Экспертная система оценки эффективности защиты информации

En **Expert System for information security effectiveness assessment**

A. N. Lulchenko,
OAO «Kontsern „Oceanpribor"»
sch00l@gkspr.ru

The article describes an expert system which provides an assessment of information security level in government companies and other companies of various forms of ownership. Presented expert system allows to assess whether organizational and technical requirements are met and to estimate the level of data protection system compliance with those requirements. An expert evaluation method is used as a basis. The expert system helps to reduce routine operations in information security audit significantly. Assessment results are presented graphically. They allow the management of a company to make reasonable decisions on further information security system improvement.

Keywords: information security, expert system, evaluation of the information security effectiveness, protected information, information system, coefficient of significance, individual information protection status evaluation indicators, organizational and administrative documents, personal data, audit

В статье рассматривается экспертная система, обеспечивающая оценку состояния защищенности информации в органах власти и организациях различных форм собственности. Предлагаемая экспертная система позволяет оценивать состояние выполнения требований как организационных мероприятий, так и технических мероприятий по обеспечению защиты информации, а также уровень соответствия предъявляемым требованиям системы защиты информации в целом. В качестве базового метода оценки состояния защиты информации используется метод экспертной оценки. Разработанная экспертная система обеспечивает существенное сокращение рутинных операций при проведении аудита информационной безопасности. Результаты оценки представляются достаточно наглядно и обеспечивают возможность руководству органов власти и организаций принимать обоснованные решения по дальнейшему совершенствованию системы защиты информации.

Ключевые слова: информационная безопасность, экспертная система, оценка эффективности защиты информации, органы власти, защищаемая информация, информационная система, комплексные показатели оценки состояния защиты информации, коэффициент значимости, единичные показатели оценки состояния защиты информации, организационно-распорядительные документы, персональные данные, аудит информационной безопасности

Андрей Николаевич Люльченко,
ОАО «Концерн „Океанприбор"»
sch00l@gkspr.ru

Необходимость разработки экспертной системы (ЭС) оценки эффективности защиты информации обусловлена целым рядом обстоятельств.

В связи с большим объемом исходных данных, громоздкими процедурами их обработки, сложностью принятия решений о состоянии обеспечения информационной безопасности в организациях в условиях большого количества учитываемых факторов проведение необходимых оценок без автоматизации этого процесса практически невозможно. Автоматизация, по сути, приводит к созданию соответствующей экспертной системы, реализующей автоматизированную поддержку принятия решений при проведении оценок состояния обеспечения информационной безопасности.

В процессе оценивания состояния обеспечения информационной безопасности и тенденций ее изменения, как правило, проводится анализ влияния существенных факторов (параметров, характеристик и условий функционирования информационных систем) на результаты оцен-

ки. Следует отметить, что необходимость такого анализа существенно усложняет требования к ЭС. Если остановиться только на процедурах сбора данных и оценки состояния обеспечения информационной безопасности, то достаточно было бы разработать соответствующую базу данных и программы расчета показателей. Однако на практике необходимо не только оценить состояние обеспечения информационной безопасности, но и установить факторы, изменение которых позволит повысить защищенность информационных систем от деструктивных информационных воздействий.

Такой анализ можно было бы проводить на основе многократных расчетов показателей оценки обеспечения информационной безопасности по разработанным аналитическим соотношениям, однако при этом необходимо осуществлять варьирование большого количества единичных показателей, используемых при расчетах комплексных показателей эффективности.

Важную роль при оценивании состояния обеспечения информационной безопасности играет назначение весовых коэффициентов для показателей всех уровней, которое проводится, как правило, с использованием методов экспертного опроса, что приводит к отклонениям в результатах оценки и необходимости корректировки весовых значений показателей. Результаты экспертной оценки во многом зависят от применяемого метода, но в любом случае эти процедуры являются достаточно рутинными.

При наличии неполных или нечетких исходных данных важным подспорьем могут оказаться результаты ранее проведенных анализов состояния обеспечения информационной безопасности, но трудоемкие процедуры сравнения многочисленных исходных данных крайне затрудняют использование прямых методов расчета показателей в интересах такого анализа.

