Продовження табл. 1

1	2	3	4	5
Систолічні процесори	25-30 %	До 50 %	25-30 %	до 1 %
Сигнальні процесори	25-30 %	25-30 %	25-30 %	до 1 %
Нейрон-сигнальні процесори	25-30 %	10-15 %	25-30 %	до 1 %
ПЛІС	25-30 %	10-15 %	10-15 %	менше 1 %

Висновки

Отже, одним із шляхів підвищення надійності апаратних реалізацій штучних нейронних мереж є використання ПЛІС-технологій. Використання зазначеної елементної бази дозволяє знизити ризик відмови системи через апаратні складові.

Сучасній ПЛІС-технології притаманні низька вартість, висока гнучкість та відмовостійкість, а тому вона є одним з ефективних засобів реалізації нейрокомп'ютерів.

Література

1. Сравнительный анализ применения ПЛИС и микропроцессоров при разработке информационно-управляющих систем, важных для безопасности АЭС // Научно-технический отчет. НАУ им. Н.Е. Жуковского «ХАИ», НТСКБ «Полисвит», ИПМЭ им. Г.Е. Пухова НАН Украины, ИПММС НАН Украины. – 2005. – С. 47.

2. Гриняев С. Нейронные процессоры // Компьютерра. – 2001. – № 38. – http://pgpu.penza.com.ru/_sites/intel/MATVEYEV_DM/materials/article_neyroprointel.html

3. Аляутдинов М.А. Нейрокомпьютеры. От программной к аппаратной реализации / Аляутдинов М. А., Галушки А. И., Казанцев П. А., Остапенко Г. П.. – СПб: «Горячая линия – Телеком», 2008 г. – 393 с.

4. Круг П.Г. Нейронные сети и нейрокомпьютеры / Круг П.Г.. – Москва: МЭИ, 2002 – 177 с.

5. Шахнов В. Нейрокомпьютеры – архитектура и реализация / Шахнов В., Власов А. Кузнецов А // http://chipnews.gaw.ru/html.cgi/archiv/00_07/stat_36.htm

6. Сергиенко А.М. VHDL для проектирования вычислительных устройств / Сергиенко А.М. – К.: ЧП «Корнейчук», ООО «ТИД ДС», 2003 г. – 187 с.

7. Федухин А.В. ПЛИС-системы как средство повышения отказоустойчивости / Федухин А.В., Муха А.А., Муха А.А // Математичні машини і системи. – 2010. – № 1. – С. 198-204.

Надійшла 5.11.2010 р.

УДК 681.5

В.С. ХАРЧЕНКО, О.Н. ОДАРУЩЕНКО, О.В. ИВАНЧЕНКО
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»
Полтавский национальный технический университет им. Юрия Кондратюка
Севастопольский национальный технический университет

ПРИНЦИПЫ АНАЛИЗА И УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Рассмотрены принципы анализа и обеспечения безопасности критических инфраструктур. Обоснована целесообразность управления критическими инфраструктурами по мегасостоянию. В качестве методологической основы предложено использовать метод FMECA-анализа.

The principles of analysis and safety of system of systems were considered. The practicability of controlling the critical infrastructures by the megastate were proved. The method of FMECA – analysis was submitted as a methodological base.

Ключевые слова: безопасность, критическая инфраструктура, FMECA-анализ, эшелонирование защит, мегасостояние.

Введение. На сегодняшний день проблема безопасности критических инфраструктур (КИ) приобрела интернациональный характер. О степени критичности различных инфраструктурных образований свидетельствуют:

- последствия деятельности вулкана в Исландии, парализовавшего практически всю авиационную инфраструктуру Европы (2010 г.);
- авария на Саяно-Шушенской ГЭС (Россия, 2009 г.), вызвавшая техногенную катастрофу;
- аварии энергетических систем США и Канады (2003 г.) и т.д.

Проблема обеспечения безопасного функционального применения различных инфраструктур, а

также осознание того факта, что отказ элементов КИ может привести к человеческим жертвам, серьезным экологическим последствиям или финансовым потерям обусловили актуальность применения формальных методов оценки, основанных на выявлении потенциальных опасностей и оценки рисков их возникновения [1– 3].

