4. Справочник «Надежность ЭРИ ИП».
5. ГОСТ 27.301-95 Расчет надежности. Основные положения.
6. РД 134-0139-2005 Методы испытаний и оценки стойкости РЭА КА к воздействию ЗЧ КП по одиночным сбоям и отказам.
7. ОСТ 134-1034-2012 Методы испытаний и оценки стойкости бортовой радиоэлектронной аппаратуры космических аппаратов к воздействию электронного и протонного излучений космического пространства по дозовым эффектам.
8. ГОСТ РВ 20.39.305-98 КСОТТ. Аппаратура, приборы, устройства и оборудование военного назначения. Требования стойкости к воздействию поражающих факторов ядерного взрыва, ионизирующих излучений ядерных установок и космического пространства.
9. Артюхова, М.А. Проблемы обеспечения стойкости бортовой радиоэлектронной аппаратуры космических аппаратов на этапах проектирования. / М.А. Артюхова, В.В. Жаднов, С.Н. Полесский. // Компоненты и технологии. - 2010. - № 9. - с. 93-98.
10. ГОСТ 27.005- 97 Надежность в технике. Модели отказов. Основные положения.
11. Жаднов, В.В. Расчетная оценка показателей долговечности электронных средств космических аппаратов и систем. / В.В. Жаднов. // Надежность и качество сложных систем. - 2013. - № 2. - с. 65-73.
12. Жаднов, В.В. Повышение точности расчётной оценки показателей долговечности бортовой космической аппаратуры. / В.В. Жаднов. / Радиовысотометрия-2013: Сборник трудов Четвертой Всероссийской научно-технической конференции. // Под ред. А.А. Иофина, Л.И. Пономарева. - Екатеринбург: Форт Диалог-Исеть, 2013. - с. 164-169.
13. ГОСТ РВ 20.39.303-98 КСОТТ. Требования к надежности. Состав и порядок задания.
14. Дружинин, Г.В. Надежность автоматизированных систем. Изд. 3-е, перераб. и доп. / Г.В. Дружинин. - М.: Энергия, 1977. - 536 с.
15. ОСТ 4.012.013-84. Аппаратура радиоэлектронная. Определение показателей долговечности.
16. Двусторонняя печатная плата. Жаднов В.В. Патент на полезную модель RU 135219 27.11.2013.
17. Артюхова, М. Оценка стойкости ИС для бортовой космической аппаратуры. / М. Артюхова, В. Жаднов, С. Полесский. - Электронные компоненты. - 2013. - № 1. - с. 72-76.
18. Жаднов, В.В. Особенности конструирования бортовой космической аппаратуры: учеб. пособие. / В.В. Жаднов, Н.К. Юрков. - Пенза: Изд-во ПГУ, 2012. - 112 с.

УДК 621.396.6, 621.8.019.8

Лушпа И.Л., Монахов М.А.

Национальный исследовательский университет «Высшая школа экономики», Московский институт электроники и математики, Москва, Россия

ИССЛЕДОВАНИЕ НАДЕЖНОСТИ МЕХАНИЧЕСКИХ КОМПОНЕНТОВ АНТЕННО-ФИДЕРНОГО УСТРОЙСТВА СИСТЕМЫ УПРАВЛЕНИЯ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ

Данное научное исследование (№ 14-05-0038) выполнено при поддержке Программы «Научный фонд НИУ ВШЭ» в 2014 г. Одним из главных показателей надежности радиоэлектронной аппаратуры (РЭА) является ее безотказность. При этом стоит отметить, что помимо электрорадиоизделий, весомый вклад в безотказность РЭА вносят механические элементы [1]. Основной характеристикой безотказности механических элементов является интенсивность отказов.

Оценка надежности РЭА выполняется на ранних стадиях проектирования для осуществления поддержки на этапе конструирования (разработки опытного образца). Выполнение расчета надежности обеспечивает уточнение требований к надежности на начальных стадиях конструирования, и характеризует вероятность отказов РЭА за время его эксплуатации [2, 3].

Как результат, осуществление расчета надежности позволяет внести усовершенствования в разработку РЭА, предотвращая дорогостоящее исправление уже существующей конструкции и сократить само время разработки.

Однако принятые в настоящее время методики расчета надежности РЭА выполняются с допущением, что если обеспечена стойкость конструкции к воздействию внешних нагрузок, то она «абсолютно надежная» [4].

В плане оценки надежности механических элементов (МЭ) больший интерес представляют модели, приведенные в американском стандарте NSWC-11 [5], разработанного специалистами Кардерокской дивизии ВМФ США. В стандарте NSWC-11 [5] приведена методика, дающая оценку показателей безотказности и ремонтопригодности механического оборудования.