Предлагаемая экспертная система представляет собой специализированный программный продукт, устанавливаемый на автоматизированные рабочие места как специалистов, отвечающих за обеспечение информационной безопасности, так и руководителей организации.

Экспертная система обеспечивает возможность проведения оценки эффективности защиты информации на предпроектной стадии создания систем защиты информации при проведении внутреннего (внешнего) аудита информационной безопасности для определения соответствия информационных систем требованиям безопасности информации.

Работа по проведению оценки эффективности защиты информации осуществляется путем выполнения следующих процедур:

- *этап 1* – подготовка исходных данных;
- *этап 2* – проведение контроля реализации требований;
- *этап 3* – расчет комплексных показателей оценки состояния системы защиты информации (СЗИ).

На этапе 1 осуществляется подготовка следующих исходных данных:

- перечень видов защищаемой информации $\{h^{и}\}$ (основными видами защищаемой информации являются: информация, содержащая сведения, составляющие государственную тайну, служебная информация, персональные данные, общедоступная информация);
- перечни требований к составу организационно-распорядительных документов (ОРД), изложенных в нормативных правовых актах $\{p^{нп}\}$ и нормативных документах $\{p^{нд}\}$ в области обеспечения защиты информации [1–3] (таблицы требований формируются для каждого вида защищаемой информации);
- перечни требований к подразделениям обеспечения безопасности информации $\{p^{с}\}$ и квалификации сотрудников данных подразделений $\{p^{к}\}$ [4];
- перечень типов информационных систем $\{\delta\}$;
- перечень требований, предъявляемых к СЗИ информационных систем и СЗИ информационных систем персональных данных, а также к уровню защищенности персональных данных $\{p^{фп}\}$ [1–3];
- классы защищенности информационных систем $\{q^{ис}\}$;
- типы информационных систем, функционирующих в организации;
- количество информационных систем каждого типа.

На этапе 2 осуществляются следующие мероприятия.

Шаг 1. Формирование анкет для проведения контроля реализации требований.

Шаг 2. Непосредственное проведение контроля реализации требований, осуществляемое методом анкетирования. С учетом имеющейся в БД информации, введенных исходных данных автоматически формируются следующие анкеты:

- анкета требований к составу ОРД, изложенных в нормативных правовых актах;
- анкета требований к составу ОРД, изложенных в нормативных документах в области защиты информации;
- анкета требований к уровню квалификации специалистов подразделения, обеспечивающего ИБ в организации;
- анкета требований к составу подразделений, специалистов, обеспечивающих ИБ;
- анкета требований к системе защиты информации информационной системы. Данные требования определяются с учетом класса защищенности информационной системы и базового набора требований к системе защиты информации информационной системы.

Количество анкет с требованиями к системам защиты информации информационных систем соответствует количеству информационных систем, функционирующих в организации.

Шаг 3. Контроль реализации требований выполняется членами комиссии, отвечающими за обеспечение информационной безопасности в организации. В ходе контроля проверяется выполнение требований по каждой анкете, и в графе «Единичные показатели, фактическое выполнение» проставляется «1» в случае выполнения требования и «0» в противном случае.

На этапе 3 осуществляется расчет показателей эффективности за-

щиты информации, как это показано в [5].

Степень выполнения требований для каждой функциональной подсистемы $W_r^{\text{пi}}$ вычисляется по зависимости

$$W_r^{\text{пi}} = \frac{\sum_h p_{rh}^{\text{фпi}}}{\sum_h p_{rh}^{\text{тпi}}},\ 0 \leqslant W_r^{\text{пi}} \leqslant 1, \quad (1)$$

где $p_{rh}^{\text{тпi}}$ – требуемое значение единичного показателя, $r = 1 \div R$ – количество функциональных подсистем в СЗИ i-й ИС, $h = 1 \div H_r$, H_r – количество единичных требований к r-й функциональной подсистеме СЗИ i-й информационной системы. Значение H_r зависит от класса защищенности ИС (уровня защищенности персональных данных); $p_{rh}^{\text{фп}i}$ – фактическая реализация h-го требования в r-й функциональной подсистеме i-й информационной системы.