В настоящее время все чаще анализ опасностей и рисков представляют не только в количественной форме, как последовательность расчетных значений соответствующих показателей, но и в форме качественного или комбинированного качественно-количественного анализа. При этом сами результаты качественного анализа представляются в виде текстового описания, таблиц, диаграмм, экспертных оценок и т.д. Однако и этот подход не всегда дает положительный результат.

На наш взгляд, одной из важнейших причин этого является отсутствие обоснованной теории анализа безопасности КИ; недостаточное понимание самих принципов анализа и обеспечения безопасной эксплуатации различных инфраструктур.

Постановка задачи. Целью работы является формирование основных принципов анализа безопасности критических инфраструктур на основе детализации множества видов, последствий отказов или иных событий, влияющих на безопасность, элементов (систем) инфраструктуры с учетом возможностей управления их состоянием на соответствующем уровне иерархии.

Результаты исследования. *Принципы анализа безопасности критических инфраструктур* заключаются в следующем:

1. Инфраструктура представляет собой множество взаимодействующих сложных систем S_i, $i = 1,...,n$. Каждая из систем может быть описана таблицей (или иерархией таблиц) FMECA, TF_i, или ее обобщением EMECA, TE_i. Степень детализации множества видов и последствий отказов (событий) каждой из систем определяется уровнем управления ее состояниями. Каждой строке таблицы TF_i (TE_i) ставится в соответствие состояние F_{ij}, $j = 1,...,m_j$.

Следовательно, множество состояний системы S_i включает работоспособное состояние (состояния) F_{io}, состояния с единичными отказами (событиями) F_{ij} и, при необходимости, состояния с кратными отказами (событиями) $F_{ij}^{(h)}$ (в общем случае $h = 2,...,m_j$:

$$MF_i = \left\{F_{io}, F_{ij}, F_{ij}^{(h)}\right\}.$$

2. Каждому состоянию F_{ij} (также как и $F_{ij}^{(h)}$) по правилам техники FMECA (EMECA) ставится в соответствие вероятность P_{ij} и тяжесть W_{ij} данного отказа (события). Их произведение определяет степень его критичности

$$R_{ij} = P_{ij} \cdot W_{ij}.$$

Результаты FMECA (EMECA)-анализа (соответствующие таблицы) свертываются в двумерные (или трехмерные при учете времени восстановления) матрицы критичности размерностью *a* x *b*, где *a* и *b* – количество строк и столбцов, определяемых шкалами задания значений вероятности P_{ij} (p) и тяжести W_{ij} (w):

$$MR_i = \left\| R_{ij}(p, w) \right\|.$$

В матрице MR_i задается диагональ критичности. Если существуют элементы, находящиеся над диагональю (неприемлемые риски, $R_{ij} > R_{i_{непр}}$), то необходимы корректирующие действия C_{ij}, обеспечивающие снижение рисков до приемлемого уровня.

На уровне системы S_i может быть поставлена и решена задача локальной оптимизаци состава и объема корректирующих действий C_{ij} (методы и средства снижения рисков) по критерию «приемелемые риски-минимум затрат».

3. Для каждой строки $FMECA_i$ ($EMECA_i$)-таблицы системы S_i определяется степень (вероятность) влияния соответствующего отказа (события) и перехода в состояние F_{ij} на состояния F_{kg} других систем инфраструктуры S_k ($k = 1,...,n, k \neq i, g = 1,...,m_g$).

Это влияние на состояние F_{kg} может быть следующим:

1) отказ (событие) F_{ij} приводит к изменению (увеличению или уменьшению) вероятности P_{kg};

2) отказ (событие) F_{ij} приводит к изменению (увеличению или уменьшению) тяжести W_{kg};

3) отказ (событие) F_{ij} вызывает появление нового (неспецифицированного ранее) отказа (события)

F_{kmg+1};

4) отказ (событие) F_{ij} приводит к комбинации событий 1– 3;

5) отказ (событие) F_{ij} не влияет на состояние F_{kg}.

