

ЗАХИСТ ІНФОРМАЦІЇ У БОРТОВИХ РАДІОТЕХНІЧНИХ ЗАСОБАХ СИСТЕМ ПОСАДКИ

¹ Харківський національний університет Повітряних Сил імені Івана Кожедуба

Анотація

Робота присвячена дослідженню проблем захисту інформації в бортових радіотехнічних засобах систем посадки повітряних суден. Враховуючи зростаючу залежність авіації від цифрових технологій та зростання кіберзагроз, забезпечення безпеки цих систем є критично важливим. У роботі аналізуються потенційні загрози та вразливості, вивчаються сучасні методи захисту інформації та розробляється модель загроз. На основі проведеного дослідження формуються рекомендації щодо підвищення рівня захисту інформації в бортових радіотехнічних засобах систем посадки, що сприятиме підвищенню безпеки авіаційного транспорту.

Ключові слова: захист інформації, бортові радіотехнічні засоби, системи посадки, авіаційна безпека, кібербезпека, модель загроз.

Abstract

This paper is devoted to the study of the problems of protecting information in the onboard radio equipment of aircraft landing systems. Given the growing dependence of aviation on digital technologies and the rise of cyber threats, ensuring the security of these systems is critical. This paper analyzes potential threats and vulnerabilities, examines modern methods of information security, and develops a threat model. Based on the study, recommendations are made to increase the level of information protection in onboard radio equipment of landing systems, which will help to improve the safety of air transport.

Keywords: information security, onboard radio equipment, landing systems, aviation security, cybersecurity, threat model.

Вступ

Авіаційна безпека залежить від надійності систем посадки [1-3]. Зростання кіберзагроз вимагає посилення захисту інформації в бортових радіотехнічних засобах [4-6]. Ця робота досліджує вразливості, розробляє модель загроз та пропонує рекомендації для підвищення безпеки. Це передбачає: аналіз потенційних загроз і вразливостей; вивчення сучасних методів захисту; розробку моделі загроз; оцінку ефективності існуючих і запропонованих методів; формування практичних рекомендацій тощо.

Метою роботи є розробка рекомендацій щодо підвищення рівня захисту інформації в бортових радіотехнічних засобах систем посадки повітряних суден.

Результати дослідження

До структури бортових радіотехнічних засобів систем посадки входить наступне обладнання: радіовисотомір, курсовий маяк, глісадний маяк, маркерні радіомаяки, приймачі сигналів систем посадки, індикатори, автоматичний радіокомпас тощо.

Наземна структура бортових радіотехнічних систем посадки вразлива до кіберзагроз, таких як втручання в сигнали (підміна, глушіння, спотворення), атаки на програмне забезпечення (шкідливий код, DoS-атаки), фізичні атаки (саботаж, викрадення), кібершпіонаж (викрадення даних, прослуховування). Для захисту необхідно застосовувати комплексний підхід, що включає захист мережі (файрволи, VPN, сегментація, оновлення), захист даних (шифрування, резервне копіювання, контроль доступу), фізичний захист (обмеження доступу, відеоспостереження), захист від шкідливого ПЗ (антивіруси, фільтрація, навчання), захист від втручання в сигнали (захищені протоколи, моніторинг, резервні системи), кібербезпеку персоналу (навчання, політики, перевірки) та регулярні перевірки/аудит (оцінка вразливостей, тестування, аудит) [1-3]. Захист є безперервним процесом, що вимагає постійного моніторингу та вдосконалення заходів безпеки [1, 7-9].

Моделі загроз є важливим інструментом для аналізу та оцінки ризиків, пов'язаних з кібербезпекою

наземної структури бортових радіотехнічних систем. Вони допомагають визначити потенційні загрози, їхні джерела та можливі наслідки. Далі наведено найбільш поширені моделі загроз, які можна застосувати до поставленої задачі.

1. Модель STRIDE. Ця модель, розроблена Microsoft, класифікує загрози за шістьма категоріями: підrobка (Spoofing) - імітація авторизованого користувача або системи; втручання (Tampering) - несанкціонована зміна даних; відмова (Repudiation) - заперечення дій; розголошення інформації (Information Disclosure) - несанкціоноване розкриття даних; відмова в обслуговуванні (Denial of Service) - перешкоджання доступу до ресурсів; підвищення привілеїв (Elevation of Privilege) - отримання несанкціонованих прав доступу.

2. Модель PASTA (Process for Attack Simulation and Threat Analysis). Ця модель орієнтована на аналіз загроз на основі моделювання атак. Вона включає сім етапів: визначення цілей; визначення технічних вимог; декомпозиція програми; аналіз загроз; аналіз вразливостей; моделювання атак; аналіз ризиків.

3. Модель Trike. Ця модель використовує підхід, заснований на моделюванні загроз, для оцінки ризиків. Вона дозволяє визначити потенційні загрози та вразливості на основі аналізу архітектури системи.

4. Модель VAST (Visual, Agile and Simple Threat modelling). Ця модель призначена для інтеграції моделювання загроз у процеси розробки програмного забезпечення. Вона використовує візуальні інструменти для представлення загроз та вразливостей.

