Увеличение количества обрабатываемых информационных сигналов и существенное усложнение алгоритма измерительной процедуры делает целесообразным построение измерительного преобразователя на базе нескольких микроконтроллеров с двухуровневой иерархической структурой. При этом каждый микроконтроллер обрабатывает измерительную и управляющую информацию, относящуюся к одному фотоэлектрическому преобразователю или одному типу ФЭП. Электрически микроконтроллеры могут быть соединены между собой магистральным или радиальным интерфейсами, а логически управление микроконтроллерами и общим процессом измерения целесообразно организовать в конфигурации «звезда». Интерфейс измерительного преобразователя с информационно-измерительной системой можно организовать через любой из микроконтроллеров, но удобнее это сделать с использованием главного микроконтроллера, например МК 1, управляющего общим алгоритмом измерения (рисунок 2). При этом главный микроконтроллер будет освобожден от многочисленных и разнообразных частичных алгоритмов выполнения процедур измерения каждого из функциональных ФЭП. Общая задача обработки измерительного сигнала S разбивается на несколько J частных задач измерения сигналов S_J. Обработка данных об изменении неинформационных факторов и выработка сигналов управления возбуждением самого объекта контроля может быть возложена как на главный микроконтроллер МК1, так и на один из МК нижнего иерархического уровня. Благодаря разделению задач измерения многопараметрического информационного сигнала на несколько групп с одним или малым числом параметров и параллельному разделению их обработки между несколькими микроконтроллерами на выходе каждого из микроконтроллеров в каждый момент времени присутствует информация о результате измерения по каждой частичной группе параметров S_J, что существенно снижает время измерения информационного сигнала S.

Несмотря на простоту конструкции ФЭП на основе полупроводников с собственной фотопроводимостью, на их основе можно построить ряд многофункциональных одноэлементных сенсоров, чувствительных к нескольким параметрам оптического излучения и к другим воздействующим факторам [2]. Оптимальная структура многофункционального измерительного преобразователя может включать совокупность нескольких чувствительных элементов, размещенных в зоне действия нескольких физических величин, формирующих соответствующие сигналы, обрабатываемых мультипроцессорной иерархической схемой обработки измерительной информации.

Литература

1. Vorobey, R.I. / R.I. Vorobey, O.K. Gusev, A.K. Tyavlovsky, K.L. Tyavlovsky, A.I. Svistun, L.I. Shadurskaya, N.V. Yarzhembitskaya, K. Kierczynski // Photoelectric semiconductor converters with a large dynamic range. // Przeglad electrotechniczny, – Nr 5/2014, – Pp. 75–78.

2. Воробей, Р.И. Измерительные преобразователи систем оптической диагностики с многофункциональными фотоприемниками / Р.И. Воробей, О.К. Гусев, А.И. Свистун, А.К. Тявловский, К.Л. Тявловский, Л.И. Шадурская // Приборы и методы измерений, 2018. – № 3. – С. 215–226.

УДК 003.26.004.7.004.9

МОДЕЛИРУЮЩИЙ СТЕНД ИССЛЕДОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГРАЖДАНСКОГО ВОЗДУШНОГО СУДНА

Медведев Н.В.

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

Введение. Объектом исследования являются средства защиты информации комплексов связи и навигации самолета, обеспечивающие безопасность всех этапов полета гражданского воздушного судна. В статье представлен разработанный в МГТУ имени Н.Э. Баумана программно-моделирующий стенд исследования подсистемы информационной безопасности (ИБ) воздушного судна, обеспечивающий разработку имитационных моделей угроз информационной безопасности элементов, оценку ИБ оборудования воздушного судна [1].

Программно-моделирующий стенд демонстрирует безопасную работу элементов оборудования ВС, позволяя осуществлять мониторинг их технического состояния. Разработанное программное обеспечение (ПО) стенда исследования ИБ гражданского воздушного судна позволяет провести комплексирование элементов программного осуществлять мониторинг работы средств защиты информации (СЗИ) на всех этапах полета.

Исследования, проведенные в МГТУ имени Н.Э. Баумана в ходе выполнения ряда НИР сделали возможным сформулировать следующие требования к стенду исследования информационной безопасности воздушного судна:

Моделирующий стенд. Стенд исследования ИБ воздушного судна представляет собой программный имитатор, моделирующий потоки

угроз безопасности совместно с функционированием СЗИ, противодействующим таким угрозам. Имитация осуществляется в соответствии с математическим аппаратом теории массового обслуживания (*Queue Theory*). Анализ показывает, что несмотря на огромное разнообразие различных инструментов для проведения имитационного моделирования, получили преимущественное распространение имитационные модели и их реализация на GPSS. Моделирование на GPSS содержит большие потенциальные возможности для формализованного описания и имитационного моделирования защищенных бортовых вычислительных систем (БВС) [2].

