Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление 09.04.01 – Информатика и вычислительная техника
Магистерская программа Компьютерное моделирование

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____2017г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему: Разработка экспертной системы для анализа и оценки информационной безопасности

Исполнитель
студент группы 553ОМ _____ (подпись, дата) С.В. Козулин

Руководитель
доцент, канд. техн. наук _____ (подпись, дата) Т.А. Галаган

Руководитель
магистерской программы
профессор, д-р. техн. наук _____ (подпись, дата) Е. Л. Еремин

Нормоконтроль
доцент, канд. ф.-м. наук _____ (подпись, дата) В.В. Еремина

Рецензент
доцент, канд. техн. наук _____ (подпись, дата) Т. В. Труфанова

Рецензент
Начальник группы ГИС ФКУ
«ЦУКС МЧС России по
Амурской области» _____ (подпись, дата) А. В. Постников

Благовещенск 2017

РЕФЕРАТ

Магистерская работа содержит 80 с., 34 рисунка, 20 таблиц, 3 приложения, 42 источника.

ЭКСПЕРТНАЯ СИСТЕМЫ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, СТРК-К, МЕТОДИКА ОПРЕДЕЛЕНИЯ УГРОЗ, НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП, ПРОЕКТИРОВАНИЕ, РАЗРАБОТКА, ПРОДУКЦИОННАЯ МОДЕЛЬ, ТЗ.

В работе выполнялась разработка экспертной системы для анализа и оценки информационной безопасности на предприятиях.

Цель работы – создание экспертной системы для анализа и оценки информационной безопасности предприятия. Оценка и анализ ИС проводятся на основании актуальных методик оценки ИБ, предложенных ФСТЭК РФ.

Выполнение работы включает несколько этапов. Первым этапом является исследование предметной области – возможности и структуру экспертных систем, проанализированы модели данных, используемых в экспертных системах. Изучены методы оценки информационной безопасности. Выполнен анализ моделей угроз ИБ. На втором этапе определен функциональный состав разрабатываемой экспертной системы. Спроектирована объектно-ориентированная модель данных разрабатываемой системы. В качестве среды реализации выбрана система 1С: Предприятие 8.3. Следующим этапом является программная реализация и тестирование экспертной системы. Для системы реализован пользовательский интерфейс, реализована модель данных как набор

справочников и документов. Сформированы и введены правила оценки экспертной безопасности на предприятии.

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей дипломной работе использованы ссылки на следующие стандарты и нормативные документы:

ГОСТ 2.104–68 ЕСКД Основные надписи

ГОСТ 2.105–95 ЕСКД Общие требования к текстовым документам

ГОСТ 2.111–68 ЕСКД Нормоконтроль

ГОСТ 7.1–2003 Библиографическое описание документа. Общие требования и правила составления

ГОСТ 19.201–78 ЕСПД Техническое задание. Требования к содержанию и оформлению

ГОСТ 19.401–78 ЕСПД Текст программы. Требования к содержанию и оформлению

ГОСТ 19.402–78 ЕСПД Описание программы

ГОСТ 19.404–79 ЕСПД Пояснительная записка. Требования к содержанию и оформлению

ГОСТ ИСО/МЭК 15408–2–2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

ГОСТ ИСО/МЭК 15408–3–2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

ГОСТ Р 50739–95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

ГОСТ Р 50922–2006. Защита информации. Основные термины и определения.

ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

ГОСТ Р 50.1.053–2005. Информационные технологии. Основные термины и определения в области технической зашиты информации.

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

БД	база данных
ЭС	экспертная система
ИС	информационная система
БЗ	база знаний
ИБ	информационная безопасность
ОРД	организационно распорядительная документация
ОС	операционная система
ПО	программное обеспечение
ПК	персональный компьютер
ФСТЭК	Федеральная служба по техническому и экспортному контролю
РФ	Российская Федерация
ЭВМ	электронная вычислительная машина
ИС	информационная система
ИТ	информационные технологии
АРМ	автоматизированное рабочее место
НСД	несанкционированный доступ
СВТ	средство вычислительной техники
СЗИ	средство защиты информации

ВВЕДЕНИЕ

Современные экспертные системы широко используются для тиражирования опыта и знаний ведущих специалистов практически во всех сферах деятельности. Традиционно знания существуют в двух видах – коллективный опыт и личный опыт. Если большая часть знаний в предлагаемой области представлена в виде коллективного опыта, эта предметная область не нуждается в экспертных системах. Если в предметной области большая часть знаний является личным опытом специалистов высокого уровня (экспертов), если эти знания по каким-либо причинам слабо структурированы, такая предметная область нуждается в экспертных системах.