Исходя из изложенного, влияние системы S_i на систему S_k можно описать с помощью матрицы

$$MD_{ik} = \left\| d_{jg}^{ik} \right\|,$$

где d_{jg}^{ik} – вектор, учитывающий влияние F_{ij} на F_{kg}; этот вектор может быть представлен следующим образом:

$$d_{jg}^{ik} = \left\langle \left(x_{jg1}^{ik}, L_{jg1}^{ik}\right), \left(x_{jg2}^{ik}, L_{jg2}^{ik}\right), \left(x_{jg3}^{ik}, L_{jg3}^{ik}\right), \left(x_{jg4}^{ik}, L_{jg4}^{ik}\right) \ldots \right\rangle,$$

причем, $x_{jgz}^{ik} = 1(0)$, если реализуется (не реализуется) соответствующий вариант z влияния F_{ij} на F_{kg}, z = 1,…,5 (единице может быть равна только одна переменная x_{jgz}^{ik}); L_{jgz}^{ik} – оператор, характеризующий вероятность и степень влияния (если $x_{jgz}^{ik} = 0$, то $L_{jgz}^{ik} = \varnothing$).

4. Описание поведения и взаимного влияния систем может быть привязано ко времени. Во времени могут изменяться параметры и значения функции риска R_{ij} и элементы вектора матрицы влияния D_{ik}. На основе матриц рисков для систем MR_i может быть построена итоговая матрица MR рисков для инфраструктуры, элементы которой также изменяются во времени.

Принципы обеспечения безопасности можно сформулировать следующим образом:

1. Для устойчивого и безопасного функционирования инфраструктуры необходимо, чтобы:

а) либо каждая из систем выполняла функцию «фильтрации» рисков, связанных с отказами (событиями) других систем; в этом случае реализуется принцип естественного эшелонирования защиты;

б) либо обеспечивалось снижение рисков по каждому из отказов (событий) до приемлемого уровня на всем множестве систем; при этом может быть поставлена и решена задача покрытия по всем траекториям (цепочкам) влияния;

в) либо существовала специальная система инфраструктурной безопасности SS, контролирующая уровень рисков и обеспечивающая его снижение до приемлемого уровня. Эта система должна состоять из подсистем безопасности каждой из систем SS_i или их групп, которые контролируют уровни рисков соответствующих систем и либо снижают их до приемлемого значения, либо информируют систему безопасности верхнего уровня.

Возможны варианты построения распределенных адаптивных систем безопасности, построенных по принципу эшелонирования защиты, защиты «в глубину».

2. Обязательным принципом, который должен реализовываться при создании и модернизации критических инфраструктур, является принцип диверсности. Он реализуется в системах S_i (локальная диверсность) и на инфраструктурном уровне (глобальная диверсность).

При этом следует рационально распределять и сочетать виды, методы и средства реализации процессно-продуктной диверсности на разных уровнях инфраструктуры, оптимизируя применяемые многоверсионные технологии для разработки информационно-управляющих систем по критерию «надежность-безопасность-стоимость» [4].

3. Задача обеспечения безопасности КИ решается в комплексе с задачами по обеспечению требуемого (максимального) уровня показателей по другим свойствам (безотказности, готовности, живучести). Учитывая, что критические инфраструктуры являются обслуживаемыми и, как правило, относятся к объектам высокой готовности [5] (или к таковым относятся отдельные системы КИ), целесообразно в качестве общего критерия оптимизации использовать критерий "требуемая безопасность (приемлемый риск) – максимальная готовность".

4. Для инфраструктур, допускающих деградацию, возможно применение принципа технического каннибализма, предполагающего использование ресурсов отказавших систем КИ в интересах других систем для минимизации общего уровня снижения функциональности или безопасности. Этот принцип может быть применен в контексте трансформации критических инфраструктур [6].