Для описания явлений распространения деструктивных воздействий на автоматизированные системы бортовых компьютерных сетей предлагается использовать модель распространения разрушающего программного кода в автоматизированных системах. Как известно, БВС летательного аппарата (ЛА) представляют собой многопроцессорную систему согласно действующим нормативным документам, разрушающее программное воздействие (РПВ) на которые есть изменение состояния автоматизированной системы, вызванное выполнением кода специально созданного программного субъекта или совокупности таких субъектов, не обладающих свойством репликации. Разрушающий программный код (РПК) представляет собой машинную реализацию разрушающего программного воздействия. РПК может поступить в среду бортовых ВС ЛА по каналам радиосвязи и навигации ЛА.

Согласно международным стандартом, эффективность защиты информации определяется классом защищённости автоматизированной системы (АС). Класс защищённости, в свою очередь, определяет набор механизмов защиты (МЗ), которые должны быть реализованы в АС. Такой подход к оценке эффективности защиты информации не позволяет учитывать качество самих МЗ, констатируя лишь факт их наличия или отсутствия, также вне критериев оценки остаётся такое понятие, как изменение условий функционирования СЗИ. Примерами таких изменений могут служить модификация аппаратной и программной среды, изменение условий информационного взаимодействия объектов и субъектов защиты, числа пользователей системы, возникновение информационных конфликтов в АС.

Существуют методы, позволяющие выполнять количественную оценку защищённости информации при использовании СЗИ. Количественно защищённость информации оценивается, как правило, рядом вероятностных показателей, основной из которых – некий интегральный показатель [3].

В общем случае СЗИ представляется в виде сетевой модели или сети *массового обслуживания* (СМО), рис. 1, состоящей из некоторого набора средств защиты S_i. На вход средств защиты поступают потоки запросов НСД, определяемые моделью нарушителя на множестве потенциальных угроз $\{U_i\}$. Каждое из средств защиты отвечает за защиту от угрозы определённого типа и использует соответствующий защитный механизм. Его задача состоит в том, чтобы распознать угрозу и заблокировать несанкционированный запрос.

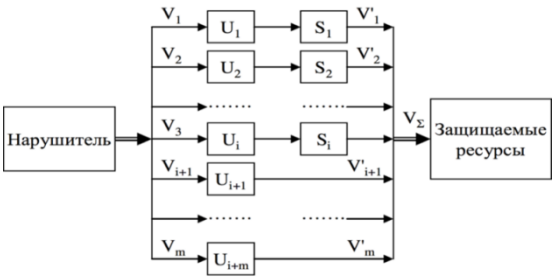

Рисунок 1 – Концептуальная модель СЗИ от НСД

В результате функционирования системы защиты исходный поток НСД разрежается, образуя выходной поток. Входные потоки несанкционированных запросов обозначены как $V_i(t)$, i = {1, ..., n}, а потоки нераспознанных (пропущенных) системой защиты НСД – $V_{i'}$. Факт неполного закрытия системой защиты всех возможных каналов проявления угроз учитывается отсутствием для m входных потоков средств защиты, что означает Vi'(t) = Vi(t). Потоки запросов на НСД, поступающие по i-м каналам, разрежаются с вероятностями $p_i(y)$, которые зависят от используемого способа обнаружения и блокирования НСД. На выходе СЗИ образуется выходной поток – объединение выходных потоков i-средств защиты и потока НСД-запросов, приходящих по m неконтролируемым каналам.

Каждое средство (механизм) защиты характеризуется вероятностью пропуска НСД – q и, соответственно, вероятностью обеспечения защиты (отражения НСД) p = 1 - q. Нарушитель характеризуется вектором интенсивностей $\lambda = \{\lambda_1, \lambda_2, ... \lambda_{i+m}\}$ попыток реализации соответствующих угроз $U_1 \ldots U_{i+m}$.

Для реализации системного подхода к решению проблемы обеспечения информационной безопасности необходимо комплексное использование методов моделирования систем и процессов защиты информации. Цели такого моделирования: поиск оптимальных решений управления МЗ, оценки эффективности использования средств и методов защиты и т.п. [3].

Представим модель СЗИ, показанную на рисунке 1 в виде функциональных блоков, объединенных в три группы, соответствующие трем основным объектам моделируемой системы: «Нарушитель», «СЗИ» и «Защищаемые ресурсы». Модель показана на рисунке 2.