Экспертные системы – это сложные программные комплексы, аккумулирующие знания специалистов в конкретных предметных областях и тиражирующие этот эмпирический опыт для консультаций менее квалифицированных пользователей.

Объектом исследования в данной работе является экспертная система для анализа и оценки информационной безопасности.

Предметом исследования является экспертная система оценки информационной безопасности.

Целью работы является создание экспертной системы для анализа и оценки информационной безопасности.

Для достижения поставленной цели необходимо решить следующие задачи:

– Исследовать возможности и структуру экспертных систем, проанализировать модели данных, используемых в экспертных системах.

– Изучить методы оценки информационной безопасности, определить алгоритмы проведения экспертной оценки.

– Определить функциональный состав разрабатываемой экспертной системы, спроектировать алгоритмы выполнения экспертных процедур, на основе введенных данных.

– Спроектировать модель данных разрабатываемой системы, выбрать среду реализации системы.

– Реализовать систему: реализовать интерфейс, модель данных, алгоритмы обработки информации для проведения экспертной оценки и экспертного анализа информационной безопасности информационной системы.

– Сформировать и ввести экспертные правила оценки и анализа информационной безопасности на предприятии, провести тестирование системы.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Современное состояние экспертных систем

В последнее время исследователями уделяется большое внимание системам, способным решить неформализованные задачи и решать задачи конкретной предметной области в отсутствие специалиста -эксперта. Подобные системы называются экспертными.

Под экспертной системой понимается система, объединяющая возможности компьютера со знаниями и опытом эксперта в такой форме, что система может предложить разумный совет или осуществить разумное решение поставленной задачи. Дополнительно желаемой характеристикой такой системы является способность системы пояснять по требованию ход своих рассуждений в понятной для спрашивающего форме.

Экспертные системы имеют ряд особенностей, отличающих их от информационных систем других видов.

Во-первых, подобные системы обрабатывают информацию об объектах реального мира; при этом системами выполняются операции, требующие наличия и использования значительного опыта, накопленного экспертом.

Во-вторых, экспертная система за достаточно короткое время должна уметь решить задачу таким образом, чтобы решение было не хуже того, что предложил бы эксперт в данной предметной области.

В-третьих, помимо предложенного решения, экспертная система должна предоставить объяснение решения, доказать обоснованность предложенного решения, при наличии альтернативных решений – предоставить их с объяснением, почему выбран именно такой вариант. При этом, экспертная система должна работать с широким кругом пользователей и объясняться на языке данной предметной области.

В соответствии с определением можно выделить следующий базовый структурные элементы экспертной системы:

– поскольку экспертная система является системой, основанной на знаниях, то такая система должна содержать базу знаний. Иногда для представления фактических данных используется база данных и база процедурных знаний;

– для наполнения базы знаний необходим модуль приобретения знаний;

– для формирования решения поставленной задачи в экспертной системе необходим механизм логических выводов;

– для правильной передачи ответов пользователю в удобной для него форме необходим пользовательский интерфейс; также он необходим эксперту для осуществления манипуляций со знаниями.

– для объяснения решения задачи необходим модуль советов и объяснений. Следует отметить, что механизм объяснений играет весьма важную роль, позволяя повысить степень доверия пользователя к полученному результат-ту. Кроме того, он важен не только для пользователя системы, но и для эксперта, который с его помощью определяет, как работает система и как используются предоставленные им знания [48].

Базовая структура экспертной системы показана на рисунке 1.