Принципы управления безопасностью критических инфраструктур можно изложить следующим образом:

1. На основании рассмотренных принципов анализа предлагается организовать управление КИ на всех возможных уровнях иерархии с учетом влияния множества факторов, включая функциональную и информационную составляющую обеспечения безопасности. Такой подход, на наш взгляд, можно реализовать путем перехода к управлению КИ по мегасостоянию.

Под мегасостоянием (МГС) Φ критической инфраструктуры будем подразумевать вектор-функцию состояний систем инфраструктуры, определяемую с учетом условий, способов обеспечения эффективного и

безопасного использования по назначению инфраструктуры в целом. Задача управления формулируется с учетом представления инфраструктуры в следующем виде:

$$\Phi = \{L, F, E, U, S, SS, I\},$$

где L – множество задач, решаемых КИ;

F – множество технических состояний, в которых может находиться КИ;

E – множество режимов эксплуатации КИ;

U – множество стратегий управления по МГС;

S – множество систем КИ;

SS – система безопасности;

I – множество видов информационных воздействий на системы КИ.

2. Управление безопасностью критической инфраструктурой по мегасостоянию базируется на известных принципах и стратегиях гибкого управления готовностью по техническому состоянию [7] или управления гарантоспособностью информационно-управляющих систем по информационно-техническому состоянию [8].

3. Управление безопасностью и другими свойствами критической инфраструктуры должно осуществляться в контексте ее эволюции, обусловленной изменением требований к системам, характеристик внешней среды и др.

Заключение. В данной работе представлены ряд принципов анализа, управления безопасностью и готовностью критических инфраструктур. Результаты комбинированного (количественного и качественного) анализа видов, последствий отказов или других событий, влияющих на безопасность, могут быть представлены в таблично-матричной форме, удобной для последующей обработки.

С учетом полученных матриц формулируется задача глобальной оптимизации корректирующих действий, которая может представлять собой суперпозицию задач локальной оптимизации по обеспечению безопасности критических инфраструктур и управления безопасностью по фактическому МГС.

Дальнейшие исследования могут быть направлены на:

- разработку детальных моделей технического (информационно-технического) состояния инфраструктур;
- постановку, решение задач управления безопасностью и готовностью КИ по мегасостоянию;
- архитектурированию систем безопасности КИ и др.

Литература

1. Тарасюк О. М. Формальные методы разработки критического программного обеспечения. Лекционный материал / О. М. Тарасюк, А. В. Горбенко; [под ред. Харченко В. С.]. – Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2009. – 214 с.

2. IEC 812. Analysis Techniques for System Reliability – Procedure for Failure Modes and Effects Analysis (FMEA). – Geneva: International Electrotechnical Commission, 1985. – 41 p.

3. H. Sozer, B. Tekinerdogan, M. Aksit. Reliability Analysis at the Software Architecture Design Level using Enhanced Failure Modes and Effects Analysis Approach. LNCS 4174, Architecting Dependable Systems IV / R. de Lemos et al. (eds.). – Springer, 2007. – P. 132– 157.

4. Kharchenko V.S., Sklyar V.V. (edits). FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment. – RPC “Radiy”, National Aerospace University “KhAI”, State Centre on Nuclear and Radiation Safety, 2008. – 188 p.

5. Технологии высокой готовности для программно-технических комплексов космических систем / [под ред. Харченко В. С., Конорева Б. М.]. – Харьков: Государственный центр регулирования качества поставок и услуг, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2010. – 369с.

6. Kharchenko V., Sklyar V., Odaruschenko O., Dependable Computing Systems for Supporting Transformation of the Force Information Infrastructure // Information & Security, 2007, vol. 22. – P.75– 91.

7. Волков Л. И. Управление эксплуатацией летательных комплексов / Л. И. Волков. – М.: Машиностроение, 1981. – 289 с.

8. Харченко В. С. Гарантоздатні системи та багатоверсійні обчислення в контексті еволюції / В. С. Харченко // Радіоелектронні та комп’ютерні системи. – 2009. – № 7. – С. 12– 27.

Надійшла 14.11.2010 р.