Математическая модель интенсивности отказов МЭ имеет следующий вид [3]:

$$\lambda_p = \lambda_{p,b} \cdot \prod_{i=1}^{n} C_i \qquad (1)$$

где: $\lambda_{p,b}$ – базовая интенсивность отказов типа (группы), рассчитанная по результатам испытаний на безотказность, долговечность, ресурс; C_i - коэффициенты, учитывающие изменения эксплуатационной интенсивности отказов в зависимости от различных факторов; n – число учитываемых факторов.

Следует отметить, что данный стандарт постоянно переиздается, и математические модели усовершенствуются.

Рассмотрим пример использования методики стандарта NSWC-11 [5] для оценки интенсивностей отказов МЭ антенно-фидерного устройства системе управления беспилотным летательным аппаратом (БЛА), эскиз конструкции которого представлен на рисунке 1.

Для определения нагрузок и нахождения слабых мест конструкции антенно-фидерного устройства в программе SolidWorks была построена 3D-модель и проведен анализ на внешние воздействия, в результате которого расчетные значения нагрузок на элементы конструкции оказались меньше предельно-допустимых.

Однако использование в конструкции устройства прокладок для герметизации и резьбовых соединений, в соответствии с методиками стандарта NSWC-11 [5], вызывают необходимость исследования интенсивности отказов. Перечь таких элементов, используемых в конструкции антенно-фидерного устройства, приведен в таблице 1.

Перечень элементов — Таблица 1

Обозначение	Наименование
Прокладка	Duraver-E-104-ML Prepeg 1080 05 AT 01 (0,063), 100+2 X 100+2
Винт	Винт М2.5-6gx4.21.11 ОСТ92-0728-72
Винт	Винт В.М1,6-6Н-6gx10.32.133 ГОСТ 17475-80

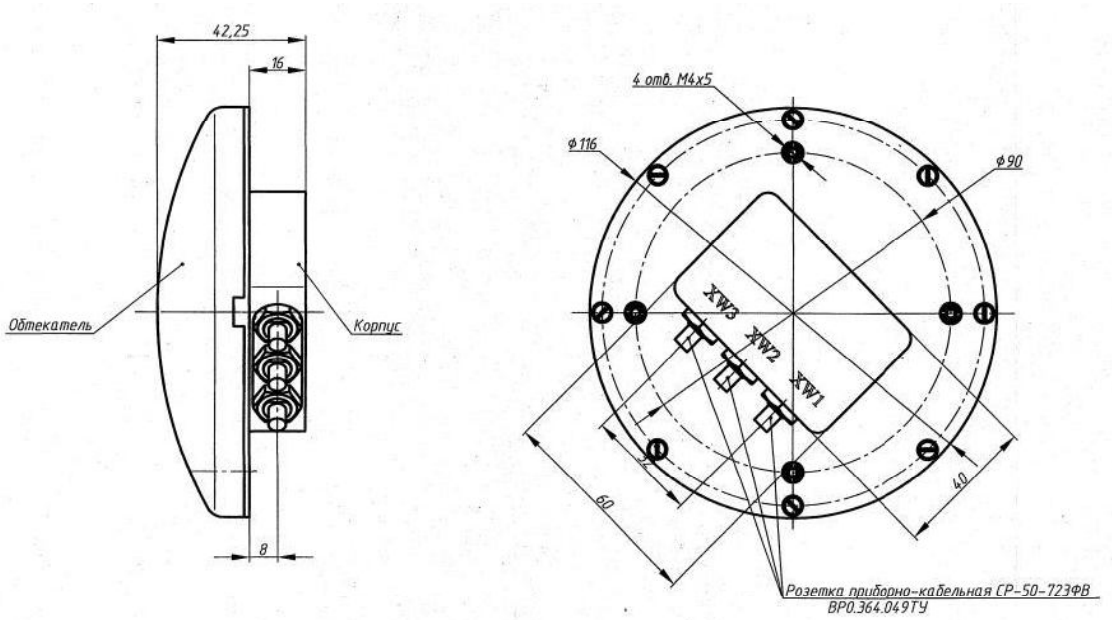

Рисунок 1 – Эскиз конструкции антенно-фидерного устройства

Математическая модель интенсивностей отказов, приведенная в стандарте NSWC-11 [5] для прокладок, имеет вид:

$$\lambda_{SE} = \lambda_{SE,B} \cdot C_P \cdot C_Q \cdot C_{DL} \cdot C_H \cdot C_F \cdot C_V \cdot C_T \cdot C_N \qquad (2)$$

