УДК 004.056.53 (043.3)

І.А. Жуков, д.т.н.,
С.В. Балакін, к.т.н
Національний авіаційний Університет, Київ

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ АПАРАТНОЇ ТА ПРОГРАМНОЇ БЕЗПЕКИ АВІАЦІЙНИХ СИСТЕМ

Авіаційні системи є критично важливою інфраструктурою і потребують високого рівня безпеки для захисту від потенційних загроз. Безпека апаратного та програмного забезпечення є важливими компонентами забезпечення безпеки та надійності авіаційних систем [1].

Апаратна безпека стосується фізичного захисту пристроїв, які складають авіаційну систему. Сюди входять сервери, маршрутизатори, комутатори та інше обладнання, яке використовується для управління та експлуатації системи. Ось деякі з основних проблем апаратної безпеки в авіаційних системах:

1. Фізична безпека. Системи часто розташовані у віддалених районах, що робить їх уразливими до пошкодження.

2. Атаки на ланцюги поставок: авіаційні системи покладаються на мережу постачальників, що робить їх уразливими до атак на ланцюги поставок.

3. Відсутність видимості: у багатьох випадках апаратне забезпечення безпеки в авіаційних системах не видно, що ускладнює виявлення потенційних загроз або атак. Відсутність видимості ускладнює впровадження та підтримку належних заходів безпеки.

5. Залежність від сторонніх компонентів. Авіаційні системи часто покладаються на сторонні компоненти, такі як сервери, маршрутизатори та комутатори, які можуть мати вразливості або бекдори.

Безпека програмного забезпечення, з іншого боку, стосується захисту програмного забезпечення та систем, які керують авіаційною системою. Важливі аспекти безпеки програмного забезпечення в авіації:

1. Практики безпечного кодування: авіаційне програмне забезпечення має бути розроблено та розроблено з використанням методів безпечного кодування. Це означає дотримання встановлених інструкцій і стандартів безпеки, таких як OWASP

Top 10, а також виявлення та усунення потенційних вразливостей безпеки під час процесу розробки.

2. Шифрування: шифрування використовується для захисту конфіденційних даних, які передаються через мережу, наприклад інформації про літаки та пасажирів. Шифрування гарантує безпеку даних і відсутність доступу для неавторизованих користувачів.

3. Виявлення та запобігання вторгненням: системи виявлення та запобігання вторгненням використовуються для виявлення та блокування несанкціонованого доступу до авіаційної системи. Ці системи відстежують мережевий трафік і можуть ідентифікувати потенційні загрози та атаки, допомагаючи запобігти порушенням безпеки [2].

4. Регулярні оновлення програмного забезпечення: регулярні оновлення програмного забезпечення та виправлення мають вирішальне значення для усунення вразливостей системи безпеки та забезпечення того, щоб система оновлювалася з найновішими протоколами безпеки.

5. Тестування безпеки: Регулярне тестування безпеки має важливе значення для виявлення вразливостей і слабких місць в авіаційній системі.

Безпека апаратного забезпечення є важливою для захисту фізичних компонентів від потенційних атак або вразливостей, тоді як безпека програмного забезпечення має вирішальне значення для захисту компонентів програмного забезпечення від потенційних атак або вразливостей. Особливості безпеки апаратного та програмного забезпечення в авіаційних системах включають заходи фізичної безпеки, резервування, шифрування, моніторинг, методи безпечного кодування, регулярні оновлення, тестування та аудит, контроль доступу та плани реагування на інциденти.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Farivarnejad, H., Rahimi, F., & Hashemi, M. (2019). A review of aviation cyber security issues and the role of the human factor in enhancing aviation cyber security. Safety Science, 120, 327-338.

2. Zhukov I. A., Balakin S.V. Detection of computer attacks using outliner. Науковий журнал «Молодий вчений». К.: 2016. № 9(36). С. 91-93.