СПИСОК ЛИТЕРАТУРЫ

1. *Бейзер Б.* Тестирование черного ящика. Технологии функционального тестирования программного обеспечения и систем. СПб.: Питер, 2004.
2. *Калбертсон Р., Браун К., Кобб Г.* Быстрое тестирование. М.: Издательский дом «Вильямс», 2002.
3. *Козиол Д., Личфилд Д., Эйтэл Д., Энли К., Эрен С., Мехта Н., Хассель Р.* Искусство взлома и защиты системы. СПб.: Питер, 2006.
4. *Соммервилл И.* Инженерия программного обеспечения. 6-е изд. М.: Издательский дом «Вильямс», 2002.

И. В. Машкина (к. т. н., доцент), М. Б. Гузаиров (д. т. н., профессор)
Уфимский государственный авиационный технический университет

МЕТОДЫ РАЗРАБОТКИ ФУНКЦИОНАЛЬНОЙ МОДЕЛИ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ

На сегодняшний день реальная практика менеджмента информационной безопасности (ИБ) в большинстве случаев сводится к наборам правил, в соответствии с которыми функционирует отдел ИБ, наборам положений и инструкций, которые слабо структурированы и взаимосвязаны.

Это обусловлено отсутствием понятия функциональной модели управления ИБ.

С помощью моделирования менеджмента ИБ можно эффективно анализировать проблемы управления и оптимизировать затраты на защиту информации. В работе предлагается подход к разработке математического метода принятия решений по организационно-техническому управлению защитой информации (ЗИ), построению модели системы управления (СУ) ЗИ с использованием IDEF-BPWin технологии.

1. Задача принятия решений по управлению модульным составом СЗИ и метод ее решения

В течение периода эксплуатации объекта информатизации (ОИ), как правило, неоднократно изменяются планы обработки информации и соответствующие им требования к уровню защищенности [1]. К тому же постоянно происходит обновление информационной системы, изменяется ее структура, используются новые ИТ, организуются новые подключения к системе. Учет этих факторов требует разработки новых подходов к обеспечению ЗИ.

Таким подходом может быть проектирование системы защиты информации (СЗИ), свойства и параметры которой динамично изменяются в зависимости от уровня критичности информации, обрабатываемой в данный период времени на объекте защиты.

Для этого должны быть реализованы механизмы *организационно-технического управления* (ОТУ) ЗИ, одной из задач которых является *обоснование наборов средств защиты*, используемых в СЗИ в определенные периоды функционирования ОИ.

Для совершенствования, развития и повышения эффективности СЗИ необходимы разработка и практическое применение методического обеспечения, связанного с решением задач проектирования СЗИ и организационно-технического управления защитой информации: синтез структуры и разработка алгоритмов функционирования системы поддержки принятия решений (ПР) для системы ОТУ ЗИ.

В работе используется идея морфологического подхода для моделирования и синтеза рациональных наборов средств защиты (СрЗ) для СЗИ.

Морфологический метод синтеза целесообразно использовать при проектировании СЗИ и в процессе ОТУ ЗИ [2], поскольку данный метод позволяет реализовать многоальтернативный и многокритериальный выбор, когда система представляет собой сложный комплекс СрЗ, включающий в себя наборы средств защиты для определенных точек их установки на объекте защиты; каждый набор

синтезируется из некоторого множества функциональных подсистем (ФП) защиты, и каждая ФП имеет более одной элементарной альтернативы для ее реализации.

Применительно к проблеме выбора рациональных наборов СрЗ морфологический метод состоит в том, чтобы для каждого рубежа защиты определить все необходимые ФП в соответствии с требованиями защиты, от которых зависит решение проблемы синтеза; представить их в виде матриц-строк, включающих в качестве элементов альтернативные СрЗ, а затем определить в этой морфологической матрице все возможные сочетания средств защиты по одному из каждой строки.

После построения матриц для рубежей защиты приступают к определению функциональной ценности каждой элементарной альтернативы и издержек от использования каждого средства защиты. Наиболее популярным для оценки альтернатив является критериальный метод, когда каждая отдельно взятая альтернатива оценивается конкретным числом.

Обобщенным показателем качества l-го СрЗ назовем вектор, компоненты которого суть показатели его отдельных свойств. Размерность этого вектора определяется числом существенных свойств СрЗ. Частные показатели качества имеют различную физическую природу и размерность. Выявление совокупности частных показателей качества средств защиты каждой ФП для проведения сравнительного анализа и обоснования выбора СрЗ для эксплуатации в конкретной СЗИ является одной из задач, решаемых при синтезе системы защиты.