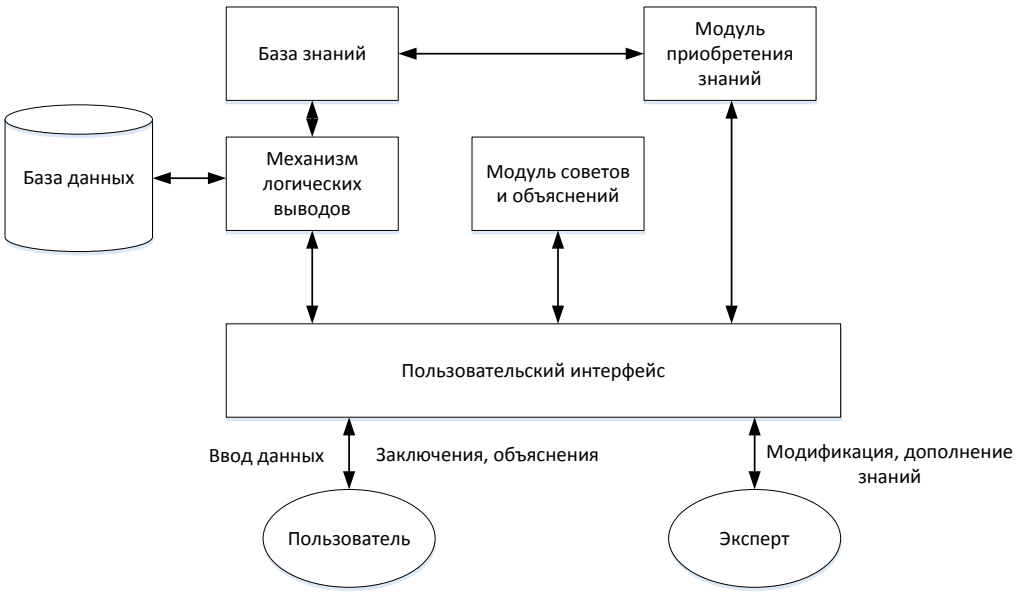


Рисунок 1 – Структура экспертной системы

Перечисленные структурные элементы являются наиболее характерными для большинства экспертных систем, хотя в реальных условиях некоторые из них могут отсутствовать.

Экспертная система должна уметь взять на себя те функции, которые выполняет специалист-эксперт или выполнить роль ассистента (советчика) для лица, принимающего решения. Использование экспертных систем позволит управляющей информационной системе получать решение непосредственно от программы и полностью исключить необходимость использования человека в управляющей системе. С другой стороны, экспертная система может повысить эффективность работы человека, предлагая наиболее верное решение поставленной задачи [47].

Важность экспертных систем состоит в следующем:

– технология экспертных систем существенно расширяет круг практически значимых задач, решаемых на компьютерах, решение которых приносит значительный экономический эффект;

– ЭС будут играть ведущую роль во всех фазах проектирования, разработки, производства, распределения, продажи, поддержки и оказания услуг;

– технология ЭС, получившая коммерческое распространение, обеспечит революционный прорыв в создании интеллектуально взаимодействующих модулей.

Процесс построения экспертной системы можно разделить на 6 относительно независимых этапов:

1) Выбор подходящей проблемы. При неправильном выборе проблемы возможно создание экспертной системы, которая не решает поставленных задач и вообще не может быть реализована. В рамках этого этапа выполняются следующие задачи:

– определение проблемной области и круга решаемых задач;

– определение эксперта, с которым будет сотрудничать разработчик;

– предварительное определение подходов к решению задачи;

– анализ экономической эффективности разработки;

– подготовка плана разработки.

2) Создание прототипа системы. Прототип является усеченной версией экспертной системы, спроектированной для проверки правильности кодирования фактов, связей и стратегий рассуждения эксперта. В рамках этого этапа

производится извлечение знаний от эксперта, структурирование знаний, формализация процедурных правил и реализация прототипа.

3) Доработка системы. При успешном создании и тестировании прототипа, экспертную систему необходимо доработать до промышленного состояния. Основная работа на данном этапе заключается в существенном расширении базы знаний, то есть в добавлении большого числа дополнительных правил, фреймов, узлов семантической сети или других элементов знаний. Эти элементы знаний обычно увеличивают глубину системы, обеспечивая большее число правил для трудно уловимых аспектов отдельных случаев.

