УДК 004.056

ФУНДАМЕНТАЛЬНЫЕ ОСНОВЫ МЕТОДИК БАЗОВОГО ЭКСПЕРТНОГО АНАЛИЗА ИНФОРМАЦИОННЫХ РИСКОВ[1]

В.В. Золотарев, Е.А. Ширкова

Сибирский государственный аэрокосмический университет, *г. Красноярск*

E-mail: amida@land.ru

В работе сделана попытка анализа процедуры формирования экспертной оценки информационного риска, целью которого явилось выявление фундаментальных основ базовых методик экспертного анализа информационных рисков. Представленные результаты получены на основе теоретико-множественного и графоаналитического подходов.

Ключевые слова: *управление риском*, *информационный риск*, *экспертные оценки.*

Практические подходы, формируемые при решении задач анализа рисков, часто не имеют хорошо проработанного формального обоснования, математического аппарата и других характеристик, необходимых для анализа проблемы. Кроме того, при разработке новых методик базового экспертного анализа информационных рисков и модификации существующих опираются не на фундаментальные результаты в предметной области, а на особенности практических задач.

В работе представлены результаты исследования, направленного на решение задачи обобщения и анализа основ методик экспертного анализа, применяемых в предметной области.

Полученные результаты свидетельствуют о необходимости пересмотра некоторых положений, широко используемых при формировании методик базового экспертного анализа информационных рисков.

Для анализа использованы исходные данные по применяемым на практике методикам CORA, NIST [1, 2], CRAMM, Digital Security Office, COBRA, RiskWatch [3], АванГард, Microsoft, ISO 17799:2000 [2], а также предложения по обобщению, изложенные в [4].

Исследование было разбито на несколько этапов:

- анализ требований стандартов и нормативных документов;
- формирование нового базового подхода на основе понятия риска несоответствия требованиям нормативных документов (см. [5]);
- обобщение подхода опросных листов с использованием полученных результатов;
- обобщение подхода табличных оценок и синхронизация обобщенного подхода с базовым.

Рассмотрим полученные результаты по каждому этапу.

Место исследования в предметной области

Поиск обобщающих характеристик подходов базового экспертного анализа информационных рисков в предметной области можно начать с оценки систем защиты информации (СЗИ). Согласно принятой в работе структуры оценки, отображенной на рис. 1, в качестве основы можно выделить экспертно-документальный метод проверки (исследование документации).

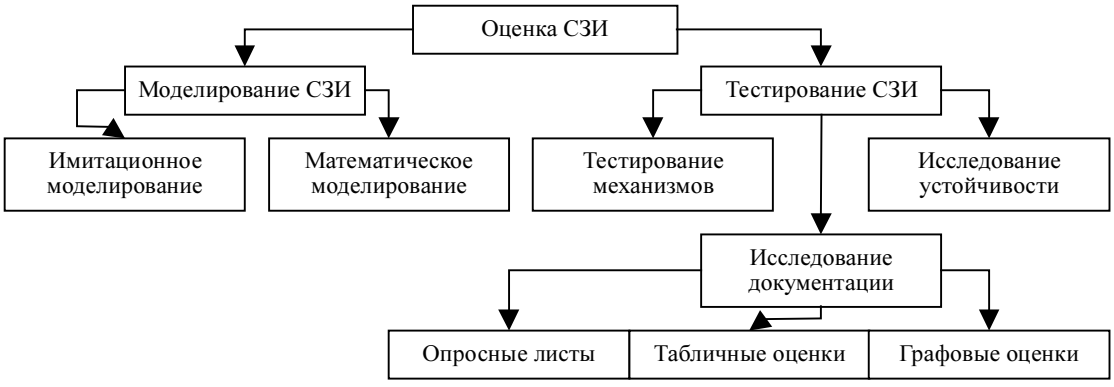

Рис. 1. Структура оценки СЗИ

[1] Работа поддержана грантом Президента молодым кандидатам наук № МК-3625.2007.9.

В данной статье не рассмотрены графовые оценки угроз и уязвимостей, поскольку находятся вне области обобщения.