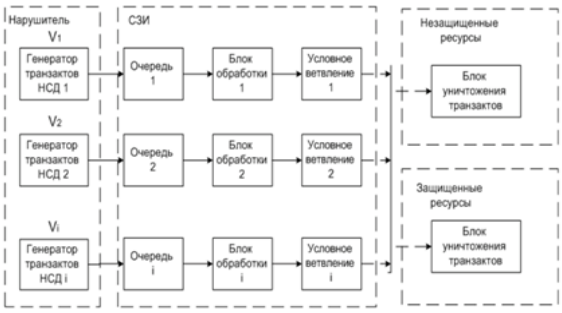

Рисунок 2 – Имитационная модель СЗИ от НСД

«Нарушитель» – это первый блок модели, в общем случае он не подвергается входному воздействию. Задача функционирования этого блока – генерация потока (потоков) запросов НСД (транзактов) с заданной интенсивностью λ. Согласно модели нарушителя, разработанной ранее, злоумышленник пытается реализовывать разные угрозы защищённости информации с соответствующими интенсивностями [4].

Блок «СЗИ» имитирует функционирование СЗИ от НСД (МЗ). Элементы этого блока могут имитировать очереди запросов НСД на входах МЗ, задержки на обслуживание, выход МЗ из строя (аппаратной части) и т.д. Однако главная задача функционирования этого блока – отсеивание запросов НСД с определённой (заданной) вероятностью.

Последний блок модели – «Защищаемые ресурсы» – не выполняет самостоятельных функций и может быть использован в имитационной модели для уничтожения запросов НСД (транзактов).

Таким образом, для построения имитационной модели СЗИ от НСД представляется целесообразным использование следующих функциональных блоков:

– генератора транзактов – для имитации поступления запросов НСД;

– блока задержки – для имитации обработки МЗ поступающих запросов НСД;

– очереди – для имитации буфера запросов каждого из МЗ;

– блоков уничтожения транзактов – для уничтожения запросов НСД (как пропущенных, так и отсеянных МЗ).

В бортовых ОС реального времени, где задержки в ряде систем критичны для работы, следует подбирать СЗИ таким образом, чтобы в случае возникновения внештатной ситуации задержки не влияли на работу системы. Для этого можно либо закладывать дополнительные мощности в СЗИ, либо использовать дублирование. Следует заметить, что, несмотря на приведённое выше общее описание системы, в данных моделях не рассматриваются угрозы, не покрываемые СЗИ: в реалиях бортовой ОС РВ оставлять какие-либо каналы незащищёнными нельзя [3]. Необходимость такого подхода обоснована приведёнными в другом разделе требованиями безопасности. Также, согласно им, в данных моделях считается, что разные СЗИ полностью независимы друг от друга, поскольку в ином случае компрометация одного СЗИ означала бы уязвимость во всём классе СЗИ.

Заключение. В целом, результаты моделирования позволяют подтвердить правомерность требований безопасности высокого уровня, а также позволяют оценить разные варианты построения системы ИБ бортового оборудования, позволяя комбинировать разные варианты использования СЗИ, исходя из известных данных об источниках угроз, имеющихся в распоряжении мощностей и топологии сети.

Тестовые сценарии стенда нацелены на демонстрацию безопасного взаимодействия между доменами Авионики и Внешней средой. Эти сценарии созданы при помощи двух мультидоменных приложений, разработанных специально для проекта. Они используют БД, размещённые в домене среднего уровня защищённости. Такой сценарий может иметь место и в процессе эксплуатации.

Литература

1. Интернет – ресурс: www.aviasafety.ru/crash-stat, последний доступ – 25.08.2017.

2. Интернет-ресурс: Документы, airspot.ru/library/dokumenty-ikao, последний доступ – 20.08.2019.

3. Интернет-ресурс: Управление инспекции по безопасности полетов РФ. www.dvmtu-favt.ru/upload/medialibrary/, последний доступ – 20.08.2019.

4. Интернет-ресурс: www.consultant.ru/popular/air/. Последний доступ 25.07.2019.

УДК 681.5:0049

МИКРОКОНТРОЛЛЕРНОЕ УПРАВЛЕНИЕ ТЕРМИЧЕСКИМИ ПРОФИЛЯ ИНФРАКРАСНОЙ ПАЙКИ ЭЛЕКТРОННЫХ МОДУЛЕЙ

Достанко А.П., Ланин В.Л., Хацкевич А.Д.

Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

По мере увеличения сложности электронных модулей растет плотность монтажа поверхностно монтируемых компонентов. Обеспечение качественных паяных соединений вызывает необходимость в технологии и оборудовании групповой пайки компонентов на плате. Современная техно-