от рассмотренного возмущающего момента в установившемся режиме уменьшается в 180 раз, а время самонастройки параметров цепи компенсации не превышает 2 с.

Работа выполнена при финансовой поддержке РФФИ. Грант №17-08-00434 А.

Литература

1. Ривкин С.С., Береза А.Д. Гироскопическая стабилизация морских гравиметров. – М. : Наука, 1985. – 176 с.

2. Современные методы и средства измерения параметров гравитационного поля Земли / Пешехонов В.Г., Степанов О.А., Августов Л.И. и др. / Под общей ред. акад. РАН В.Г. Пешехонова; научн. редактор О.А. Степанов. – СПб. : ГНЦ РФ АО «Концерн «ЦНИИ «Электроприбор», 2017. – 390 с.

3. Форсберг Р. Проведение аэрогравиметрических измерений гравиметрами «ЛАКОСТА-РОМБЕРГ» и «ЧЕКАН-АМ» с целью определения геоида / Форсберг Р., Олесен А.В., Эйнарссон И. // Гироскопия и навигация., № 3 (90), 2015. – С. 19–29.

4. Глазко В.В. Морские гравиметрические комплексы и гравиметры гидрографической службы военно-морского флота РФ / Глазко В.В., Шустов Е.Б., Филакок И.Н. // Навигация и гидрография. – № 32. – 2011. – С. 79–87.

5. Железняк Л.К. Гравиметры двойного назначения для измерений с морских и воздушных носителей / Железняк Л.К., Конешов В.Н., Несенюк Л.К. и др. // Известия высших учебных заведений. Приборостроение 2005. – Т. 48. – № 5. – С. 23–28.

6. Малютин Д.М. Распопов В.Я. Исследование динамики гиростабилизатора морского гравиметра с самонастройкой параметров / Малютин Д.М. Распопов В.Я. // Известия Тульского государственного университета. Технические науки. Вып. 9. Ч. 2. – 2017. – С. 96–104.

7. Малютин Д.М. Система для морских гравиметрических измерений повышенной точности с самонастройкой параметров гиростабилизатора // Фундаментальные и прикладные проблемы техники и технологии. № 5 (325). – 2017. – С. 147–156.

8. Бессекерский В.А., Попов Е.П. Теория систем автоматического управления. С-П. : Профессия., 2004. – 752 с.

9. Малютин Д.М. Гиростабилизатор гравиметра с комбинированным управлением // Фундаментальные и прикладные проблемы техники и технологии. № 3 (329). – 2018. – С. 123–136.

УДК 004.056

АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БОРТОВЫХ ОПЕРАЦИОННЫХ СИСТЕМ ГРАЖДАНСКОГО ВОЗДУШНОГО СУДНА

Медведев Н.В.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Безопасность информационной среды бортового оборудования гражданских воздушных судов является важнейшей составной частью безопасности полетов.

Для составления актуального и отвечающего реалиям списка угроз и атак на бортовую операционную систему (БОС) гражданского воздушного судна (ВС) необходимо в полной мере представлять себе отличительные особенности таких систем, выделяющие их в ряде других ОС.

Рассмотрим эти особенности на примере уже существующих операционных систем реального времени (ОСРВ), использующихся в настоящее время [1]:

- QNX Neutrino,
- VxWorks,
- LynxOS.

Главным требованием к ОСРВ является минимальное время задержки обработки того или иного события. На практике это означает, что должны быть малы следующие параметры:

- время отклика на прерывание – время между фактическим возникновением прерывания и началом обработки первой инструкции обработчика прерывания;
- время переключения потока управления – время переключения между двумя потоками в одном процессе;
- время переключения контекста процесса (только для ОС, поддерживающих модель процессов) – время переключения между двумя потоками управления, принадлежащими двум различным процессам.

Помимо характеристик времени обработки для ОСРВ важна также стабильность этих характеристик. Именно этот критерий во многом определяет «жесткость» ОСРВ, т. е. предсказуемость времени обработки данных, момента выдачи результатов и т. д.