где: $\lambda_{SE,B}$ - базовая интенсивность отказов; C_P - поправочный коэффициент, учитывающий давление жидкости на базовую интенсивность отказа; C_Q - поправочный коэффициент, учитывающий эффект от допустимой утечки на базовую интенсивность отказа; C_{DL} - поправочный коэффициент, учитывающий эффект от размера заглушки на базовую интенсивность отказа; C_H - поправочный коэффициент, учитывающий эффект от контактного напряжения и стойкости изоляции на базовую интенсивность отказа; C_F - поправочный коэффициент, учитывающий эффект от шероховатости гнезда заглушки на базовую интенсивность отказа; C_V - поправочный коэффициент, учитывающий влияния вязкости жидкости на базовую интенсивность отказа; C_T - поправочный коэффициент, учитывающий влияние температуры на базовую интенсивность отказа; C_N - поправочный коэффициент, учитывающий влияние загрязнений на базовую интенсивность отказа;

Математическая модель интенсивностей отказов, приведенная в стандарте NSWC-11 [5] для резьбовых соединений, имеет вид:

$$\lambda_F = \lambda_{F,B} \cdot C_{SZ} \cdot C_L \cdot C_T \cdot C_I \cdot C_K \qquad (3)$$

где: $\lambda_{F,B}$ - базовая интенсивность отказов; C_{SZ} - поправочный коэффициент, учитывающий влияние отклонения размера от размеров тестового образца S-N; C_L - поправочный коэффициент, учитывающий влияние различных нагрузок; C_T - поправочный коэффициент повышенной температуры; C_I - поправочный коэффициент, учитывающий влияние нагрузки от циклических ударов; C_K - поправочный коэффициент нагрузки для резьбы соединителя;

Как видно из (2) и (3), модель резьбовых соединений проще, чем модель прокладок, что даёт менее точный результат оценки интенсивности отказов.

Расчетные значения интенсивность отказов прокладки и резьбовых соединений приведены в таблице 2.

Таблица 2

Результаты расчета интенсивности отказов

Наименование	Интенсивность отказов, $ч^{-1}$
Прокладка	$3.072 \cdot 10^{-7}$
Винт 1	$4.364 \cdot 10^{-7}$
Винт 2	$2.241 \cdot 10^{-7}$

Заключение

На основе проведенного исследования можно сделать следующие выводы:

- анализ интенсивности отказов МЭ на начальных этапах позволяет решить проблемы на более поздних этапах проектирования РЭА.

- результаты проведенного расчета позволяют сделать вывод о том, что при большом числе механических элементов они могут существенно увеличивать суммарную интенсивность отказов РЭА.

- расчет интенсивностей отказов механических элементов позволяет дать более полную картину в оценке надежности РЭА.

Таким образом очевидно, что при оценки показателей надежности РЭА необходимо учитывать не только электрорадиоизделия, но и механические элементы, поэтому современные программные средства расчетов надежности должны иметь соответствующие модули [6, 7].

ЛИТЕРАТУРА

1. Маркин, А.В. Методы оценки надёжности элементов механики и электромеханики электронных средств на ранних этапах проектирования. / А.В. Маркин, С.Н. Полесский, В.В. Жаднов. // Надёжность. - 2010. - № 2. - с. 63-70.

2. Жаднов, В.В. Управление качеством при проектировании теплонагруженных радиоэлектронных средств: учебное пособие. / В.В. Жаднов, А.В. Сарафанов - М.: СОЛОН-ПРЕСС, 2012. - 464 с. - Сер. «Библиотека инженера».

3. Жаднов, В.В. Автоматизация проектных исследований надёжности радиоэлектронной аппаратуры: научное издание. / В.В. Жаднов, Ю.Н. Кофанов, Н.В. Малютин. - М.: Радио и связь, 2003. - 156 с.

4. Абрамешин, А.Е. Информационная технология обеспечения надёжности электронных средств наземно-космических систем: научное издание. / А.Е. Абрамешин, В.В. Жаднов, С.Н. Полесский; отв. ред. В.В. Жаднов. - Екатеринбург: Форт Диалог-Исеть, 2012. - 565 с.

5. NSWC-11. Handbook of reliability prediction procedures for mechanical equipment.
6. Жаднов В.В. Методы и средства оценки показателей надежности механических и электромеханических приборов и систем. / В.В. Жаднов. // Датчики и системы. - 2013. - № 4. - с. 15-20.
7. Zhadnov, V. Methods and means of the estimation of indicators of reliability of mechanical and electromechanical elements of devices and systems. / V. Zhadnov. // Reliability: Theory & Applications. - 2011. - Vol. 2, No 4. - p. 94-102.