4) Оценка экспертной системы. После завершения этапа разработки промышленной экспертной системы необходимо провести ее тестирование в отношении критериев эффективности. К тестированию широко привлекаются другие эксперты с целью апробирования работоспособности системы на различных примерах. Экспертные системы оцениваются главным образом для того, чтобы проверить точность работы программы и ее полезность. Оценку можно проводить, исходя из различных критериев:

– критерии пользователей (понятность и «прозрачность» работы системы, удобство интерфейсов и др.);

– критерии приглашенных экспертов (оценка советов-решений, предлагаемых системой, сравнение ее с собственными решениями, оценка подсистемы объяснений и др.);

– критерии коллектива разработчиков (эффективность реализации, производительность, время отклика, дизайн, широта охвата предметной области, непротиворечивость БЗ, количество тупиковых ситуаций, когда система не может принять решение, анализ чувствительности программы к незначительным изменениям в представлении знаний, весовых коэффициентах, применяемых в механизмах логического вывода, данных и т. п.).

5) Стыковка системы. Выполняется интеграция экспертной системы с другими информационными системами в среде, в которой она будет работать, и обучение персонала. Также обеспечивается связь экспертной системы с базами

данных, существующими на предприятии.

6) Поддержка системы. Данный этап подразумевает постоянное обновление базы знаний, добавление новых правил и логических конструкций [48].

1.2 Анализ моделей данных экспертных систем

Представление знаний в экспертных системах должно удовлетворять двум противоречивым требованиям – первое требование означает способность представлять сложные системы понятий и объективно описывать отношения между этими понятиями, второе требование предполагает, что логика предикатов обладает четкими механизмами вывода, которые позволяют решать задачи на основе этого представления. В более общих представлениях, обладающих большей выразительной силой, механизмы вывода оказываются либо гораздо сложнее, либо гораздо слабее.

Экспертное знание часто представляется в виде правил или как данные в компьютере. В зависимости от требований эти правила и данные могут использоваться повторно. Экспертные системы на основе правил применяются в планировании, проектировании, распределении средств по задачам, контроле неисправностей и диагностике. [44].

Существуют десятки моделей представления знаний для различных предметных областей. Наиболее популярные из них следующие.

1. Продукционная модель – модель, позволяющая представить знания предложениями, которые называют продукциями. Продукции имеют вид «Если (условие), то (действие)». Условием (антецедентом) считается некоторое предложение-образец, по которому осуществляется поиск в базе знаний, а действием (консеквентом) – операции, которые выполняются при успешном поиске.

Существуют две основные стратегии вывода на множестве правил-продукций:

– прямой вывод (вывод от исходных данных-фактов, аксиом - к цели, по пути вывода пополняя исходную базу знаний новыми полученными истинными фактами; процесс заканчивается лишь тогда, когда выведен факт, эквивалентный искомому);

– обратный вывод (вывод от целевого факта к данным, на очередном шаге отыскивается очередной факт, в заключительной части содержится факт, эквивалентный исходному факту; процесс заканчивается тогда, когда для каждого факта, выведенного на очередном шаге, не будет найдено правило, имеющее этот факт в качестве заключения, а посылками - исходные или выведенные на предыдущих шагах факты) [51].

К достоинствам продукционной модели относятся наглядность, высокая модульность, простота внесения дополнений и изменений. Недостатком данной модели является то, что при накоплении достаточно большого количества продукций они могут противоречить друг другу.

Существует большое количество программных средств, реализующих продукционный подход: язык OPS 5, оболочки ЭС – EXSYS Professional, Kappa и др.

2. Семантическая сеть представляет собой ориентированный граф, вершины которого отображают некоторые понятия, а дуги – отношения между ними. Таким образом, семантическая сеть отражает семантику предметной области в виде понятий и отношений.

Характерная особенность семантических сетей - наличие трех типов отношений:

– класс - элемент класса;

– свойство - значение;

– пример элемента класса [51].

Недостатком данной модели представления знаний является сложность организации процедуры поиска вывода на семантической сети.

3. Фреймовая модель представления знаний задает остов описания класса объектов и удобна для описания структуры и характеристик однотипных объектов (процессов, событий) описываемых фреймами - специальными ячейками (шаблонами понятий) фреймовой сети. Фрейм – это абстрактный образ для представления некоего стереотипа информации [51]. Основным преимуществом фреймовой модели представления знаний является то, что она отражает

концептуальную основу организации памяти человека, а также ее гибкость и наглядность.

