

Д. А. Полянский, О. И. Файман, С. Ю. Кириллова

**ИНСТРУМЕНТАЛЬНЫЙ КОМПЛЕКС КОНТРОЛЯ
ДОСТОВЕРНОСТИ ИНФОРМАЦИИ
В КОРПОРАТИВНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ АСУ**

Рассмотрены структура и состав комплекса инструментальных средств контроля достоверности данных, циркулирующих в корпоративной сети. Проанализированы особенности применения инструментального комплекса.

Ключевые слова: достоверность данных, информационный ресурс, корпоративная сеть, дестабилизирующий фактор, экспертная оценка.

Контроль текущего уровня достоверности информации, циркулирующей в корпоративной сети передачи данных (КСПД), предполагает выполнение большого количества операций, в том числе действий по математической обработке экспертных данных. Любое варьирование структуры и/или состава средств системы обеспечения достоверности информации (СОДИ) приводит к изменению общих показателей.

Следовательно, для оперативного контроля уровня достоверности информации, а также с целью выбора комплекса средств обеспечения достоверности путем сравнения получаемых общих показателей необходим инструментальный комплекс (ИК), позволяющий решать следующие задачи:

— поддержка базы знаний дестабилизирующих факторов (ДФ), структурно-функциональных недостатков (СФН), информационных ресурсов (ИР), оценочных таблиц и результатов ранее проведенных исследований [1];

— обеспечение процесса проведения экспертизы корпоративной телекоммуникационной сети (КТКС) на основе базы знаний;

— математическое обеспечение процесса получения частных показателей качества КТКС и СОДИ и показателей достоверности.

Сказанное выше определяет состав ИК: база знаний, модуль поддержки базы знаний, модуль обеспечения процесса проведения экспертизы КСПД и вычислительный модуль.

Высокая структурная сложность моделей определения качества средств защиты и необходимость в решении сопутствующей задачи оценки рисков и экономической эффективности СОДИ [2] диктуют требования к ИК.

Требования к базе знаний и модулю ее поддержки как к единому целому следующие:

- поддержка хранения в систематизированном виде списков ДФ, СФН, ИР и оценочных лингвистических таблиц;
- поддержка возможности добавления новых ДФ, СФН, ИР и оценочных лингвистических таблиц;
- поддержка возможности изменения формулировок ДФ, СФН, ИР и описаний в лингвистических таблицах;
- поддержка возможности изменения структуры и классификации ДФ, СФН и ИР.

Требования к модулю обеспечения процесса проведения экспертизы:

- поддержка возможности выбора из базы знаний ДФ, СФН, ИР, актуальных для исследуемой КТКС;
- обеспечение процесса ввода оценок количественных показателей: „стоимость“, „весовой коэффициент“, „степень выполнения“;
- обеспечение процесса выбора по лингвистическим таблицам первичных оценок качественных показателей: „сравнительная значимость“, „ценность“, „доступность“, „причинно-следственная связь“, „предел достаточности“, „степень соответствия“, „степень влияния“.

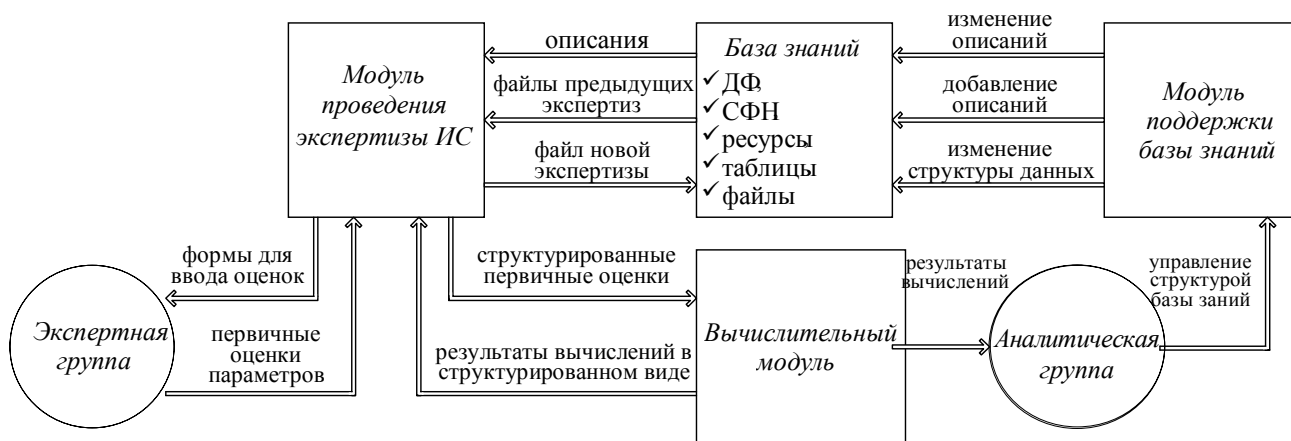
Вычислительный модуль выполняет расчеты:

