УДК 004.05

В.В. СКЛЯР

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина

ЭЛЕМЕНТЫ МЕТОДОЛОГИИ АНАЛИЗА ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Предложены элементы методологии анализа функциональной безопасности информационно-управляющих систем (ИУС), включающие: принципы анализа функциональной безопасности ИУС, теоретико-множественную модель и ER-модель рисков, процедуру сравнительного анализа рисков, теоретико-множественную и вероятностную модели эшелонирования защиты активов, метод повышения функциональной безопасности ИУС.

Ключевые слова: *функциональная безопасность, анализ рисков, информационно-управляющая система.*

Введение

Безопасность (свобода от неприемлемого риска) является важнейшим свойством критических объектов. В самом определении безопасности заложены два термина, являющихся весьма важными для построения методологии обеспечения и оценки безопасности.

Это, во-первых, понятие риска. Риск – комбинация (произведение) вероятности P(t) возникновения ущерба и его последствий C: $R(t) = P(t) \cdot C$. В частном случае, когда последствие конкретно и измеряется по типу «Да/Нет», «Происходит/Не происходит», тогда риск становится численно равен вероятности P(t) возникновения ущерба: $R(t) = P(t)$.

Во-вторых, поскольку риск возможно измерить, важным является установление его приемлемого уровня, который является достижимым с технической точки зрения и основан на текущих ценностях общества [1].

Для информационно-управляющих систем (ИУС) критических объектов, которые сами по себе опасности не несут, а лишь выполняют функции, важные для безопасности критических объектов, рассматривается свойство функциональной безопасности. Функциональная безопасность (functional safety) – часть безопасности, относящаяся к управляемому оборудованию и управляющей системе, которая зависит от правильного функционирования электрических, электронных и программируемых электронных систем, связанных с безопасностью, других связанных с безопасностью технологических систем и оборудования для снижения внешнего риска (согласно стандартам серии МЭК 61508 «Функциональная безопасность электрических, электронных и программируемых систем, важных для безопасности»). Понятие функциональной безопасности (ФБ) включает в себя функции безопасности и целостность (интегрированность) безопасности. Целостность безопасности (safety integrity) – вероятность того, что система, связанная с безопасностью, удовлетворительно выполняет заданные функций безопасности во всех установленных условиях в пределах установленного периода времени [2].

В качестве показателей ФБ могут рассматриваться риски (с учетом значений ущерба либо как вероятности неблагоприятных событий).

Кроме того, могут применяться детерминированные критерии ФБ, которые устанавливают требования, которым должна соответствовать система (например, требования к наличию резервированных каналов, требования к испытательным значениям климатических, радиационных, механических и др. воздействий и т.д.) [3].

Понятие ФБ было сформулировано и раскрыто около 10 лет назад в стандартах серии МЭК 61508. Несмотря на исключительную важность для теории и практики, на сегодняшний день не существует удовлетворительной методологии анализа ФБ ИУС.

В данной статье предлагаются элементы методологии анализа ФБ ИУС.

– принципы анализа ФБ ИУС;

– теоретико-множественную модель и ER-модель рисков;

– процедуру сравнительного анализа рисков;

– теоретико-множественную и вероятностную модели эшелонирования защиты активов;

– метод повышения ФБ ИУС.

Некоторые составляющие методологии (теоретико-множественная модель рисков, процедура сравнительного анализа рисков, модели эшелонирования защиты активов) изложены в работе [4].

Поэтому в данной статье детально рассмотрены принципы анализа ФБ ИУС, ER-модель рисков, а также метод повышения ФБ ИУС.

1. Принципы анализа функциональной безопасности ИУС

Принципы анализа функциональной безопасности ИУС включают:

1) принцип многоуровневости – при анализе функциональной безопасности рассматриваются несколько уровней «сверху-вниз»: уровень критического объекта, уровень ИУС, уровень компонентов ИУС, и, возможно, уровень внутренней структуры компонентов ИУС, если такая требуется такая детализация;

2) принцип поуровневой унификации – при анализе функциональной безопасности на каждом из уровней рассматриваются одни и те же сущности (активы, опасности, ущерб, риски, контрмеры по защите активов) и одинаковая структура связей между сущностями;

3) принцип единства функциональной и информационной безопасности – анализ ФБ и информационной безопасности (ИБ) основывается на унифицированных сущностях; различие между ИБ и ФБ заключается в том, для каких активов обеспечивается безопасность: ИБ рассматривается, когда активами является информация, а ФБ рассматривается, когда активом является критический объект контроля и управления.

Кроме того, к принципам анализа ФБ следует также отнести известный принцип ALARA (as low as reasonably applicable – разумная достаточность) – подход к управлению риском, который подразумевает его максимально возможное снижение, достигаемое за счет ограниченных ресурсов.