Вычисление комплексного показателя степени выполнения требований к составу ОРД, изложенных в нормативных документах в области ЗИ – $W^{\text{нд}} = F(p_n^{\text{нд}})$, осуществляется с учетом следующей зависимости:

$$W^{\text{нд}} = \frac{\sum_n p_n^{\text{фнд}}}{\sum_n p_n^{\text{тнд}}},\ 0 \leqslant W^{\text{нд}} \leqslant 1, \quad (2)$$

где $p_n^{\text{тнд}}$, $p_n^{\text{фнд}}$ – требования к составу ОРД, изложенные в нормативных документах в области ЗИ, и их фактическое выполнение.

Комплексный показатель степени выполнения требований к составу ОРД, изложенных в нормативных правовых актах – $W^{\text{нп}}$, рассчитывается по формуле:

$$W^{\text{нп}} = \frac{\sum_s p_s^{\text{фнп}}}{\sum_s p_s^{\text{тнп}}},\ 0 \leqslant W^{\text{нп}} \leqslant 1, \quad (3)$$

где $p_s^{\text{тнп}}$, $p_s^{\text{фнп}}$ – требования по разработке документа, необходимого в соответствии с требованиями нормативной базы в области ЗИ, и его фактическое выполнение.

Расчет комплексного показателя степени выполнения требований к структуре и составу подразделения по обеспечению ИБ – $W^{\text{с}} = F(p_m^{\text{с}})$ – выполнятся следующим образом:

$$W^{\text{с}} = \frac{\sum_m p_m^{\text{фс}}}{\sum_m p_m^{\text{тс}}},\ 0 \leqslant W^{\text{с}} \leqslant 1, \quad (4)$$

где $p_m^{\text{тс}}$, $p_m^{\text{фс}}$ – требования к структуре и составу подразделения по обеспечению информационной безопасности и их фактическое выполнение.

Комплексный показатель степени выполнения требований к квалификации специалистов подразделения по обеспечению информационной безопасности – $W^{\text{к}} = F(p_q^{\text{к}})$ – вычисляется по зависимости:

$$W^{\text{к}} = \frac{\sum_q p_q^{\text{фк}}}{\sum_q p_q^{\text{тк}}},\ 0 \leqslant W^{\text{к}} \leqslant 1, \quad (5)$$

где $p_q^{\text{тк}}$, $p_q^{\text{фк}}$ – требования к квалификации специалистов подразделения по обеспечению информационной безопасности и их фактическое выполнение.

В ЭС принято, что все функциональные подсистемы R имеют одинаковое влияние на выполнение требований СЗИ ИС. Поэтому, комплексные показатели степени выполнения требований к СЗИ ИС, функционирующих в организации – $W_i^{\text{ис}}$ – вычисляются по формуле:

$$W^{\text{ис}i} = \frac{\sum_r p_{\text{r}}^{\text{п}i}}{R},\ 0 \leqslant W^{\text{ис}i} \leqslant 1, \quad (6)$$

где $r = 1 \div R$, R – количество функциональных подсистем в СЗИ i-й ИС.

На следующем шаге осуществляется расчет комплексных показателей, характеризующих степень выполнения организационных, правовых и технических мер защиты информации в организации.

Комплексный показатель к организационным мерам защиты информации $W^{\text{о}} = F(W^{\text{с}}, W^{\text{к}})$ рассчитывается по формуле:

$$W^{\text{о}} = \frac{\sum_m p_m^{\text{фс}} + \sum_q p_q^{\text{фк}}}{\sum_m p_m^{\text{тс}} + \sum_q p_q^{\text{тк}}},$$
$$0 \leqslant W^{\text{о}} \leqslant 1, \quad (7)$$

Аналогичным способом вычисляется комплексный показатель степени выполнения требований к правовым мерам ЗИ $W^{\text{п}} = F(W^{\text{нп}}, W^{\text{нд}})$.

