УДК 621.396.96

ЗАХИСТ РАДІОЛОКАЦІЙНОЇ ІНФОРМАЦІЇ В СИСТЕМАХ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

Білоцерківець О.Г.
Науковий керівник – к.т.н., доц. Свид І.В.
Харківський національний університет радіоелектроніки, каф. МТС,
м. Харків, Україна, тел. +38057-702-0229, e-mail: d_mts@nure.ua

In the presented work, the quality of protection of radar information in airspace surveillance systems is assessed. It is shown that the unauthorized use of the information resources of the airspace control system, on the one hand, is a way of disclosing or compromising radar information, and on the other hand, it allows for unauthorized long-range detection and assessment of the coordinates of air objects.

Відомо [1-4], що до основних елементів процедури контролю повітряного простору відносяться: аналіз повітряної обстановки та прийняття рішень. Рішення приймає особа на основі аналізу відповідним чином підготовленої радіолокаційної інформації (РЛІ) про стан повітряної обстановки. Правильне рішення може бути прийнято лише тоді, коли є досить повна, точна, достовірна та безперервна РЛІ про повітряну обстановку в зоні управління. Таким чином, якість прийняття рішень визначаються складом та достовірністю РЛІ, на основі якої особа приймає рішення. Це передбачає що РЛІ, яка циркулює в системі контролю повітряного простору, повинна бути всебічно захищена.

Дійсно, це пов’язано з цим що процеси отримання, обробки, зберігання, розподілу, подання, використання РЛІ та прийняття управлінських рішень в процесі контролю повітряного простору проходить в умовах гострого інформаційного протиборства та небезпечних дестабілізуючих (випадкових і навмисних) впливів. Це призводить до того, що недооцінка питань інформаційної безпеки може привести до непередбачуваних наслідків. Відомо, що під загрозою безпеки розуміється дія або подія, яка може привести до руйнування, спотворення чи несанкціонованого використання інформаційних ресурсів [5-7].

Компрометація РЛІ, як правило, реалізується за допомогою внесення несанкціонованих змін до бази даних. В системі контролю повітряного простору зацікавлена сторона може, впливаючи на запитальну радіолокаційну систему ідентифікації за ознакою «свій-чужий», виключити можливість достовірної ідентифікації повітряних об’єктів, що призведе до жахливих результатів [8, 9]. Таким чином, у разі використання скомпрометованої РЛІ споживач наражається на небезпеку прийняття неправильних рішень з усіма наступними наслідками. Несанкціоноване використання інформаційних ресурсів, за рахунок постановки навмисних корельованих завад запитальній радіолокаційній системи в системі контролю

повітряного простору, з одного боку є засобом розкриття або компрометації РЛІ, а з іншого – дозволяє здійснити дальнє виявлення та оцінку координат повітряних об’єктів за рахунок несанкціонованого використання літакових відповідачів. В докладі наводяться методи захисту РЛІ в інформаційній мережі радіолокаційних систем спостереження [7-10], які базуються на виключені можливості несанкціонованого використання інформаційних ресурсів систем контролю повітряного простору зацікавленою стороною.

Список використаних джерел.

1. Свид І.В., Обод І.І. (2021). Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий». Харків: Друкарня Мадрид. 254 с.
2. Обод І.І., Свид І.В., Штих І.А. (2014). Завадозахищеність запитальних систем спостереження повітряного простору. Харків: ХНУРЕ. 312 с.
3. Свид І.В. (2022). Обробка радіолокаційної інформації систем спостереження повітряного простору: монографія. Дніпро : ЛІРА ЛТД. 224 с.
4. Обод І.І., Свид І.В., Мальцев О.С. (2021). Обробка даних радіолокаційних систем спостереження повітряного простору: навчальний посібник. Харків: Друкарня Мадрид. 255 с.
5. Svyd, I., Obod, I., & Maltsev, O. (2021). Interference Immunity Assessment Identification Friend or foe systems. Data-Centric Business and Applications, 287–306. https://doi.org/10.1007/978-3-030-71892-3_12.
6. Obod, I., Svyd, I., Vorgul, O., Maltsev, O., Datsenko, O., & Boiko, N. (2021). Optimization of data processing structure for multi-position radar surveillance systems. 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering. https://doi.org/10.1109/ukrcon53503.2021.9575286.
7. K. Abdul-Hussein, M., Strelnytskyi, O., Obod, I., Svyd, I., & Alrikabi, H.T.S. (2022). Evaluation of the interference’s impact of cooperative surveillance systems signals processing for healthcare. International Journal of Online and Biomedical Engineering (IJOE), 18(03), 43–59. https://doi.org/10.3991/ijoe.v18i03.28015.
8. Obod, I., Svyd, I., Maltsev, O., & Starokozhev, S. (2020). The effect of masking interference on the quality of request signal detection in aircraft responders of the identification friend or Foe Systems. 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T). https://doi.org/10.1109/picst51311.2020.9467955.
9. Svyd, I., Obod, I., Maltsev, O., Vorgul, O., Shevtsov, I., & Bilotserkivets, O. (2022). Optimizing the request signals detection of aircraft secondary radar system transponders. 2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO). https://doi.org/10.1109/elnano54667.2022.9926991.
10. Obod, I., Svyd, I., Maltsev, O., & Bakumenko, B. (2020). Comparative analysis of noise immunity systems identification friend or foe. 2020 IEEE 40th International Conference on Electronics and Nanotechnology (ELNANO). https://doi.org/10.1109/elnano50318.2020.9088856 .