Важным пунктом можно считать открытость исходных кодов ОСРВ. Открытая ОСРВ имеет явные преимущества с точки зрения ИБ. Кроме этого:

- разработчики прикладного ПО могут разобраться в сложных проблемах без привлечения службы технической поддержки;

- более простая сертификация (на отсутствие закладок и т. д.);
- динамичное развитие, так как в компанию-разработчик ОС РВ зачастую приходят не только запросы на исправления ошибок, но и предложения по устранению ошибок, улучшению системы. Сообщества разработчиков, открытых ОС РВ, как правило, растут гораздо быстрее, лучше организованы. Появляются независимые эксперты, помогающие решать задачи службы технической поддержки и участвующие в развитии, отладке и тестировании системы.

В контексте рассмотрения особенностей ОСРВ в системах воздушного движения следует упомянуть, что в настоящее время широкое распространение получают автоматизированные системы управления специального назначения, такие, как системы управления воздушным движением при посадке воздушных судов, обзора летного поля, системы предупреждения столкновений и др., в которых активно используются в качестве источников информации системы ближней радиолокации миллиметрового диапазона волн. Указанные системы функционируют совместно с БОС, решая задачи измерения координат наземных объектов, их селекции и распознавания.

БОС ВС, как правило, работают при наличии случайных и преднамеренных помех.

При формировании перечня угроз БОСРВ ВС необходимо использовать основной современный стандарт стран Европы в области обеспечения информационной безопасности и защиты информации, а именно Стандарт ИСО/МЭК 15408 – 2012.

Такой подход предполагает определить следующие понятия [2]:

- угрозы безопасности;
- политики безопасности;
- предположения безопасности.

Эти действия обычно выполняются в рамках построения Профиля Защиты (ПЗ) на Объект Оценки (в данном случае – БОСРВ ВС. Также для стандартизации требований к разрабатываемому ПО в соответствии с указанным Стандартом следует использовать Задания по Безопасности (ЗБ) и Пакеты защиты.

Определение объекта оценки (ОО) является одним из главных понятий в Стандарте ИСО/МЭК 15408. ОО – это набор программных, аппаратно-программных и/или аппаратных средств, сопровождаемый руководствами пользователя и администратора. ОО может включать ресурсы в виде электронных носителей данных (таких, как основная память, дисковое пространство), периферийных устройств (таких, как принтеры) и вычислительных возможностей (таких, как процессорное время), которые могут использоваться для обработки и хранения информации и являются предметом оценки.

Фактически, всё воздушное судно (ВС) может рассматриваться как ОО. При этом, однако, в дальнейшем мы разделим перечень угроз на угрозы отдельно для системного программного обеспечения и угрозы для функционального программного обеспечения [3].

Чтобы дать возможность заинтересованным группам или сообществам потребителей выражать свои потребности безопасности и облегчить разработку ЗБ, стандарт ИСО/МЭК 15408 предоставляет две специальные конструкции: пакеты и профили защиты (ПЗ). Требования безопасности включают две группы требований:

- функциональные требования безопасности (ФТБ): перевод целей безопасности для ОО на некоторый стандартизированный язык. ФТБ определяют правила, по которым ОО управляет использованием и доступом к своим ресурсам и, таким образом, к информации и сервисам, контролируемым ОО.
- требования доверия к безопасности (ТДБ): описание того, каким образом должно быть получено доверие к тому, что ОО удовлетворяет ФТБ.

Пакет – это именованный набор требований безопасности. Пакеты делятся на:

- функциональные пакеты, включающие только ФТБ;
- пакеты доверия, включающие только ТДБ.

Пакет может быть определен какой-либо стороной и предназначен для многократного использования. Для этой цели он должен включать требования, которые в сочетании являются полезными и эффективными.

Доверие – основа для уверенности в том, что продукт ИТ отвечает целям безопасности. Доверие могло бы быть получено путем обращения к таким источникам, как бездоказательное утверждение, предшествующий аналогичный опыт или специфический опыт. Однако ИСО/МЭК 15408 обеспечивает доверие с использованием активного исследования. Активное исследование БОС – это определение ее свойств безопасности.

Литература

1. «Comparison between QNX RTOS V6.1, VXWORKS AE 1.1 and WINDOWS CE .NET», Dedicated Systems Experts NV, June 21, 2002.

2. ГОСТ Р ИСО/МЭК 15408-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Москва, Издательство «Стандарты», 2013.

3. LynxOS. Электронный ресурс, режим доступа: http://www.rtsoft.ru/catalog/os/osrv/detail/.