2. ER-модель рисков

Для описания исследуемой области наиболее подходящей является модель «сущность–связь» или «Entity–Relationship» (сокращенно ER-модель), широко применяемая для разработки баз данных.

ER-модель модель рисков приведена на рис. 1. В отличие от теоретико-множественных моделей рисков для отдельных уровней, ER-модель модель рисков позволяет представить все уровни анализа ФБ одновременно. В соответствие с принципом многоуровневости данная модель включает две сущности, соответствующие уровням анализа ФБ: уровень активов и уровень ИУС. В соответствие с принципом поуровневой унификации для каждой из сущностей используются одинаковые атрибуты: активы (для уровня ИУС активами являются функции безопасности), опасности, риски и контрмеры. Связь между сущностями осуществляется между атрибутом «контрмеры» уровня активов и атрибутом «функции безопасности» уровня ИУС. Тип всех связей на рис. 1 установлен как «многие–ко–многим». Объекты, включаемые в состав ER-модели, могут иметь сложную многоуровневую структуру, например, представлять собой набор моделей и методов, применяемых для анализа опасностей или рисков. При необходимости в ER-модель рисков могут быть включены уровни аппаратных и программных и компонентов. Проведенный анализ показал, что развивать ER-модель рисков в глубину целесообразно лишь тогда, когда выполняются следующие два условия:

1) когда компоненты нижнего уровня являются контрмерами по обеспечению ЦБ верхнего уровня;

2) когда контрмеры ЦБ верхнего уровня являются активами для компонентов нижнего уровня.

Для сравнительного анализа объектов, описываемых ER-моделью рисков могут быть применены операции реляционной алгебры.

Реляционная алгебра включает четыре теоретико-множественные операции (объединение, пересечение, разность и расширенное декартово произведение), а также четыре специальные операции (фильтрация, проектирование, условное соединение и деление). Проведенный анализ показал, что для анализа контрмер по снижению рисков целесообразно применение операций объединения, пересечения, разности и фильтрации. Дадим формальное определение и интерпретацию операциям реляционной алгебры, применимым к модели рисков.

1. Объединение. Результатом данной операции является отношение, содержащее множество кортежей, принадлежащих либо первому, либо второму исходным отношениям, либо обоим отношениям одновременно.

$$Re1 \cup Re2 = \{ re \mid re \in Re1 \vee re \in Re2 \},$$

где $Re1 = \{ re1 \}$, $Re2 = \{ re2 \}$ – исходные отношения;

re1, re2 – кортежи исходных отношений;

re – кортеж отношения, полученного в результате выполнения операции.

Операция объединения применяется для определения полного набора компонентов модели рисков в составе нескольких ИУС.

2. Пересечение. Результатом данной операции является отношение, содержащее множество кортежей, принадлежащих и первому, и второму исходным отношениям.

$$Re1 \cap Re2 = \{ re \mid re \in Re1 \wedge re \in Re2 \}.$$

Операция объединения применяется для определения компонентов модели рисков, которые являются общими для нескольких ИУС.

3. Разность. Результатом данной операции является отношение, содержащее множество кортежей, принадлежащих первому, и не принадлежащих второму исходным отношениям:

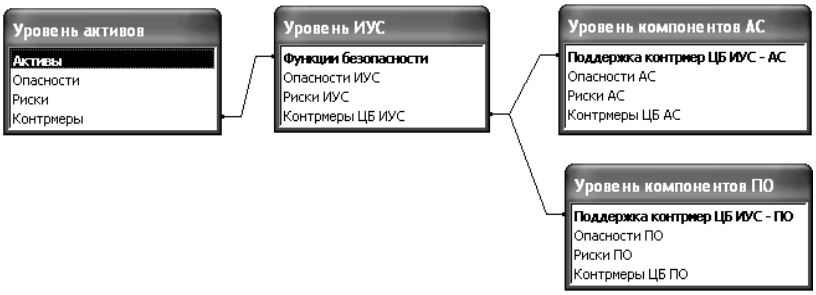

Рис. 1. ER-модель рисков для уровня активов, уровня ИУС и уровня компонентов ИУС

$Re1 \setminus Re2 = \{ re \mid re \in Re1 \wedge re \notin Re2 \}$;

$Re2 \setminus Re1 = \{ re \mid re \in Re2 \wedge re \notin Re1 \}$.

В отличие от других теоретико-множественных операций, операция разности не является коммутативной, т.е. ее результат зависит от порядка аргументов.

Операция разности применяется для определения различий между компонентами модели рисков в составе нескольких ИУС.

4. Фильтрация. Результатом данной операции является отношение, содержащее те кортежи из исходного отношения, для которых истинно условие фильтрации (выбора).

