження складається з мережі доступу та магістральної мережі. Дані СС є нестійкими, тобто вони мають значення лише за умови вчасного надходження їх до місця обробки. Це потребує обмеженого часу затримки даних тобто передавання інформації у реальному часі. Обмін даними спостереження котре полягає у транспортуванні даних спостереження від СС до споживачів відбувається за допомогою відповідної інфраструктури зв'язку, як правило, на основі мереж. Основним питанням наразі є забезпечення багатоадресного розповсюдження даних спосте- реження від одного джерела поміж декількома споживачами. Таким чином, групове розповсюдження та маршрутизація є обов'язковими базовими функціями обміну даними спостереження.

Якісні вимоги до мережі розповсюдження даних повинні передбачати:

- безпечну, надійну та вчасну доставку даних спостереження;
- безпечну та надійну доставку даних контролю та управління;
- безперервну готовність;
- мінімальні взаємні впливи між вузлами мережі.

Дані спостереження є критично важливими для споживачів. Вони повинні бути максимально точними та вчасними.

Інформація, яка використовується в ІМ СС, потребує захисту у зв'язку з впливом значної кількості існуючих дестабілізуючих факторів (ДФ). Ці фактори впливають на якість ІЗ споживачів на етапі їх використання за призначенням.

ІМ СС повинна бути інформаційно стійкою навіть при одночасному впливі декількох дестабілізуючих факторів, що повинно забезпечуватись при її розробці та використанні.

Наявність різноманітних ДФ вимагає розробки та впровадження спеціальних заходів та засобів захисту інформації.

ІМ СС ПП як інформаційна система може характеризується наступними властивостями:

- гарантією того, що система своєчасно надає об'єкту, неперекручену, доступну інформацію тільки певному колу користувачів;
- користувачі інформації повинні бути впевненими щодо її вірогідності, надійності, повноти і об'єктивності.

Вплив ДФ на функціонування ІМ СС ПП може призвести до уможливлення загроз (наслідків) різного характеру. Ризики наразитися на наслідки реалізації загроз можуть і повинні бути оцінені з використанням кількісних та якісних показників з урахуванням якомога більшої кількості факторів.

На практиці найважливішими є три аспекти інформаційної безпеки:

• цілісність (актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни);

• доступність (можливість за розумний час отримати необхідну інформаційну послугу);

• конфіденційність (захист від несанк- ціонованого використання).

Порушення доступності, цілісності і конфіденційності інформації можуть бути викликані різними небезпечними впливами на ІМ. Тобто інформаційний ризик може бути оцінений ймовірністю порушення цілісності ($P_ц$), доступності ($P_д$) та конфіденційності ($P_к$) інформації. У цьому разі інформаційний ризик можливо записати як

$$R_i \approx P_ц + P_д + P_к, \qquad (1)$$

а ймовірність нормального ІЗ становить

$$1 - R_i \approx (1 - P_ц)(1 - P_д)(1 - P_к).$$

При захисті інформації важливими є поняття загрози та вразливості. Загроза – сукупність умов і факторів, що можуть стати причиною порушення цілісності, доступності та конфіденційності інформації. Вразливість – слабкість у системі захисту інформації, яка створює можливість реалізації загрози. Ризик виникає лише тоді, коли реалізується відповідна пара «загроза-вразливість».

При цьому вважаємо, що стани порушення цілісності, доступності та конфіденційності взаємно незалежні, тому що виникають в результаті дії різних взаємонезалежних загроз при наявності взаємонезалежних вразливостей ІМ.

Існує декілька підходів до вибору допустимого рівня ризику. Визначення допустимого рівня ризику

пов'язане з витратами на реалізацію підсистеми інформаційної безпеки.

Важливою задачею забезпечення безпеки інформації є визначення контрзаходів щодо можливих загроз (адміністративних, організаційних, програмно-технічних тощо). Методологічно це буває надзвичайно складною задачею.

На практиці використовують різні методи оцінки та управління інформаційними ризиками. Вона нерідко здійснюється за таким планом:

– ідентифікація та кількісна оцінка інформаційних ресурсів організації;

– оцінювання можливих загроз;

– оцінювання існуючих вразливостей;

– оцінювання ефективності засобів забезпечення інформаційної безпеки.

Інформаційні ризики залежать від:

– показників цінності інформаційних ресурсів;

– ймовірність реалізації загроз щодо ресурсів;

– ефективності існуючих або запланованих засобів забезпечення інформаційної безпеки.