Описание модели исследования

В работе рассматривается модель процедуры экспертной оценки системы защиты информации организации, которая представляет собой ориентированный взвешенный граф $G = (V, E)$, множество вершин описывает состояния системы с позиции экспертной оценки. Каждая вершина V_i ($i \in \{1, \ldots, N\}$, N – число вершин графа) описана следующими характеристиками: R_i, F_i, U_i, T_i, где R_i – интегральная качественная характеристика информационного риска; F_i – набор факторов, воздействующих на информацию; U_i – набор угроз и уязвимостей, активных в данном состоянии системы защиты информации; T_i – набор требований стандартов и нормативных документов, задействованных для данного состояния. Ребра графа описаны универсальными характеристиками переходов между состояниями системы – вероятность $P(T_s, T_l, T_o, T_t)$ невыполнения требований заданных подмножеств – соответственно стандартов, законодательных документов, организационной документации, технической документации. Таким образом, уникальными переходами между состояниями можно описать 16 состояний системы.

Каждое состояние характеризует порядок применения операций приведения в исходное (безопасное, то есть полностью соответствующее требованиям). Набор операций приведения уникален для каждого состояния и должен учитывать оптимальный путь приведения.

Рассмотрим такой набор операций конкретного состояния: $\alpha(V_i)$: A_f, A_u, A_t. Для каждого конкретного множества – A_f, A_u, A_t – операции задаются согласованно всеми экспертами, принимающими участие в оценке. При этом критична оценка адекватности выполняемых операций, например, по методам [4, 5].

Согласование экспертных оценок состояния системы

Задание видов операций приведения требует учета метода оценки каждого из элементов данных множеств. Согласно исследованию, выделены следующие базовые методы:

- опросных листов, позволяющих пользователям получить информацию из базы знаний экспертной системы в результате указания качественных характеристик процесса исследования;
- табличных оценок, позволяющих поэтапно оценить влияние факторов, воздействующих на ресурсы системы, на качественные характеристики процесса исследования;
- графоаналитические, позволяющие согласовать взаимное влияние угроз и уязвимостей, характеризующих различные состояния на графе G.

Кроме того, предусмотрен метод расчета финальных вероятностей перехода по графу G с использованием соотношений цепи Маркова.

Анализ требований стандартов и нормативных документов

Функционирование любой системы (организации) проходит, прежде всего, с учетом того правового поля, в котором она существует. В общем случае деятельность организации по обеспечению информационной безопасности осуществляется на основе следующих документов:

- действующих законодательных актов и нормативных документов РФ по обеспечению информационной безопасности;
- внутренних документов организации по обеспечению информационной безопасности.

Несоответствие документации организации каким-либо требованиям перечисленных документов приводит к появлению уязвимостей в системе, что может вызвать реализацию угрозы.

Можно проиллюстрировать необходимость анализа требований стандартов, используя метод стратификации и разделяя понятие идентификации риска:

- идентификация факторов, воздействующих на объект защиты;
- идентификация угроз и уязвимостей;
- идентификация требований стандартов и нормативных актов для формирования базы знаний экспертной системы.

На рис. 2 отображены переходы между упомянутыми уровнями, интерпретированные с использованием теоретико-множественного подхода.

Очевидно, при идентификации факторов, воздействующих на объект защиты, невозможно со сколько-нибудь приемлемой точностью оценить степень их влияния на конкретные элементы системы, но возможно проведение предварительной оценки. Множество факторов имеет отображение на множество угроз, которое в общем случае содержит большее количество элементов. Здесь необходимо ввести в анализ понятие качества изучения системы, которое влияет на степень детализации второго множества.

Отображая множество угроз и уязвимостей на множество требований стандартов и нормативных документов, можно увидеть, что такая операция делает анализируемое множество дискретным и четко определяет количество его элементов.

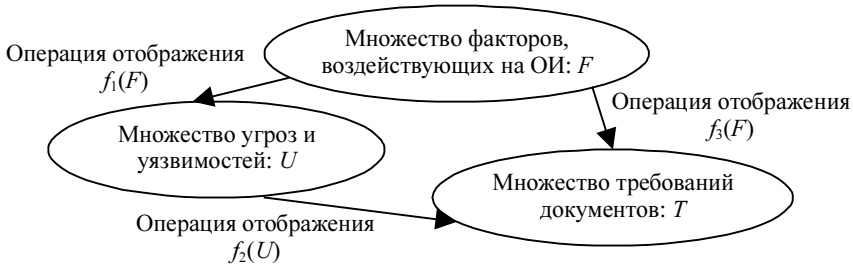

Рис. 2. Соотношение уровней идентификации информационного риска

Анализ требований стандартов и нормативных документов требует использования специальных методик формирования базы знаний экспертной системы, например указанной в [5].