$Re[a(re)] = \{ re \mid re \in Re \wedge a(re) = \text{“ИСТИНА”} \}$,

где a – булевское выражение, составленное из термов сравнения с помощью операторов булевой алгебры.

Операция фильтрации применяется для определения компонентов модели рисков, соответствующих заданным условиям применения.

3. Метод анализа функциональной безопасности ИУС

Метод анализа ФБ ИУС (рис. 2) интегрирует принципы, модели и процедуры, разработанные в рамках методологии.

Исходными данными для реализации метода является информация об активах, безопасность которых следует обеспечить. Метод анализа ФБ ИУС включает следующие этапы.

1. Выполняется анализ опасностей, и согласно формируется множество опасностей для активов

$$H = \{h_1,...,h_i,...,h_P\}.$$

2. Выполняется идентификация рисков, и согласно формируется множество рисков для активов

$$R = \{r_1(t),...,r_j(t),...,r_M(t)\}.$$

3. Для диапазона рисков больше или равного уровню неприемлемого риска R_N согласно принципу ALARA выполняется процедура П1, заключающаяся в выборе таких контрмер для снижения риска, для которых при заданном снижении риска стоимость будет минимальной.

4. Для диапазона рисков ниже уровня неприемлемого риска R_N согласно принципу ALARA выполняется процедура П2, заключающаяся в выборе таких контрмер для снижения риска, для которых при заданном уровне стоимости снижение риска будет максимальным.

5. Устанавливаются функции безопасности активов, которые будут выполняться посредством ИУС, и согласно формируется множество функций безопасности, выполняемых ИУС

$$SF = \{sf_1,...,sf_p,...,sf_Q\}.$$

6. Проверяется соблюдение ограничений для контрмер по снижению риска $\Delta R \geq R_{\text{заданное}}$ и по стоимости $C \leq C_{\text{заданное}}$. Если ограничения не выполняются, то необходимо вернуться к шагу 1. Если ограничения выполнены, то следует продолжить выполнения метода, перейдя к шагу 7. По результатам выполнения шагов 1-6 формируется содержание модели рисков верхнего уровня.

7. Контрмеры, включая ИУС, распределяются по эшелонам защиты активов, и формируется множество эшелонов защиты активов

$$B = \{B_1,...,B_i,...,B_N\}$$

и множества контрмер, включая функции безопасности, выполняемых i-м эшелоном защиты

$$CM_i = \{cm_{i1},...,cm_{ij},...,cm_{iM}\}.$$

8. Выполняется анализ опасностей ИУС, и формируется множество опасностей для выполнения функции безопасности ИУС

$$H_{I\&C} = \{h_{I\&C\ 1},...,h_{I\&C\ i},...,h_{I\&C\ L}\}.$$

9. Выполняется идентификация рисков ИУС, и согласно формируется множество рисков выполнения функций безопасности ИУС

$$R_{I\&C} = \{r_{I\&C\ 1}(t),...,r_{I\&C\ j}(t),...,r_{I\&C\ M}(t)\}.$$

10. Для диапазона рисков ИУС больше или равного уровню неприемлемого риска R_N согласно принципу ALARA выполняется процедура П1, заключающаяся в выборе таких средств обеспечения целостности безопасности ИУС, для которых при заданном снижении риска стоимость будет минимальной.