Процесс принятия решения о выборе рационального варианта набора СрЗ для рубежа защиты — это функция преобразования содержания информации о требованиях, предъявляемых к средствам защиты определенных ФП, входящих в набор, о характеристиках средств защиты в подмножество наилучших вариантов набора $S' \subseteq S$.

Множество вариантов набора

$$S = \{S_1, ..., S_r, ..., S_R\}, \text{ где}$$

R — число вариантов альтернатив, из которых осуществляется выбор.

В задачах ПР используют понятие механизма выбора, который представляет собой кортеж из двух элементов: совокупность сведений, позволяющих сопоставлять варианты или группы вариантов, и правило выбора, указывающее, как, используя структуру сведений, выделить из предъявленного для выбора множества альтернатив S подмножество S′ или одну альтернативу S_R.

Обозначим общую совокупность сведений о средствах защиты ФП рубежа, позволяющих задавать бинарные отношения сходства, предпочтения, через W; совокупность сведений о СрЗ l-й ФП, позволяющих задавать те же отношения, — через W_l. Тогда механизм выбора:

$$M = \{W; J\}.$$

Для средств защиты l-й ФП множество W_l включает в себя два подмножества:

$$W_{\text{ЗЩ}l} \subset W_l \text{ и } W_{\text{и}l} \subset W_l, \text{ где}$$

$W_{\text{ЗЩ}l}$ — показатель «защищенность»,

$W_{\text{и}l}$ — показатель «издержки» средства защиты для l-ой ФП.

Следует отметить, что в условиях автоматизированного управления и при использовании экспертной информации в процессе принятия решения можно говорить (даже в случае формализованного правила выбора) о *рациональном*, а не оптимальном решении.

При использовании морфологического метода синтеза модель ПР можно представить в следующем виде:

$$\text{ПР}: <\text{Ц}, \Phi, \Pi_s, S, W_l, J, S_r\ (S')>, \text{ где}$$

Ц — цель принятия решения,

Ф — исходные данные для порождения альтернатив (множество функциональных подсистем для рубежа защиты),

Π_s — правило порождения альтернатив,

S — множество порожденных альтернатив,

W_l — данные для выбора рациональных вариантов: множество характеристик защищенности и издержек элементарных альтернатив — СрЗ для каждой l-й ФП,

J — правило выбора наилучшей альтернативы,

S_r — выбранная альтернатива,

$$Ф = \{Ф_1, Ф_2, ..., Ф_l, ..., Ф_L\}.$$

Правило порождения альтернатив $П_s$ может быть представлено в аналитическом виде как векторное произведение множеств:

$$S = Ф_1 \times Ф_2 \times ... \times Ф_l \times ... \times Ф_L, \text{ где}$$

$Ф_l$ — *l*-я ФП — множество, состоящее из элементарных альтернатив (средств защиты для данной подсистемы),

$$Ф_l = \{A_{l1}, A_{l2}, ..., A_{lm}, ..., A_{lKl}\}.$$

Задача ПР, обеспечивающая преобразование исходных данных в решение по выбору рационального варианта набора СрЗ для рубежа, может быть представлена в виде последовательности правил порождения альтернатив и выбора наилучшей по заданной целевой функции.

Обозначим целевую функцию — принцип выбора, по которому осуществляется выбор рационального набора СрЗ, через J. Тогда множество выбранных альтернатив, в частности, одна:

$$S_r = J(S, W).$$

Для решения этой задачи разработан метод обработки знаний, который использует неформализуемый опыт специалистов — экспертов в области ЗИ. Такой метод обеспечивает преобразование данных из базы знаний и вывод решений в аналитической форме.

Планирование ЗИ как функция управления в процессе ОТУ представляет собой процесс последовательного *снятия неопределенности* относительно структуры СЗИ и *состава* средств защиты на объекте управления. В первую очередь необходимо сформулировать *перечень требований*. Исходя из целевого назначения, требуемое состояние СЗИ можно оценить значением уровня защищенности (риска). Нужно сформировать структуру СЗИ и задать диапазон изменения выходной управляемой переменной, затем реализуется выбор способа достижения планируемого, требуемого уровня защищенности. В [3] приведено выражение, описывающее структуру процесса планирования:

$$Р_{ПЛ} = \langle I, F \rangle, \text{ где}$$

I — информационный компонент, описывающий сведения, используемые для получения текущего решения в форме задачи ПР;

F — процедурный компонент, включающий основные функции принятия решений (обмен информацией, расчетные, эвристические процедуры).

Эвристические процедуры основаны на неформальных правилах экспертов.