УДК 621.322

Агафонова М.Е.
НПО «Эшелон», Москва, Россия

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ АУДИТА СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время сложно представить организацию, которую бы не интересовали вопросы управления информационной безопасностью. С ростом ценности активов компании и усложнением бизнес-процессов требуется все большее количество ресурсов для построения комплексной системы управления (менеджмента) информационной безопасностью и ее обеспечения [6]. Данную систему необходимо подвергать аудиту на соответствие требованиям информационной безопасности. Опыт проведения аудита и сертификации систем менеджмента информационной безопасности позволил выявить ряд практических приемов, которые будет приведены ниже по тексту.

Основы аудита информационной безопасности

Аудит системы управления информационной безопасностью позволяет определить наиболее уязвимые места в защите компании, помогает оценить эффективность действующих организационно-технических мер по защите информационной системы организации. Уровень обеспечения информационной безопасности различается в зависимости от конкретно рассматриваемой компании, но должен соответствовать некоторому минимальному набору требований безопасности [1, 11-14]. Данные требования, вырабатывались в течение многих лет компаниями-разработчиками и исследовательскими институтами, а также профессионалами в области защиты информации объединяются в своды правил и стандартизируются на государственном уровне. Сегодня существует ряд стандартов в области информационной безопасности, наиболее известны - международный стандарт ISO/IEC 27001:2005, содержащий требования по созданию системы управления информационной безопасностью компании, и «производные» от него [13].

Основной задачей аудита является подтверждение конфиденциальности, целостности и доступности информации, обрабатывающейся в корпоративной системе предприятия.

Аудит на соответствие требованиям информационной безопасности – это комплексный, циклический процесс, который состоит из следующих этапов:

планирование аудита;

планирование мероприятий по аудиту (разработка, согласование и утверждение планов мероприятий);

проверка на соответствие группе требований (например, на соответствие стандарту ISO/IEC 27001:2005);

систематизация результатов обследования и формирование отчетности.

Эти четыре этапа составляют жизненный цикл аудита [3,7]. Рассмотрим их подробнее.

Жизненный цикл аудита информационной безопасности

Наиболее сложным этапом является практическое проведение аудита, так как российских стандартов в этой области нет, следовательно, законодательной базой, которая легла бы в основу методики поведения аудита системы управления информационной безопасностью, могут стать стандарты серии ISO 270xx, часть из которых адаптирована в России [2-5, 13]. Рассмотрим более подробно указанный выше этап.

Непосредственно перед проведением аудита аудиторская группа должна иметь четко сформулированные задачи аудита и его область, критерии аудита, документы различных уровней (политики, процедуры, инструкции, стандарты организации и др.), перечень процессов и активов компании, подлежащих проверке, согласованную программу аудита от проверяемой организации, подтверждение проведения аудита.

Аудит начинается со вступительного совещания с представителями организации, на котором обсуждается повестка дня, программа аудита. После этого аудиторы начинают проверять организацию. Аудит документации является первым этапом проверки на соответствие требования. Вначале проверяются документы верхнего уровня: политика информационной безопасности или концепция информационной безопасности, частные политики, стандарты организации. Перечисленные документы должны отражать не только идеологию организации в целом в области информационной безопасности, но и отражать распределение ответственности между сотрудниками и руководством организации. Обязательно необходимо проверять осведомленность о содержании этих документов у сотрудников проверяемой организации и понимание целей, принципов и обязательства по защите активов организации, используемых конкретным подразделением компании. Проверку документов нижних уровней целесообразно проводить на месте, т.е. при проверке конкретных процессов или мер по обеспечению безопасности.

Аудитор должен поочередно пройти каждое заявленное в программе подразделение и проверить выполнение необходимых требований. В ходе проверки может быть использовано интервьюирование, частичная проверка процесса, проверка с помощью выборки (проверка выполнение в определенные промежутки времени), либо полная проверка всех составляющих процесса.

При рассмотрении стандарта ГОСТ Р ИСО/МЭК 27001-2006 – российского аналога ISO/IEC 27001:2005 логичным будет анализ доменов, приведенных в стандарте:

уязвимости политики безопасности;

уязвимости организационных мер;

уязвимости классификации и контроля ресурсов;

уязвимости процедур, связанных с персоналом;

уязвимости физической безопасности;

уязвимости эксплуатации систем;

уязвимости контроля доступа;

уязвимости обслуживания и разработки систем;

уязвимости обеспечения непрерывности бизнеса;

уязвимости инцидентов информационной безопасности [9].

В процессе аудита важным фактором является сбор фактов и свидетельств для последующего анализа и отчета. Свидетельства всегда должны быть объективными, аудитор не должен использовать собственную фантазию для получения картины происходящего. Свидетельство может быть получено посредством наблюдения, измерения, испытания или любым другим разумным способом. Хорошей практикой является открытость аудитора и умение задавать правильные вопросы, которые мотивируют интервьюируемого рассказать о процессе либо пояснить требуемые детали.