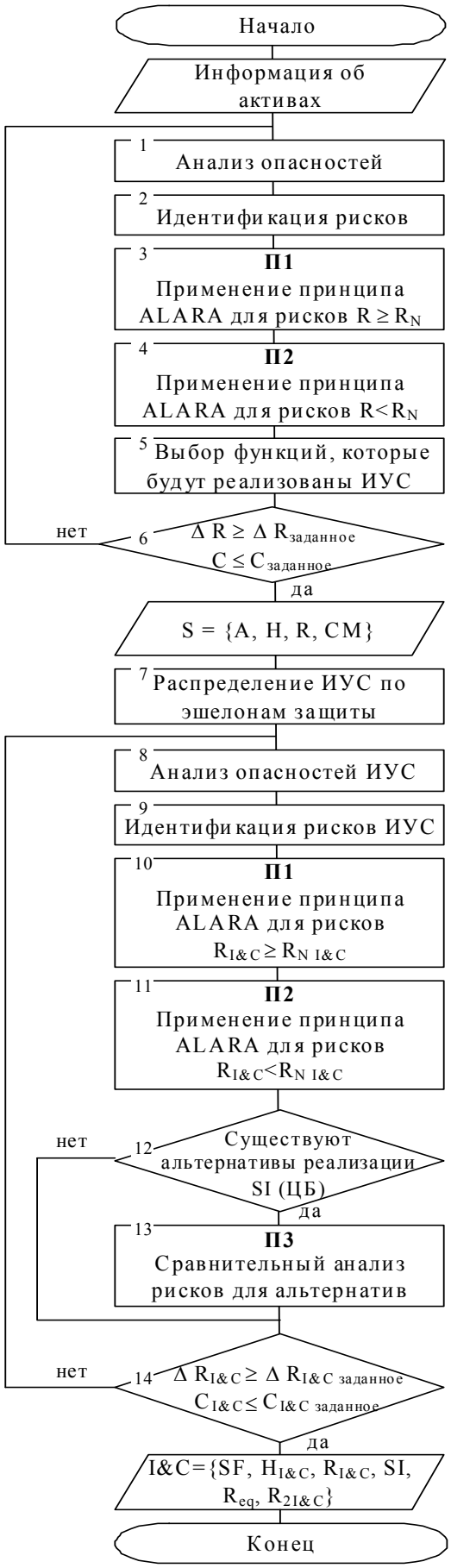

Рис. 2. Этапы метода анализа функциональной безопасности ИУС

11. Для диапазона рисков ИУС ниже уровня неприемлемого риска R_N согласно принципу ALARA выполняется процедура П2, заключающаяся в выборе таких средств обеспечения целостности безопасности ИУС, для которых при заданном уровне стоимости снижение риска будет максимальным.

12. Проверяется наличие альтернатив реализации множества средств обеспечения целостности безопасности ИУС $SI = \{si_1,...,si_k,...si_N\}$. Если таких альтернатив нет, то необходимо перейти к выполнению шага 14. Если альтернативы существуют, то следует перейти к выполнению шага 13.

13. Выполняется процедура П3 сравнительного анализа риска для альтернатив.

14. Проверяется соблюдение ограничений для средств обеспечения целостности безопасности ИУС по снижению риска $\Delta R_{I\&C} \geq R_{I\&C\ заданное}$ и по стоимости $C_{I\&C} \leq C_{I\&C\ заданное}$. Если ограничения не выполняются, то необходимо вернуться к шагу 8. Если ограничения выполнены, то следует закончить выполнения метода. По результатам выполнения шагов 7-14 формируется содержание модели рисков нижнего уровня.

Заключение

В статье впервые предложена методология анализа ФБ ИУС, которая, в отличие от известных, базируется на структурном, теоретико-множественном и реляционном представлении модели рисков, процедурах оптимизации согласно принципу ALARA (as low as reasonably applicable – разумная достаточность) и сравнительного анализа рисков, что формирует единый подход к оценке и обеспечению функциональной и информационной безопасности, а также позволяет выбирать набор контрмер и информационных технологий для снижения рисков.

Литература

1. Минаев В.А. Теоретические основы информатики и информационная безопасность / В.А. Минаев, В.Н. Саблин. – М.: Радио и связь, 2000. – 451 с.

2. Хохлов Н.В. Управление риском / Н.В. Хохлов. – М.: ЮНИТИ-ДАНА, 2001. – 239 с.

3. Дубров А.М. Моделирование рисковых ситуаций в экономике и в бизнесе / А.М. Дубров, Б.А. Лагоша, Е.Ю. Хрусталев, Т.П. Барановская; под ред. Б.А. Лагоша. – М.: Финансы и статистика, 2001. – 224 с.

4. Скляр В.В. Оценка качества и экспертиза программного обеспечения: Лекционный материал / В.В. Скляр; под ред. В.С. Харченко – Х.: Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2008. – 204 с.

Поступила в редакцию 2.03.2009

Рецензент: д-р техн. наук, проф., зав. кафедрой компьютерных систем и сетей В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского, Харьков, Украина.

ЕЛЕМЕНТИ МЕТОДОЛОГІЇ АНАЛІЗУ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ

В.В. Скляр

Запропоновано елементи методології аналізу функціональної безпеки інформаційно-управляючих систем (ІУС), що включають: принципи аналізу функціональної безпеки ІУС, теоретико-множинну модель і ER-модель ризиків, процедуру порівняльного аналізу ризиків, теоретико-множинну та імовірнісну моделі ешелонування захисту активів, метод підвищення функціональної безпеки ІУС.

Ключові слова: функціональна безпека, аналіз ризиків, інформаційно-управляюча система.

METHODOLOGY ELEMENTS OF FUNCTIONAL SAFETY ANALYSIS OF INSTRUMENTATION AND CONTROL SYSTEMS

V.V. Sklyar

Methodology elements of functional safety analysis of Instrumentation and Control (I&C) systems are proposed. These methodology elements include the following: principles of functional safety analysis of I&C systems, a theoretical-set model and an ER-model of risks, a procedure of comparative risks analysis, theoretical-set and probabilistic models of actives defense in depth, a method of increasing functional safety of I&C systems.

Key words: functional safety, risks analysis, Instrumentation and Control system.

Скляр Владимир Владимирович – канд. техн. наук, доцент, доцент кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: vvsklayr@mail.ru.