можно существенно уменьшить путем построения системы по блочно-узловому способу. При этом все системы разбиваются на отдельные функционально законченные блоки, которые в электронных системах соединяются между собой кабелями, а в механических – связываются кинематически. Блоки в свою очередь разбиваются на функционально законченные узлы, выполняемые в виде легкосъемных конструкций. При таком построении восстановление состоит в замене вышедших из строя блоков или узлов, что значительно ускоряет процесс ввода системы в строй. Осуществление блочно-узловых конструкций тесно связано с унификацией элементов и систем, которая производится на основе отбора наиболее надежных вариантов. При этом не только повышается надежность технических систем, но и снижается их стоимость, и упрощается изготовление. В ряде случаев удается создать очень сложные системы из элементов всего двух-трех типов [3].

На стадии проектирования технических систем необходима разработка системы эксплуатационного обеспечения. Проектирование технических систем при этом должно осуществляться в соответствии с номенклатурой работ по техническому обслуживанию. Например, для планирования периодического регулирования определяющих параметров системы необходимо предусмотреть возможность контроля и прогнозирования значений этих параметров и т.д. Структурные (схемные) и конструктивные методы повышения надежности безусловно являются основными для обеспечения соответствующего уровня надежности разрабатываемых технических систем.

Литература

1. Боровиков, С. М. Расчет показателей надежности радиоэлектронных средств / С. М. Боровиков, И. Н. Цырельчук, Ф. Д. Троян ; под ред. С. М. Боровикова. – Минск: БГУИР, 2010. – 68 с.

2. Базовые элементы автоматики [Электронный ресурс]. – Режим доступа: http://electricalschool.info. – Дата доступа: 20.08.2022.

3. Надежность технических систем [Электронный ресурс]. – Режим доступа: https://studfile.net. – Дата доступа: 18.08.2022.

4. Дефекты основных типовых средств автоматизации. [Электронный ресурс]. – Режим доступа: https://www.arhivinfo.ru. – Дата доступа: 20.08.2022.

УДК 681.3

ПРОФИЛЬ ЗАЩИТЫ БОРТОВОГО ШЛЮЗА ГРАЖДАНСКОГО ВОЗДУШНОГО СУДНА

Медведев Н.В.

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

Аннотация. Предлагаются принципы построения защищенного комплекса управления гражданского воздушного судна, основанные на трех информационных доменах и открытой сетевой структуре.
Ключевые слова: гражданское воздушное судно, информационный домен, защищенный сервер, единая информационно-вычислительная платформа, комплекс.

SECURITY PROFILE OF A CIVIL AIRCRAFT AIRLOCK

Medvedev N.

Bauman State Technical University
Moscow, Russian Federation

Abstract. The principles of building a secure civil aircraft control complex based on three information domains and an open network structure are proposed.
Key words: civil aircraft, information domain, secure server, unified information and computing platform, complex.
Адрес для переписки: Медведев Н.В., ул. Вторая Бауманская, 5, Москва 105005, Российская Федерация
e-mail: medvedevnick54@yandex.ru

Бортовой защищенный шлюз (БЗШ) гражданского воздушного судна (ГВС), представляет собой программно-техническое средство, реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков и используемое в целях обеспечения защиты, в том числе и криптографическими методами, информации ограниченного доступа.

БЩЗ должен обеспечивать нейтрализацию следующих угроз безопасности информации (УБИ):

– несанкционированный доступ к информации, передаваемой по каналам взаимодействия бортового оборудования и наземных служб (табл. 1);

– отказ в обслуживании бортовых и наземных средств связи, навигации, наблюдения и наведения; бортовых информационно-вычислительных сетей ГВС; бортовых беспроводных и сенсорно-актуаторных сетей ГВС (табл. 1); информационно-вычислительной системы и системы управления ГВС;

– несанкционированная передача информации из информационно-вычислительной системы и

системы управления ГВС и (или) ее отдельных компонентов путем кибератаки по техническим каналам, см. табл. 1;

– несанкционированное воздействие на информационно-вычислительную систему и систему управления ГВС и (или) ее отдельные компоненты путем кибертатак (см. табл. 1), целью которого является нарушение функционирования, включая преодоление или обход установленных функций безопасности.

Таблица 1. Современные методы кибератак по техническим каналам

Пассивные методы	Активные методы
Электромагнитный канал	
Анализ изменения электромагнитного излучения процессоров и других компонентов	Воздействие электромагнитным полем с возникновением отказа в произвольном месте устройства или ошибки работы
Магнитный канал	
Анализ магнитного поля физически изолированных и экранированных устройств	Воздействие переменным магнитным полем, генерирующим вихревые токи, которые могут изменять состояние ячеек памяти
Акустический канал	
Прослушивание жесткого диска, трансформаторов в преобразователях питания материнской платы и т.д.	Воздействие ультразвуком на датчик вибрации жестких дисков, оптических датчиков и т.д.
Оптический канал	
Анализ изменения интенсивности рассеянного от индикаторов света	Воздействие ионизирующего лазера на полупроводники (оптическое индуцирование сбоев)
Тепловой канал	
Анализ изменения теплового излучения компонентов вычислительной системы	Изменение температуры компонентов может привести к ошибкам вычислений и передачи данных
Электрический канал	
Анализ (визуальный, статистический) изменения энергопотребления компонентов	Изменение питания вычислительной системы может привести к ошибкам вычислений

В БЗШ не должно содержаться программ, не выполняющих (не задействованных в реализации) функций безопасности или не предназначенных для обеспечения функционирования БЗШ (сторонних программ).