Специальные языки представления знаний в сетях фреймов FRL (Frame Representation Language), KRL (Knowledge Representation Language), фреймовая оболочка Kappa и другие программные средства позволяют эффективно строить промышленные ЭС. Широко известны такие фрейм-ориентированные экспертные системы, как ANALYST, МОДИС, TRISTAN, ALTERID [51].

В ходе исследования был проведен сравнительный анализ моделей представления знаний, приведенный в таблице 1.

Таблица 1 – Сравнительный анализ моделей представления знаний

МПЗ	Преимущества	Недостатки	Программы-оболочки	Пример реализации
Продукционная	Простота представления знаний и логических выводов	Элементы знаний могут вступать в противоречие друг с другом при большом количестве знаний	OPS 5	R1/XCON - система для помощи разработчикам при определении конфигурации вычислительной системы на базе вычислительных устройств и блоков семейства VAX
			EXSYS Professional	Cessna Diagnostic & Repair Systems Cessna Aircraft – программа для диагностики и ремонта реактивных систем корпорации Cessna

Продолжение таблицы 1

			KAPPA	Saphir NL: Анализ данных высокой частоты и разрешения, записанных во время остановки скважины
Семантическая	Наглядность представления знаний Простота решения Возможность использования математических методов	Сложность поиска и вывод решения Громоздкость выражений	SIMER+ MIR	Экспертная система "Определение качества питьевой воды"
				PROSPECTOR – геологоразведочная система
			CASNET	CASNET/GLAUCOMA - диагностирует болезненные состояния, связанные с глаукомой, и строит планы их лечения.

Фреймовая	Полное теоретическое обоснование модели Возможность реализации любого механизма вывода	Затруднение при обмене больших объемов данных между объектами Сложность обработки Отсутствие встроенного механизма вывода	FRL (потомок LISP)	KNOBS - помогает офицеру тактического центра управления ВВС планировать операции.

Продолжение таблицы 1

			Fuzzy CLIPS (потомок LISP)	Экспертная система технологического процесса для единичного и мелкосерийного производства РЭА
			FRANZ (потомок LISP)	ANALYST строит схему развертывания боевых соединений противника в режиме реального времени на основании сообщений от многих источников инструментальных данных

В семантической модели, где знания представлены наиболее наглядно, возникают проблемы с дискретизацией элементов. Фреймовая модель

предоставляет максимум творческой свободы, однако, эта свобода может привести к излишним затратам сил и вычислительных мощностей. В построении базы знаний, прежде всего, важна простота построения алгоритма, а также наибольшая приближённость к человеческому мышлению [55].

Наиболее удачными для применения в построении базы знаний для требуемой экспертной системы являются продукционная и фреймовая модель представления знаний.

1.3 Модели и требования информационной безопасности

Основными органами государственной системы защиты информации являются:

–Межведомственная комиссия по защите государственной тайны;

–Федеральная служба по техническому и экспортному контролю (ФСТЭК) России;

–Федеральная служба безопасности (ФСБ) РФ;

–другие органы исполнительной федеральной власти и их структурные подразделения по защите информации;

–органы исполнительной власти субъектов федерации и их структурные подразделения;

–структурные подразделения и штатные специалисты по защите информации организаций (предприятий, учреждений) [30].

Основные методы обеспечения информационной безопасности рассмотрены в Концепции национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24) [4] и Доктрине информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895 [3].

Основные принципы информационного взаимодействия и защиты информации рассмотрены в следующих федеральных законах:

1. № 149-ФЗ «Об информации, информационных технологиях и защите информации» от 27.07.2006 г [2].

2. № 152-ФЗ «О персональных данных» от 27.07.2006 г [1].

В законе «Об информации, информационных технологиях и защите информации» определены меры защиты информации, а также определено, что именно входит в защиту информации.

В законе «О персональных данных» прописаны способы и условия обработки персональных данных, их хранения и защиты. Практически на всех предприятиях обрабатываются персональные данные сотрудников, поэтому при определении мер защиты необходимо опираться на положения данного закона.

Организация защиты информации на предприятии должна быть построена в соответствии со следующими стандартами [6-25].

Федеральной службой по техническому и экспортному контролю (ФСТЭК России) разработан ряд регламентирующих документов [6-15],

Очевидно, что отправными моделями при анализе информационной безопасности предприятия являются модель угроз информационной безопасности и модель нарушителя информационной безопасности.