При расчете комплексного показателя эффективности технических мер защиты информации в информационной системе – $W^{\text{ис}} = F(W_i^{\text{ис}})$ – необходимо учитывать, что в ИС обрабатывается, как ранее указывалось, информация ограниченного доступа различного уровня конфиденциальности. Нарушения защищенности ИС, обрабатывающих информацию различных видов конфиденциальности, имеют различную значимость в формировании комплексного показателя $W^{\text{ис}}$. С учетом вышеизложенного при расчете показателя вводятся коэффициенты весомости ИС, комплексный показатель $W^{\text{ис}}$ рассчитывается по формуле:

$$W^{\text{ис}} = \sum_i a_i W_i^{\text{ис}},\ 0 \leqslant W^{\text{ис}} \leqslant 1, \quad (8)$$

где a_i – коэффициент значимости i-й ИС ($W_i^{\text{ис}}$), $\sum_i a_i = 1$.

Последним шагом оценки эффективности является вычисление комплексного показателя $W^{\text{СИБ}}$. При расчете $W^{\text{СИБ}}$ учитывается степень выполнения требований по защищаемым ИС ($W^{\text{ис}}$), степень выполнения организационных ($W^{\text{о}}$) и правовых ($W^{\text{п}}$) требований в интересах обеспечения информационной безопасности в организации. Вклад каждого показателя в обеспечение ИБ имеет разную весомость, поэтому $W^{\text{СИБ}}$ рассчитывается по формуле

$$W^{\text{СИБ}} = b_1 W^{\text{о}} + b_2 W^{\text{п}} + b_3 W^{\text{ис}},$$
$$0 \leqslant W^{\text{СИБ}} \leqslant 1, \quad (9)$$

где b_1, b_2, b_3 – коэффициенты значимости показателей $W^{\text{о}}$, $W^{\text{п}}$ и $W^{\text{ис}}$ соответственно, $b_1 + b_2 + b_3 = 1$.

Коэффициенты значимости a_i, b_1, b_2, b_3 определяются с учетом рекомендаций по результатам экспертного опроса.

Расчет показателей эффективности осуществляется в соответствии с алгоритмом, показанным на рис. 1.

Экспертная система реализована в виде программного продукта, на который имеется свидетельство о госрегистрации программ для ЭВМ. Последовательность проведения работ с использованием экспертной системы представлена на рис. 2.

Экспериментальные исследования программы оценки состояния системы обеспечения информационной безопасности (ПОС СОИБ) выполнялись с использованием принципов модульного тестирования. В ходе проведения экспериментальных исследований было определено, что алгоритм оценки степени выполнения требований обладает такими существенными свойствами, как дискретность, детерминированность, конечность, результативность.