Зростання кіберзагроз становить серйозну небезпеку для авіаційних систем, особливо для критично важливих систем посадки [8-10]. Зловмисники постійно вдосконалюють методи впливу, використовуючи складне шкідливе програмне забезпечення, фішинг та атаки на системи передавання, зберігання й обробки інформації. Багато існуючих систем, особливо застарілих, мають вразливості, які можуть бути використані для несанкціонованого доступу або спотворення даних. Недостатня увага до безпеки на етапах проектування та розробки лише посилює ці проблеми.

Міжнародні стандарти, такі як стандарти ICAO, EUROCAE та RTCA, встановлюють вимоги до безпеки авіаційних систем [1-3]. Дотримання цих стандартів є обов'язковим, але також необхідно постійно оновлювати їх відповідно до нових загроз. Співпраця між виробниками обладнання, авіакомпаніями та регулюючими органами є ключовою для обміну інформацією та розробки ефективних методів захисту.

Отримані результати можуть сприяти підвищенню рівня кібербезпеки авіаційного транспорту та запобіганню можливим авіаційним критичним негараздам.

Висновки

Кіберзагрози для бортових систем посадки зростають, що вимагає посилення захисту інформації. Для ефективного захисту необхідний комплексний підхід, що охоплює технічні, організаційні та людські аспекти. Технічні заходи включають шифрування даних, системи виявлення вторгнень та міжмережеві екрани. Організаційні заходи передбачають розробку політик безпеки, навчання персоналу та регулярні аудити. Людський фактор також має велике значення, тому необхідно підвищувати обізнаність персоналу щодо кібербезпеки та впроваджувати процедури реагування на інциденти.

Результати досліджень підтверджують ефективність таких методів захисту, як шифрування даних, системи виявлення вторгнень та регулярні оновлення програмного забезпечення. Крім того, технології радіоелектронної боротьби можуть допомогти протидіяти втручанням в радіочастотний спектр. Постійне вдосконалення методів захисту є необхідним для забезпечення безпеки польотів у дедалі складнішому кіберпросторі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ICAO (Міжнародна організація цивільної авіації) стандарти та рекомендовані практики (SARPs) щодо авіаційної кібербезпеки.
2. EUROCAE (Європейська організація з обладнання цивільної авіації) стандарти та рекомендації.
3. Національні стандарти та нормативні документи з авіаційної безпеки та кібербезпеки.
4. Свид І. В. Обробка радіолокаційної інформації систем спостереження повітряного простору: монографія. / І. В. Свид. Дніпро : ЛІРА ЛТД, 2022. 224 с.

5. Свид І. В., Обод І. І. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий»: монографія. / І. В. Свид, І. І. Обод. Харків : Друкарня Мадрид, 2021. 254 с.
6. І. І. Обод, І. В. Свид, О. С. Мальцев. Обробка даних радіолокаційних систем спостереження повітряного простору: навчальний посібник. Харків: Друкарня Мадрид, 2021. 255 с.
7. І. В. Свид, А. І. Обод. Інформаційні технології обробки даних систем спостереження. // Системи управління, навігації та зв'язку. Полтава, Полтавський національний технічний університет імені Юрія Кондратюка, 2016. Вип. 4 (40). С. 91-93.
8. Свид І.В. Шляхи та методи захисту вторинних систем спостереження повітряного простору від навмисних корельованих завад. // матеріали XXV міжнародної науково-практичної конференції MicroCAD-2017 Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: секція № 22, 17-19 травня 2017 р.: у 4 ч. Ч. IV. Харків: НТУ «ХПІ», 2017. С. 161.
9. I. Svyd, I. Obod, O. Maltsev, O. Vorgul, I. Vorgul and I. Shevtsov, "Method for Increasing the Interference Immunity of the Channel for Measuring of the Short-Range Navigation Radio System," 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2022, pp. 802-807, doi: <https://doi.org/10.1109/TCSET55632.2022.9767069>.
10. D.B. Pavlova, G.E. Zavolodko, I.I. Obod, I.V. Svyd, O.S. Maltsev, L.F. Saikivska. Optimizing Data Processing in Information Networks of Airspace Surveillance Systems. Conference Proceedings of 2019 10th International Conference on Dependable Systems, Services and Technologies, DESSERT'2019, United Kingdom, Leeds, 5-7 June, 2019. Leeds: 2019. P. 136-139. doi: 10.1109/DESSERT.2019.8770022.

Ігнатович Данило Сергійович — слухач групи 453С, факультет автоматизованих систем управління та наземного забезпечення польотів авіації, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, e-mail: danila02ignatovich@gmail.com.

Науковий керівник: **Свид Ірина Вікторівна** — к.т.н., доцент, доцент кафедри авіаційних радіотехнічних систем навігації та посадки, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків; професор кафедри комп'ютерної інженерії та електроніки, Прикарпатський національний університет імені Василя Стефаника.

Ihnatovych Danylo S. — student of group 453C, Faculty of Automated Control Systems and Ground Support of Aviation, Kharkiv National Air Force University named after Ivan Kozhedub, Kharkiv, e-mail: danila02ignatovich@gmail.com.

Supervisor: **Svyd Iryna V.** — PhD, Associate Professor, Associate Professor of the Department of Aviation Radio Navigation and Landing Systems, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv; Professor of the Department of Computer Engineering and Electronics Vasyl Stefanyk Precarpathian National University.