Використовуючи вищевикладене можливо зобразити схему забезпечення інформаційної безпеки ІМ СС ПП яка наведена на рис. 1. В результаті оцінки ризиків з'являються можливості вибрати засоби та заходи, які забезпечують бажаний рівень інформаційної безпеки ІМ. При оцінці ризиків враховуються цінність інформації, значущість загроз та вразливостей, ефективність засобів захисту. Оцінка цих показників може здійснюватися як якісно, так і кількісно. Для кожного з ризиків визначається ймовірність його виникнення та розмір пов'язаних з ним втрат. На основі допустимих рівнів ризиків, розмірів потенційних втрат та ймовірностей виникнення встановлюються їхні пріоритети. Їх використовують для визначення тих ризиків, на які в першу чергу слід звернути увагу.

Висновки

Несанкціоноване втручання в роботу ІМ СС ПП може здійснюватись як на етапі тримання інформації, так і на етапах розповсюдження даних спостереження з метою порушення процесу її функціонування.

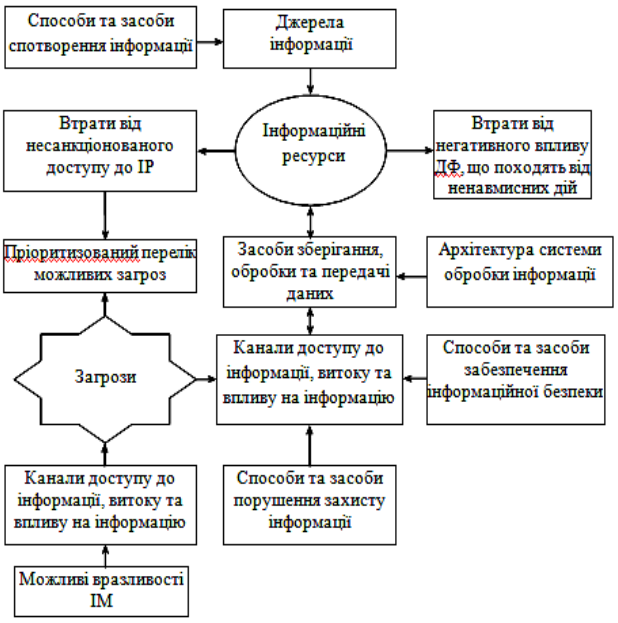

Рис. 1. Структура забезпечення інформаційної безпеки

Список літератури

1. Агаджанов П.А. Автоматизация самолетовождения и управления воздушным движением / П.А. Агаджанов, В.Г. Воробьев, А.А. Кузнецов. – М.: Транспорт, 1980. – 342 с.

2. Грачев В.В. Радиотехнические средства управления воздушным движением / В.В. Грачев, В.М. Кейн.– М.: Транспорт, 1975. – 237 с.

3. Lok J.J. C^2 for the air warrior / J.J. Lok // Jane's International Defense Review. – October 1999. – V.2. – P. 53-59.

4. Комплексне інформаційне забезпечення систем управління польотами авіації та протиповітряної оборони / [Ткачев В.В., Даник Ю.Г., Жуков С.А. і др.] – К.: МОУ, 2004. – 342 с.

5. Обод І.І. Інформаційна мережа систем спостереження повітряного простору / І.І. Обод, О.О. Стрельницький, В.А. Андрусевич. – Х.: ХНУРЕ, 2015. – 270 с.

Надійшла до редколегії 23.04.2015

Рецензент: д-р техн. наук, проф. О.А. Сєрков, Національний технічний університет «Харківський політехнічний інститут», Харків.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ СЕТИ СИСТЕМ НАБЛЮДЕНИЯ ВОЗДУШНОГО ПРОСТРАНСТВА

И.И.Обод, А.А.Стрельницкий

В статье на основе анализа функциональной архитектуры и инфраструктуры распространения данных наблюдения приводится структура информационной безопасности информационной сети систем наблюдения воздушного пространства.

Ключевые слова: *информационная безопасность, сеть систем наблюдения воздушного пространства.*

INFORMATION SECURITY INFORMATION NETWORK SURVEILLANCE AIRSPACE

I.I. Obad, A.A. Strelnickiy

The article, based on an analysis of functional and infrastructure arhitertury dissemination of observation, given the structure of the information security of the information network surveillance airspace.

Keywords: *information security, network surveillance airspace.*