В каждом процессе планирования процедуры порождения альтернатив и использования правила выбора наилучшей альтернативы (набора СрЗ) образуют механизм получения решения. Для каждого рубежа защиты задается множество ФП, результатом процесса планирования является командная информация, которая содержит конкретные данные по распределяемым ресурсам, направляемым на достижение целевого состояния СЗИ как объекта управления.

2. Результаты структурного системного анализа системы ОТУ ЗИ с использованием IDEF технологии

В работе сделана попытка расширить спектр компьютеризованных инструментальных методов анализа с использованием IDEF-BPWin технологии на изучение процессов ОТУ ЗИ.

Поскольку модели IDEF0 [4] представляют систему как множество иерархических (вложенных) функций, в первую очередь должна быть определена функция, описывающая систему в целом, — *контекстная функция*.

Наименование контекстного блока — функционального блока самого высокого уровня — обобщает определение границ моделирования.

На рис. 1 представлен функциональный блок самого высокого уровня IDEF0-модели контура ОТУ ЗИ.

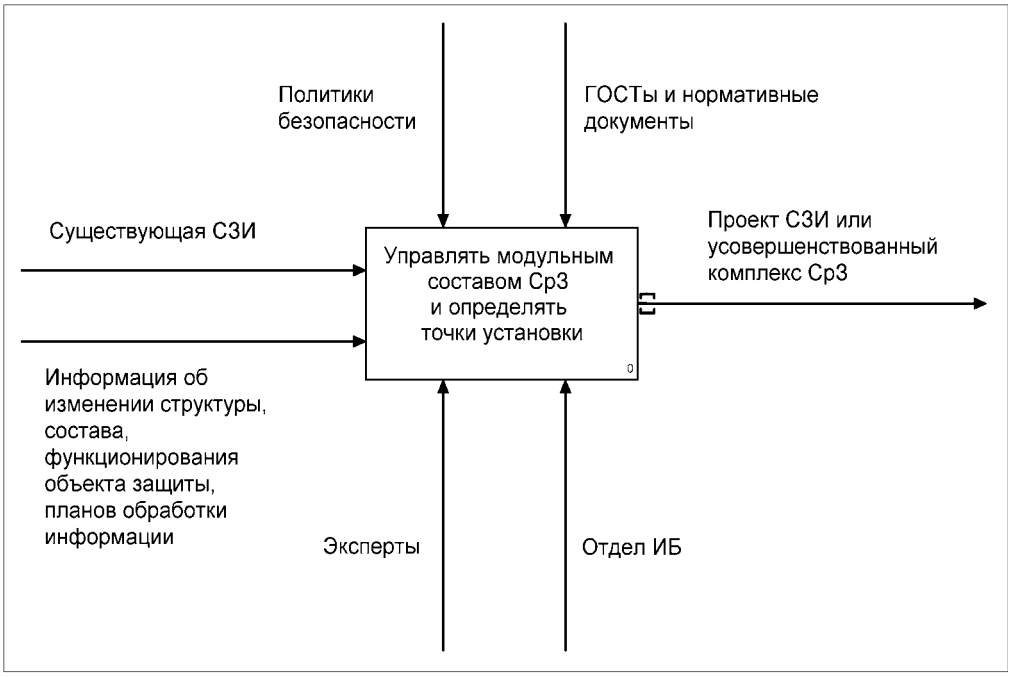

Рис. 1. Функциональный блок самого высокого уровня — контекстная функция

На нулевом уровне подробности приводится система как функциональный блок, затем она детализируется, приобретая иерархическую структуру со все большим числом уровней.

На рис. 2 представлена диаграмма разбиения процесса ОТУ ЗИ на функциональные блоки — подпроцессы.

