ОЦІНКА ЗАХИСТУ РАДІОЛОКАЦІЙНИХ ДАНИХ В СИСТЕМІ КОНТРОЛЮ ПОВІТРЯНОГО ПРОСТОРУ

Сухоруков Д.О.[1], Шевцов І.О.[1], Обод І.І.[1]

[1]*Кафедра мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, м. Харків, Україна, E-mail: d_mts@nure.ua*

Анотація. В роботі показано, що в системах радіолокаційної ідентифікації наявна можливість перекручування радіолокаційних даних, як на етапах їх отримання і обробки, так і при передачі даних. І це заважає прийняттю вірного рішення та призводить до значних негативних наслідків.

Ключові слова – радіолокаційні дані (РД), системи радіолокаційної ідентифікації (СРІ), повітряний простір, оцінка, захист інформації.

I. Вступ

В системі контролю повітряного простору (КПП) здійснюється аналіз повітряної обстановки та прийняття рішень. Рішення приймає особа на основі аналізу відповідним чином підготовлених РД про стан повітряної обстановки. Правильне рішення може бути прийнято лише тоді, коли є досить повні, точні, достовірні та безперервні РД про повітряну обстановку в зоні управління. Отже, якість прийняття рішень визначається якістю й складом РД, на основі яких приймається рішення.

II. Оцінка захисту радіолокаційних даних

Найбільш серйозною задачею в області захисту РД залишається задача забезпечення захисту радіолокаційних даних від несанкціонованого доступу (НСД) до РД, як в процесі їх отримання, так і в процесі розповсюдження з метою їх руйнування, знищення або спотворення [1, 2].

В системі КПП існує багато джерел РД. Захист від НСД може здійснюватися в різних складових інформаційної системи і в найбільшій міри на етапі отримання РД про повітряні об'єкті (ПО). Основним видом спостереження є незалежне, некооперативне на основі локальної мережі спостереження в складі первинної радіолокаційної системи спостереження (РСС) та системи радіолокаційної ідентифікації (СРІ) за ознакою «свій-чужий» [3, 4]. Первинна РСС надає дані про місцезнаходження ПО, тобто відповідає на завданні «де», а СРІ відповідає на запитання «хто» [5, 6]. Наявність вторинної СС дозволяє отримати польотну інформацію з борту ПО. Розглянемо характеристики РСС інформація яких формує інформаційний пакет, тобто первинних, вторинних та ідентифікаційної СС.

Енергетична скритність зазначених СС визначається інформаційним сигналом, який вони використають. Використання вузько смугових сигналів у вторинних та ідентифікаційних СС призводить до практичної відсутності енергетичної скритності цих інформаційних засобів (як наземних запитувачів, так і літакових відповідачів (ЛВ) і, як наслідок, до широкого використання ЛВ зацікавленою стороною, як для дальнього виявлення та навмисного енергетичного подавлення.

Можливість несанкціонованого використання є тільки у вторинних та ідентифікаційних СС. Існуючі запитальні СС, до яких відносяться вторинні й ідентифікаційні системи (ІС), побудовані за однаковими принципами: несинхронної мережі та одноканальної системи масового обслуговування з відмовами.

Побудова ІС за такими принципами виключила часові й просторові відмінності між корисними та імітованими сигналами. Це призвело то того, що зацікавлена сторона має можливість, як несанкціоновано отримувати інформацію від розглядаємого ЛВ ІС, так і подавляти їх функціонування імітованими сигналами запиту потрібної інтенсивності.

При цьому слід зазначити, що СРІ мають високу можливість для перекручування РД. СРІ вирішують одну задачу – ідентифікації виявлених ПО за ознакою «свій-чужий». Існуючи СРІ мають однаковий принцип функціонування та імітостійкий режим. Зазначений режим дозволяє, за рахунок використання значного поля сигналу запиту (СЗ) та сигналу відповіді (СВ), випадковим вибором чергового СЗ з поля СЗ та постійною зміною відповідності СВ конкретному СЗ, це не дозволяє імітувати зацікавленій стороні «Я свій». Однак імітування СЗ з потрібною інтенсивністю дозволяє зацікавленій стороні перекрутити інформацію про ідентифікацію ПО. Ця особливість СРІ істотно знижує ефективність її використання, тому що зацікавлена сторона може паралізувати цю систему на значному віддаленні за допомогою одного запитувача, що імітує СЗ необхідної інтенсивності.

Несанкціоноване втручання в роботу окремих СС інформаційної мережі може здійснюватися, як на етапі отримання РД, так і на етапах розповсюдження даних спостереження з метою порушення процесу її функціонування. Все це показує, що захист РД в системі КПП потрібно починати з систем спостереження.

III. Висновки

Несанкціоноване втручання в роботу існуючих СРІ дозволяє здійснити перекручування радіолокаційних даних з метою порушення процесу її функціонування та виключення можливості прийняття вірного рішення.

IV. Список літератури

[1] Свид І.В. Обробка радіолокаційної РД систем спостереження повітряного простору: монографія. Дніпро : ЛІРА ЛТД, 2022. 224 с.

[2] І.І. Обод, І.В. Свид, О.С. Мальцев. Обробка даних радіолокаційних систем спостереження повітряного простору: навчальний посібник. Харків: Друкарня Мадрид, 2021. 255 с.

[3] Свид І.В., Обод І.І. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий»: монографія. Харків : Друкарня Мадрид, 2021. 254 с.

[4] Обод І.І., Свид І.В., Штих І.А. Завадозахищеність запитальних систем спостереження повітряного простору: монографія. / За заг. ред. І.І. Обода. Харків: ХНУРЕ, 2014. 312 с.

[5] I. Svyd, I. Obod, and O. Maltsev, "Interference Immunity Assessment Identification Friend or foe systems," Data-Centric Business and Applications, pp. 287–306, 2021. doi:10.1007/978-3-030-71892-3_12

[6] V. Semenets, I. Svyd, I. Obod, O. Maltsev, and M. Tkach, "Quality Assessment of measuring the coordinates of airborne objects with a secondary surveillance radar," Data-Centric Business and Applications, pp. 105–125, 2021. doi:10.1007/978-3-030-71892-3_5