Базовая модель угроз безопасности данных при их обработке в информационных системах содержит систематизированный перечень угроз безопасности данных при их обработке в информационных системах [7]. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения информационной безопасности, которое ведет к ущербу жизненно важных интересов личности, общества и государства. Модель угроз содержит единые исходные данные по угрозам безопасности данных, обрабатываемых в информационных системах, связанным:

– с перехватом (съемом) данных по техническим каналам с целью их копирования или неправомерного распространения;

– с несанкционированным, в том числе случайным, доступом в ИС с целью изменения, копирования, неправомерного распространения данных или деструктивных воздействий на элементы ИС и обрабатываемых в них данных с

использованием программных и программно-аппаратных средств с целью уничтожения или блокирования данных.

В данном документе определены частные модели информационной безопасности для следующих классов систем:

–автоматизированные рабочие места, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

–автоматизированные рабочие места, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

–локальные ИС, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

–локальные ИС, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

–распределенные ИС, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

–распределенные ИС, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

На основании классификации, приведенной в [7], можно составить сравнительный обзор моделей угроз приведен в таблице 2.

Таблица 2 – Сравнительный обзор моделей угроз ИБ

Класс систем	Локальные угрозы	Внешние угрозы	Специфические угрозы
Автоматизированные рабочие места не подключенные к сетям общего использования , а так же международного обмена информацией.	угрозы НСД к персональным данным, обрабатываемым на АРМ. угрозы утечки акустической (речевой) информации; угрозы утечки видовой информации; угрозы утечки информации по каналу побочные электро-		

	магнитные излучения и наводки; угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов		
Автоматизированные рабочие места, использующие сети связи общего пользования, а так же сетям международного обмена информацией.		угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации; угрозы сканирования, направленные на выявление типа ОС	угрозы получения НСД путем подмены доверенного объекта;
локальные информационные системы, не подключенные к сетям связи общего пользования и/или сетям международного информационного обмена	модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой; угрозы, которые реализуются после загрузки ОС и направленные на несанкционированный доступ с применением стандартных функций (удаление, копирование, перемещение и т.п.) операционной системы или какого-либо прикладного ПО (например, СУБД), с применением специально созданных для выполнения несанкционированного доступа программ (например,	Автоматизированные рабочие места, открытых портов и служб, открытых соединений и др.; угрозы выявления паролей; угрозы удаленного запуска приложений; угрозы внедрения вредоносных программ по сети; угрозы получения НСД с помощью подмены доверенного объекта;	угрозы получения несанкционированного доступа путем подмены доверенного объекта;

	просмотр и изменение реестра ПК, поиск текста в текстовых файлах и т.п.);		
локальные ИС, подключенные к сетям связи общего пользования и/или сетям международного информационного обмена			угрозы сканирования, направленные на выявление типа ОС информационной системы, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;
распределенные ИС, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;			угрозы внедрения ложного объекта сети; угрозы навязывания ложного маршрута путем несанкционирванного редактирования маршрутно-адресных данных;
распределенные информационные системы, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.	поиска текстов в текстовых файлах и т.п.); угрозы внедрения вредоносных программ	угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации; угрозы сканирования.	угрозы внедрения ложного объекта как в ИС, так и во внешних сетях; угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри, так и во

			внешних.

Как видно из таблицы, большинство угроз характерны для всех видов АРМ и ИС, особые угрозы связаны с подключением ИС к сетям международного обмена.

Методика определения актуальных угроз безопасности содержит порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных. В соответствии с методикой оцениваются показатели исходной защищенности данных, в зависимости от количественной оценки составляется перечень актуальных угроз и количественная оценка вероятности каждой угрозы. С использованием данных о классе ИС и составленного перечня актуальных угроз, на основе «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» формулируются конкретные организационно-технические требования по защите ИС от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИС.

В соответствии с Постановлением № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г [5], при обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

1.4 Методики оценки информационной безопасности

Общий алгоритм проведения оценки безопасности информационной системы приведен на рисунке 2.

Рисунок 2 – Алгоритм оценки информационной безопасности на предприятии

Процесс оценки рисков информационной безопасности как комплексного подхода производится сотрудниками компании совместно с руководством, а также с представителями разных отделов предприятия.