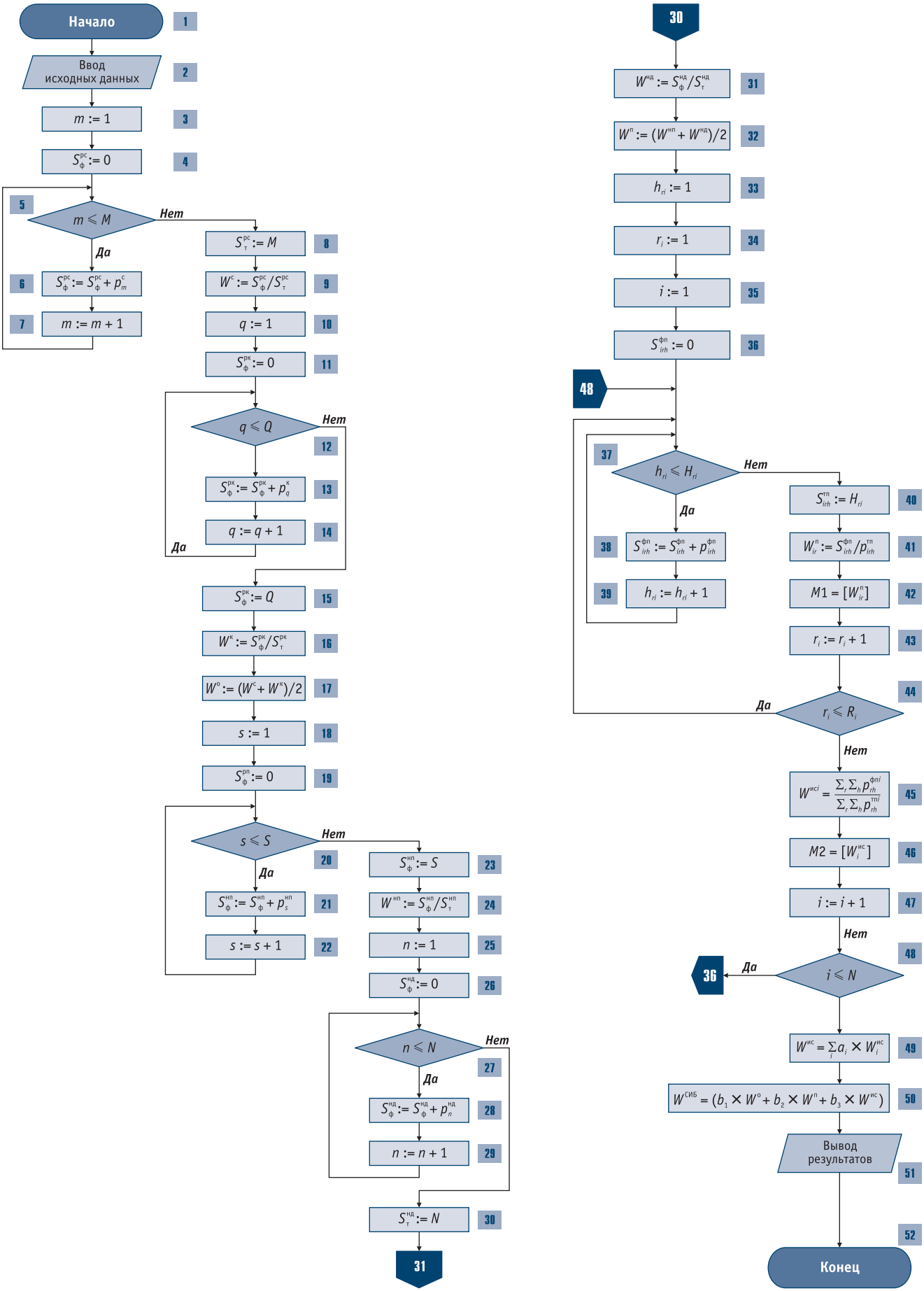
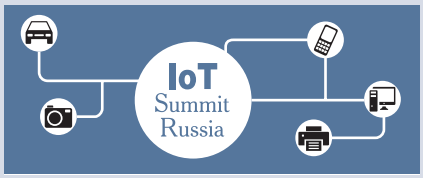


Рис. 1. ***Блок-схема алгоритма оценки эффективности защиты информации***

НОВОСТИ

Прошел IoT Summit Russia

7 июня 2016 года в преддверии Петербургского международного экономического форума в Санкт-Петербурге состоялся IoT Summit Russia.



Мероприятие было организовано Некоммерческим партнерством РУССОФТ с целью продвижения Национальной технологической инициативы (НТИ).

Интернет вещей как очередной этап развития глобальной сети является ключевым трендом конкурентоспособного производства. По прогнозам международных исследовательских компаний, к 2019 году Интернет вещей станет крупнейшим в мире рынком по числу электроники. «Умные» предприятия и объединенное в большие производственные системы «умное» оборудование способны будут изменить традиционную производственную систему и поднять экономику на более высокий уровень производительности.