Обобщение подхода опросных листов

Обобщенный подход опросных листов предполагает следующий метод извлечения информации из базы знаний экспертной системы. Используются качественные или количественные оценки состояния системы – вершины V графа состояний G системы, пользователь экспертной системы получает взвешенные рекомендации, разделенные согласно составляющих операции $\alpha(V)$. Анализ информационных рисков состоит из нескольких этапов (рис. 3):

- анализируются путем экспертной оценки с заданной статической либо динамической системой весов рекомендаций исходные данные по информационной системе;
- производится непосредственно анализ информационных рисков системы исходя из сформированных требований и исходных данных по организации, выдача практических рекомендаций по повышению уровня информационной безопасности и минимизации информационных рисков организации.

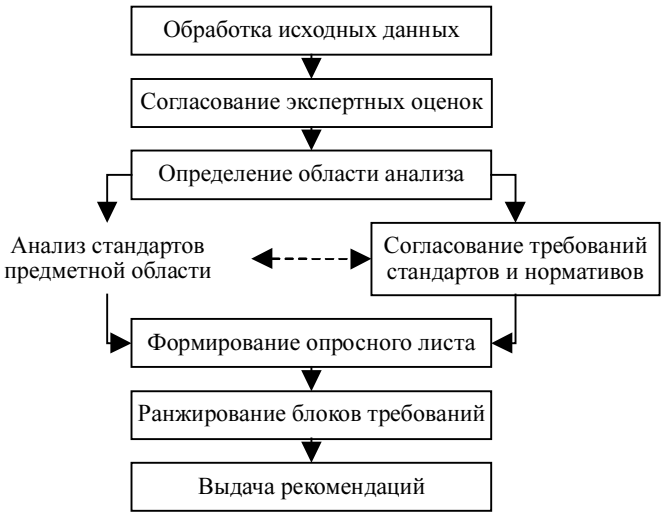

Рис. 3. Схема методики анализа остаточного информационного риска

Обобщенная методика отличается от классического понимания экспертного анализа рисков. На первом этапе классической методики происходит анализ всех возможных угроз и уязвимостей. Здесь же рассматривается только уровень требований нормативных документов, как упорядоченный и связанный непосредственно с предметной областью. Предполагается, что ранжирование угроз рассматривалось при составлении требований нормативных документов.

Анализ остаточных информационных рисков в данной работе основан на экспертных оценках, при этом учитывается несколько аспектов, позволяющих оценить их качество:

- квалификация эксперта;
- количество выданных рекомендаций в среднем по тематическим блокам;
- количество задействованных тематических блоков;
- средняя квалификация экспертов, выдавших конкретные рекомендации.

При этом алгоритм оценки принимает следующий вид (рис. 4):

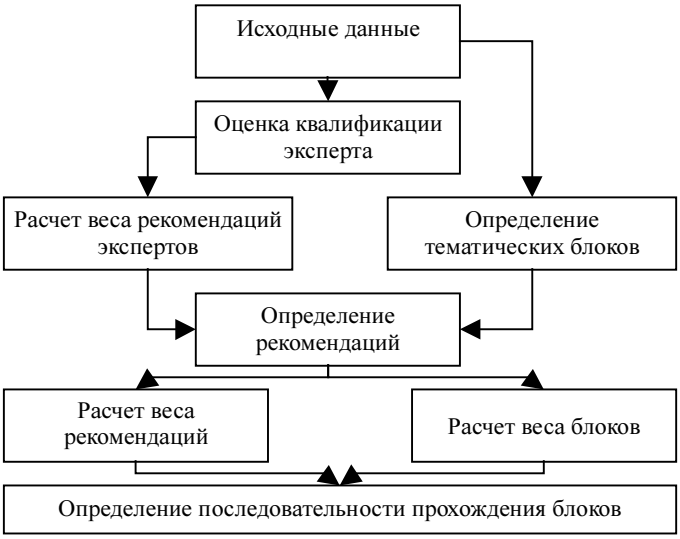

Рис. 4. Техника экспертного анализа

В данной методике существенны следующие моменты:

- эксперты, принимающие участие в оценке, могут иметь различную квалификацию;
- количество экспертов не ограничено сверху;
- рекомендации и вопросы опросного листа разбиваются по тематическим блокам, связанным с конкретными стандартами и нормативными актами;
- при опросе конкретного эксперта могут быть задействованы не все тематические блоки.

