

В.І. Моржов, д.т.н.,
Л.І. Моржова,
Ю.О. Єрмачков,
Т.В. Німченко, к.т.н.

Національний авіаційний університет, Київ

ЗАХИСТ РОБОЧОГО МІСЦЯ ІНСТРУКТОРА АВІАЦІЙНОГО ТРЕНАЖЕРА ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Широке впровадження мультимедійних технологій та цифрової обчислювальної техніки в робоче місце інструктора (РМІ) - пілота сучасних авіаційних тренажерів (АТ) різного типу створило певні труднощі щодо захисту від несанкціонованого копіювання аеродинамічних характеристик повітряного судна та програмного забезпечення з масивами службової інформації, що розміщуються в комп'ютері РМІ.

До числа основних факторів, що обумовлюють необхідність розробки ефективних методів щодо захисту апаратно-програмних засобів АТ, відносяться: забезпечення недоступності інформації про характеристики повітряного судна (ПС) та його систем, яка є власністю організацій-розробників і не може передаватися нікому без їх відома; захист авторських прав розробників авіаційної техніки, яка моделюється в імітаторах АТ і розробників апаратних і програмних засобів тренажерної техніки.

Вся інформація про структуру побудови бортових систем та їх технічні характеристики, а також аеродинамічні і висотно-швидкісні характеристики ПС (цивільного або спеціального призначення) зберігається на технічних пристроях довгострокового зберігання інформації (жорсткі магнітні диски) комп'ютера тренажера. Суттєвим недоліком цих пристроїв є незахищеність від несанкціонованого копіювання інформації, яка зберігається на них. Це дозволяє досить просто здійснювати копіювання масивів інформації, що знаходяться на цих жорстких дисках.

Все це змушує розробляти спеціальні проектні рішення РМІ, які б забезпечували неможливість несанкціонованого доступу і копіювання масивів інформації та програмного забезпечення РМІ.

У зв'язку з цим, рішення цього завдання слід шукати при проектуванні РМІ, зокрема при розробці складу та структури

програмно-апаратних засобів РМІ. РМІ різного типу мають свої як апаратні, так і програмні особливості, які повинні враховуватися при розробці засобів захисту від несанкціонованого копіювання інформації.

Основною конструктивною особливістю є модульний принцип побудови програмного забезпечення РМІ, кожен модуль якого реалізує мультимедійну модель відповідної авіаційної системи

У зв'язку з цим, для такої модульної структури ПЗ доцільно здійснювати захист індивідуально по кожному мультимедійному модулю, тобто доступ до конкретної мультимедійної моделі РМІ буде здійснюватися тільки після підтвердження авторизації.

Цікавим є використання пристрою USB в якості міні HASP апаратного ключа (Hardware Against Software Piracy).

Доцільність такого використання пояснюється наступними факторами:

- незначна ціна таких апаратних ключів;
- тривалий термін використання ПЗ АТ;
- індивідуальний алгоритм захисту від несанкціонованого копіювання інформації.

У загальному випадку порядок організації захисту ПЗ від несанкціонованого копіювання необхідно здійснювати в наступній послідовності: 1) вибрати тип USB-пристрою, який буде використано в якості HASP апаратного ключа; 2) визначити серійні номери PID і VID USB-пристрою; 3) визначити точки входу в ПЗ тренажера через файл USB-ключа; 4) написати програму шифрування з використанням криптографічного алгоритму; 5) забезпечити автономність роботи РМІ (комп'ютер РМІ не повинен бути підключений до будь-якої комп'ютерної мережі).

Таким чином, особливості побудови ПЗ спеціалізованих АТ і їх апаратних засобів показують, що ефективний захист інформації може бути реалізовано на основі USB-пристроїв. Файл-ключ, записаний на зазначеному пристрої, відкриває доступ до певної програми цифрової моделі імітатора АТ.

Всі ці вимоги повинні бути викладені в тактико-технічному завданні на спеціалізований тренажер конкретного типу ПС.