- относительной частоты возникновения ДФ;
- возможности нарушения достоверности ИР;
- ущерба, вызванного нарушением достоверности данных ИР;
- экономических характеристик использования ресурсов;
- рисков при отсутствии и наличии СОДИ;
- достоверности данных ИР в КТКС.

Потребности в проведении переоценок различных показателей вследствие изменения конфигурации КТКС диктуют дополнительные требования к ИК:

- хранение результатов экспертизы КТКС и оценки достоверности информации в формате текстового документа;
- возможность пересчета итоговых показателей в автоматическом режиме после внесения изменений в файл экспертных данных;
- возможность сравнения и расчет эффективности изменений, вносимых в КТКС с целью повышения достоверности представленных новым файлом экспертных данных;
- дружественный интерфейс в использовании, обновлении и добавлении информации в базу знаний.

Функциональная схема работы ИК, представленная на рисунке, отражает приведенные выше задачи, состав и требования к системе, а также информационное взаимодействие с ней аналитической и экспертной групп.



Анализ особенностей проведения экспертизы для предприятий с разной как по размерности, так и по структуре информационной системой показывает, что база знаний должна со-

держат следующие массивы данных, а также экспериментально установленные отношения и описания:

- классификатор типов ДФ;
- массив наименований ДФ, ассоциированных с каждым типом, и их описания;
- классификатор типов СФН;
- массив наименований СФН, ассоциированных с каждым типом, и их описания;
- массив видов ИР;
- оценочные таблицы описаний для исследования всех качественных характеристик КТКС;
- файлы экспертных данных, содержащие результаты исследования КТКС предприятий в виде полных массивов ДФ, СФН, ИР, ресурсов системы обработки информации, средств СОДИ, а также рассчитанные величины рисков и показателей достоверности информации.

Вычисление текущего уровня достоверности данных ИР основано на исследовании КТКС предприятия. Решить эту задачу позволяет модуль проведения экспертизы, который реализует интерфейс взаимодействия эксперта с базой знаний:

- выбор из базы знаний ДФ и СФН, актуальных для исследуемой КТКС;
- выбор из базы знаний описаний ИР;
- ввод первичных оценок отдельных параметров в формы, созданные модулем на основе выборки ДФ, СФН и ИР;
- изменение исходных данных предыдущего исследования КТКС и их дополнение на основе файлов предыдущих экспертиз, хранящихся в базе знаний.

Модуль формирует массив исходных данных экспертизы и передает его в вычислительный модуль, где происходит их обработка и получение конечных результатов: информационные риски, экономическая эффективность и достоверность данных ИР. Первичные данные экспертизы и результаты вычислений модуль заносит в файл новой экспертизы и вносит его в базу знаний.

Дополнительным в ИК является модуль поддержки базы знаний, назначение которого состоит в управлении содержимым файлов базы знаний: изменение структуры и содержания отдельных описаний, добавление новых описаний и удаление старых.

СПИСОК ЛИТЕРАТУРЫ

1. Полянский Д. А. Применение методики экспертных оценок для расчета вероятностей возникновения угроз безопасности информационной системе предприятия // Тр. XXVI Междунар. науч.-техн. конф. „Проблемы эффективности безопасности функционирования сложных технических и информационных систем“. Серпухов: Серпуховской ВИ РВ, 2007. № 1. С. 68—72.
2. Полянский Д. А., Файман О. И. Комплексная защита объектов информатизации. Кн. 16. Экономика защиты информации. Владимир: Изд-во ВлГУ, 2009. 96 с.

Сведения об авторах

- Дмитрий Александрович Полянский** — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: polyansk@rambler.ru
- Ольга Игоревна Файман** — Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; ассистент; E-mail: Olich06@inbox.ru
- Светлана Юрьевна Кириллова** — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информационных систем и информационного менеджмента; заместитель заведующего кафедрой; E-mail: sv-kir@mail.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.