Преимуществом такой техники, по мнению авторов, является гибкость и независимость от конкретной ситуации, существенное достоинство – возможность добавления новых стандартов и нормативных документов. Тогда алгоритм опроса будет изменен путем введения новых тематических блоков и, возможно, удаления уже существующих.

Обобщение подхода табличных оценок

При таком подходе производится анализ факторов риска, т.е. источников угроз. При выборе факторов риска можно руководствоваться ГОСТ Р 51275-2006 «Объекты информатизации. Факторы, воздействующие на информацию». В данном случае можно анализировать как всю информационную систему организации в целом, так и ее отдельные составляющие. В общем виде анализ рисков, основанный на данном подходе, можно представить следующим образом (рис. 5):

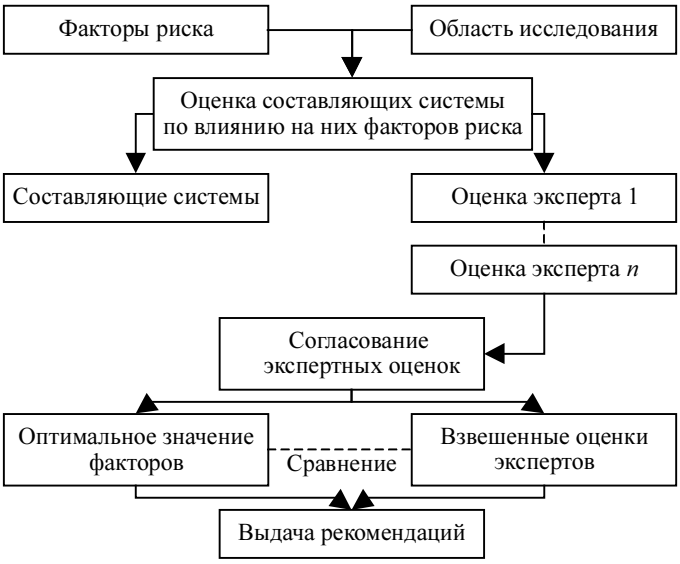

Рис. 5. Анализ факторов риска

Уровень каждого фактора оценивается экспертами, после чего проводится согласование экспертных оценок. Для удобства программной реализации необходимо получить шкалу оценки факторов риска – перевод качественных показателей в количественные – это осуществляется с помощью методов нечеткой логики. После получения количественных показателей можно определять функцию риска путем применения подходов математической логики.

Идея метода оптимизации следующая: по каждому фактору задается некоторое пороговое значение на шкале и производится оценка условно оптимального по заданному критерию значения фактора.

Выводы

Применение предложенных подходов позволяет упростить постановку задачи анализа информационных рисков автоматизированной системы. Использование экспертных систем в данных подходах является шагом к получению объективных результатов в процессе управления рисками.

Результатом работы является комплексный подход, формализующий требования к разработке некоторых видов экспертных систем заданной области.

ЛИТЕРАТУРА

1. *Прищеп С.В.* Сравнительный анализ методик NIST и CORA // Актуальные проблемы безопасности информационных технологий: Материалы I Междунар. науч.-практич. конф. Красноярск: Изд-во Сиб. гос. аэрокосмич. ун-та, 2007. С. 93 – 97
2. *Петренко С.А.*, *Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи, ДМК Пресс, 2004. 384 с.
3. *Информационная* безопасность. М.: Компания АйТи, 2005. 468 с.
4. *Жданов О.Н.*, *Золотарев В.В.* Анализ информационных рисков при передаче данных по открытому каналу // Актуальные проблемы безопасности информационных технологий: Материалы I Междунар. науч.-практич. конф. Красноярск: Изд-во Сиб. гос. аэрокосмич. ун-та, 2007. С. 32 – 38.
5. *Золотарев В.В.*, *Ткаченко К.П.*, *Ширкова Е.А.* Управление информационными рисками несоответствия требованиям нормативных документов в области защищенного документооборота // Управление риском: науч.-технич. журн. Вып. 1. М.: Изд-во Анкил, 2008.