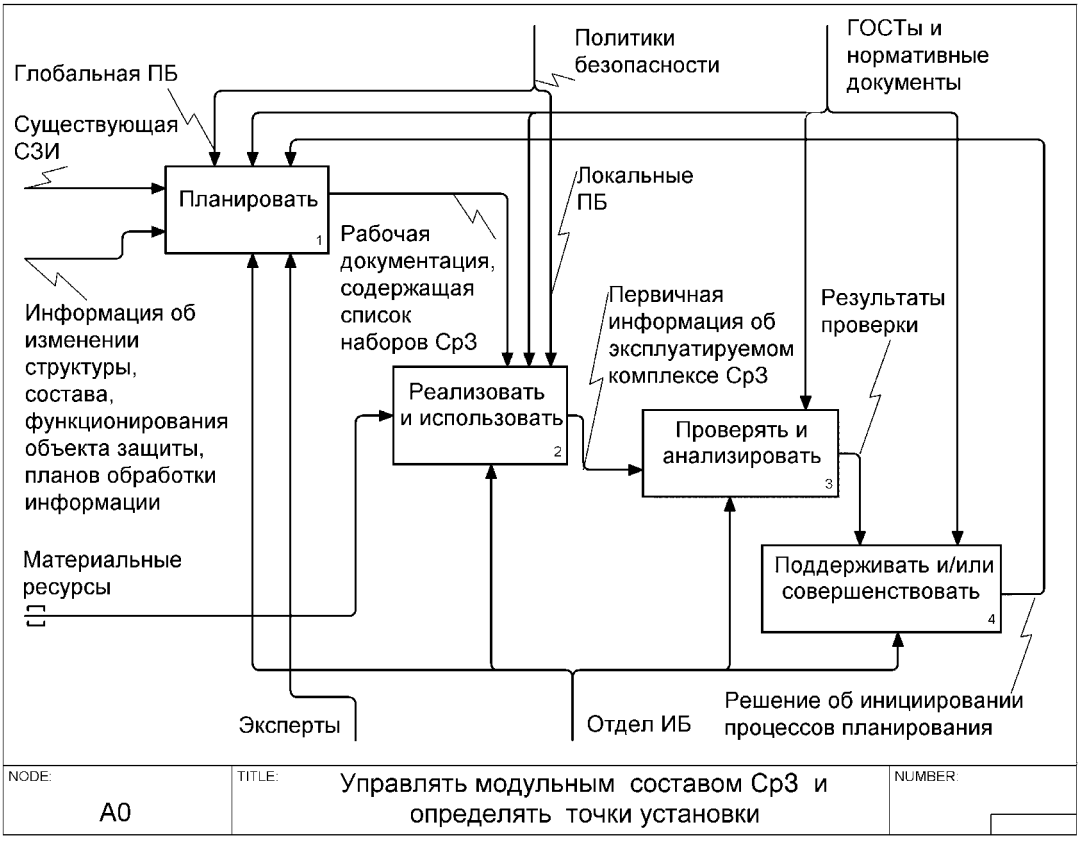

Рис. 2. Дочерняя диаграмма контекстного функционального блока

Любой блок диаграммы может быть декомпозирован на составляющие его блоки. Для того чтобы быть полезным, описание любого блока должно включать в себя описание объектов, которые блок создает в результате своей работы (выход), и объектов, которые он потребляет (вход). Функциональная декомпозиция определяется как моделирование «снаружи вовнутрь».

На рис. 3 представлен результат декомпозиции функционального блока «Планировать».

Рис. 3. Результат детализации функционального блока «Планировать»

На рис. 4 представлен результат декомпозиции одного из наиболее содержательных функциональных блоков диаграммы «Разработать концепцию».

Рис. 4. Результат детализации функционального блока «Разработать модель принятия решения»

Иерархическую декомпозицию можно продолжить до необходимого уровня подробности.

При проектировании сложных проектов, таких как система ОТУ ЗИ, разработка моделей в стандарте IDEF0 позволяет наглядно и эффективно отобразить весь механизм управления ЗИ в нужном разрезе. Реализация процессов, отображаемых моделью, осуществляется сотрудниками отдела информационной безопасности, экспертами в области ИБ, специалистами по теории принятия решений, автоматизированной системой (АС).

В результате IDEF0-диаграммы дают возможность ответить на вопросы: какие функции выполняются системой управления, в какой последовательности, кто является ответственным, что является результатом? Таким образом, IDEF0 позволяет с помощью своего простого инструментария решать сложные вопросы управления защитой информации.

Использование стандарта IDEF0 — это эффективный путь оптимизации систем управления ЗИ, тем более что проекты управления ЗИ связаны с построением *автоматизированных систем управления*.

СПИСОК ЛИТЕРАТУРЫ

1. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пос. для вузов. М.: Горячая линия — Телеком, 2004.

2. *Машкина И. В., Васильев В. И., Рахимов Е. А.* Проектирование системы защиты информации объекта информатизации // Информационные технологии. 2006. № 10. С. 17—26.

3. *Анфилатов В. С., Емельянов А. А., Кукушкин А. А.* Системный анализ в управлении: учебное пособие / Под ред. А. А. Емельянова. М.: Финансы и статистика, 2006.

4. *Черемных С. В., Семенов И. О., Ручкин В. С.* Моделирование и анализ систем. IDEF-технологии: практикум. М.: Финансы и статистика, 2006.