В БЗШ должны быть реализованы следующие функции безопасности:

– контроль и фильтрация;

– идентификация и аутентификация;

– регистрация событий безопасности (аудит);

– обеспечение бесперебойного функционирования и восстановление;

– тестирование и контроль целостности;

– управление (администрирование).

В среде, в которой функционирует БЗШ, должны быть реализованы следующие функции безопасности среды:

– исключение каналов связи в обход правил фильтрации;

– обеспечение доверенного канала;

– обеспечение доверенного маршрута;

– физическая защита;

– инспекция состояния кибербезопасности;

– трансляция протоколов домена авионики и информационного домена;

– обеспечение безопасного функционирования;

– обеспечение взаимодействия с сертифицированными средствами защиты информации;

– обеспечение безопасной управляемой коммутации.

Функции безопасности БЗШ должны обладать составом функциональных возможностей (функциональных требований безопасности), обеспечивающих реализацию этих функций.

В Профиле Защиты (ПЗ) изложены следующие виды требований безопасности, предъявляемые к БЗШ:

– функциональные требования безопасности БЗШ;

– требования доверия к безопасности БЗШ.

Функциональные требования безопасности БЗШ, изложенные в ПЗ, включают:

– требования к управлению потоками информации;

– требования к идентификации и аутентификации субъектов межсетевого взаимодействия;

– требования к регистрации событий безопасности (аудиту);

– требования к обеспечению бесперебойного функционирования БЗШ и восстановлению;

– требования к тестированию и контролю целостности ПО БЗШ;

– требования к управлению БЗШ.

Функциональные требования безопасности для БЗШ выражены на основе компонентов требований из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности».

Состав функциональных требований безопасности, включенных в настоящий ПЗ, обеспечивает следующие функциональные возможности БЗШ типа «Д»:

– возможность осуществлять фильтрацию сетевого трафика для отправителей информации, получателей информации (в том числе исполнительных устройств) и всех операций передачи контролируемой БЗШ информации к узлам автоматизированной системы управления и от них;

– возможность обеспечения фильтрации для всех операций перемещения через БЗШ информации к узлам автоматизированной системы управления и от них;

– возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности субъектов: сетевой адрес узла отправителя; сетевой адрес узла получателя; и информации: сетевой протокол, который используется для взаимодействия;

– возможность явно разрешать информационный поток, базируясь на устанавливаемых администратором БЗШ наборе правил фильтрации, основанном на идентифицированных атрибутах;

– возможность явно запрещать информационный поток, базируясь на устанавливаемых администратором БЗШ наборе правил фильтрации, основанном на идентификационных и аутентификационных атрибутах;

– возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности информации: протоколы, которые используются для взаимодействия;

– возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности информации: разрешенные/запрещенные команды;

– возможность осуществлять проверку использования отдельных команд, для которых администратором БЗШ установлены разрешительные или запретительные атрибуты безопасности;

– возможность запрещать информационный поток, если в нем обнаружены аномалии функционирования (нарушение структуры протокола, статистические аномалии и иные аномалии) действующих протоколов;

– возможность разрешать информационный поток, основываясь на результатах проверок;

– возможность запрещать информационный поток, основываясь на результатах проверок;

– возможность разрешать информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на отсутствие нарушений безопасности информации;

– возможность запрещать информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на наличие нарушений безопасности информации;

– возможность регистрации и учета выполнения проверок информации сетевого трафика;

– возможность читать информацию из записей аудита уполномоченным администраторам;

– возможность выбора совокупности событий, подвергающихся аудиту, из совокупности событий, в отношении которых возможно осуществление аудита;

– возможность оповещения уполномоченных лиц о критичных видах событий безопасности, в том числе сигнализация о попытках нарушения правил межсетевого экранирования.

Литература

1. Информационные технологии. Сеть управления электросвязью : ГОСТ Р 53633.2-2009. – Введ. 01.12.2010. – Стандартинформ. – 11 с.

2. Обеспечение безопасности сетей электросвязи : ГОСТ Р 52448-2005. – Введ. 01.01.2007. – Стандартинформ. – 16 с.

3. Объект информатизации, факторы. Воздействующие на информацию : ГОСТ 51275-2006. – Введ. 01.02.2002. – Стандартинформ. – 8 с.

4. Изделия авиационной техники. Комплексные программы обеспечения безопасности полета, надежности, контролепригодности, эксплуатационной и ремонтной технологичности. Общие требования : ГОСТ Р 56080-2014. – Введ. 01.01.2015. – Стандартинформ. – 26 с.

УДК 532; 614.8

НЕОБХОДИМОСТЬ УЧЕТА РЕАЛОГИЧЕСКИХ СВОЙСТВ РАСТВОРОВ В СИСТЕМАХ ПОЖАРОТУШЕНИЯ

Мисюкевич Н.С., Шабан Е.И.

Белорусский национальный технический университет
Минск, Республика Беларусь

Аннотация. Обоснована необходимость учета реалогических свойств пенообразующих растворов в системах пожаротушения.

Ключевые слова: реологические свойства, пожар, вода, пена, расчет.

THE NEED TO CONSIDER THE REALOGICAL PROPERTIES OF SOLUTIONS IN FIRE EXTINGUISHING SYSTEMS

Misiukevich M., Shaban L.

Belarusian National Technical University
Minsk, Republic of Belarus

Annotation. The necessity of taking into account the rheological properties of foaming solutions in fire extinguishing systems is substantiated.

Key words: rheological properties, fire, water, foam, mortar.

Адрес для переписки: Мисюкевич Н.С., пр. Независимости, 65, Минск 220113, Республика Беларусь
e-mail: misjukevitsch@mail.ru