IoT Summit Russia стал площадкой для обсуждения возможностей развития IoT в России, обмена опытом между российскими и иностранными компаниями, работающими в этой сфере. В мероприятии приняло участие более 200 человек: сотрудники органов государственной власти, представители ИТ-бизнеса, крупных промышленных предприятий России, государственных корпораций, профессиональных ассоциаций и объединений, научных и образовательных учреждений.

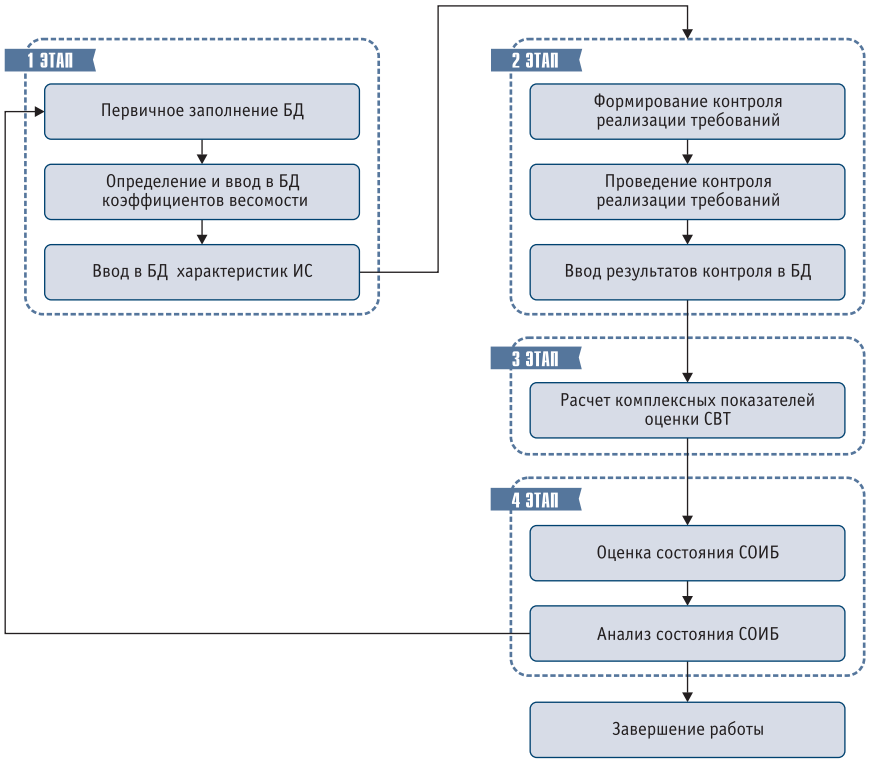


Рис. 2. ***Последовательность выполнения работ с использованием экспертной системы***

Установлено, что разработанная программа ПОС СОИБ после проведения тестирования и отладки:

- обеспечивает правильные результаты решения задачи;
- обладает низкой вероятностью отказа в процессе решения задачи;
- обеспечивает достаточную производительность решения задачи;
- отвечает требованиям практичности (применимости).

Таким образом, можно сделать вывод о том, что предлагаемая математическая модель, алгоритм и программа могут быть использованы в практической деятельности подразделений, отвечающих за безопасность информации. Описываемая экспертная система, в отличие от существующих, позволяет выполнять экспресс-оценку состояния информационной безопасности органов власти и организаций при проведении аудита ИБ, при периодическом контроле эффективности обеспечения защиты информации, автоматизировать процесс выработки рекомендаций по совершенствованию системы ИБ организации, а также обеспечивает решение задач оценки и анализа состояния систем обеспечения ИБ. ■

ЛИТЕРАТУРА

1. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите ПДн при их обработке в ИСПДн».

2. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4. Единый квалификационный справочник должностей руководителей, специалистов и других служащих (ЕКС) «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации», утв. Приказом Минздравсоцразвития РФ от 22.04.2009 № 205.

5. Люльченко А. Н., Бувайлик С. С. Методика оценки состояния системы обеспечения информационной безопасности организации // Межвузовский сборник трудов: V Всероссийская научно-техническая конференция НИУ ИТМО. – СПб, 2015. – С. 84–88.