Этап 1. Идентификация активов. На этом этапе эксперты интервьюируют персонал каждого подразделения или отдела, чтобы выявить используемые активы. Данные активы системы информационных технологий являются компонентами или частями общей информационной системы, в которую предприятие вкладывает средства и которым, соответственно, требуется защита. При идентификации активов следует иметь в виду, что любая информационная система включает в себя не только аппаратные, но и программные средства. Существуют следующие типы активов: информация/данные (то есть файлы, содержащие информацию о платежах или продукте); аппаратные средства (компьютеры, принтеры); программное обеспечение, включая прикладные программы (например, программы обработки текстов, программы целевого назначения); оборудование для обеспечения связи (например, телефоны, медные и оптоволоконные кабели); программно-аппаратные средства (например, электронные носители информации); документы (договоры, контракты); продукция предприятия; услуги (например, информационные, вычислительные услуги); конфиденциальность и доверие при оказании услуг (например, услуг по совершению платежей); обеспечивающее оборудование, необходимое для создания необходимых условий работы; персонал организации.

Этап 2. Определение риска несоответствия требованиям законодательства в области ИБ. Всякая организация, имеющая информационные системы, должна соблюдать федеральные законы в этой отрасли. Неисполнение данных требований влечет за собой гражданскую, уголовную, административную и иную предусмотренную законодательством Российской Федерации ответственность. Риск невыполнения требований законодательства влияет на общий риск ИБ.

Методика определения риска несоответствия требованиям законодательства в области ИБ содержит в себе осуществление многостороннего анализа состояния системы защиты для дальнейшего определения выполнения требований в соответствии с законодательством. В процессе проведения анализа, всем требованиям, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются. В заключение анализа необходимо определить уровень риска несоответствия требований по ИБ.

Этап 3. Разработка модели угроз. В методике с целью максимально точного определения риска ИБ необходимо разработать частную модель угроз ИБ предприятию. Для определения модели угроз можно воспользоваться базовой моделью, описанной в [7]. Определение вероятности наступления неблагоприятных событий определяется экспертом или группой экспертов, занимающихся разработкой модели угроз. Экспертным методом определяется и актуальность угроз ИБ. После завершения оценки угроз составляют перечень актуальных идентифицированных угроз на каждый идентифицированный актив или групп активов, подверженных этим угрозам, а также определяют вероятность реализации угроз [60].

Этап 4. Процедура количественной оценки рисков ИБ. Основным этапом в процессе оценки рисков является процедура количественного определения рисков ИБ. Пошаговый алгоритм количественного определения риска ИБ представлен на рисунке 3.

Рисунок 3 – Алгоритм количественной оценки ИБ

Принять риск – значит осознать его, смириться с его возможностью и продолжить действовать как прежде. Применимо для угроз с малым ущербом и малой вероятностью возникновения.

Снизить риск – значит ввести дополнительные меры и средства защиты, провести обучение персонала и т д. То есть провести намеренную работу по снижению риска. При этом необходимо произвести количественную оценку эффективности дополнительных мер и средств защиты. Все затраты, которые несет организация, начиная от закупки средств защиты до ввода в эксплуатацию (включая

установку, настройку, обучение, сопровождение и проч.), не должны превышать размера ущерба от реализации угрозы.

Перенести риск – значит переложить последствия от реализации риска на третье лицо, например, с помощью страхования.

В результате количественной оценки рисков должны быть определены:

– ценность активов в денежном выражении;

– полный список всех угроз ИБ с ущербом от разового инцидента по каждой угрозе;

– частота реализации каждой угрозы;

– потенциальный ущерб от каждой угрозы;

– рекомендуемые меры безопасности, контрмеры и действия по каждой угрозе.

При качественном подходе не используются количественные или денежные выражения для объекта оценки. Вместо этого объекту оценки присваивается показатель, проранжированный по трехбалльной (низкий, средний, высокий), пятибалльной или десятибалльной шкале (0… 10). Для сбора данных при качественной оценке рисков применяются опросы целевых групп, интервьюирование, анкетирование, личные встречи.

Анализ рисков информационной безопасности качественным методом должен проводиться с привлечением сотрудников, имеющих опыт и компетенции в той области, в которой рассматриваются угрозы.

Алгоритм качественной оценки ИБ представлен на рисунке 4.

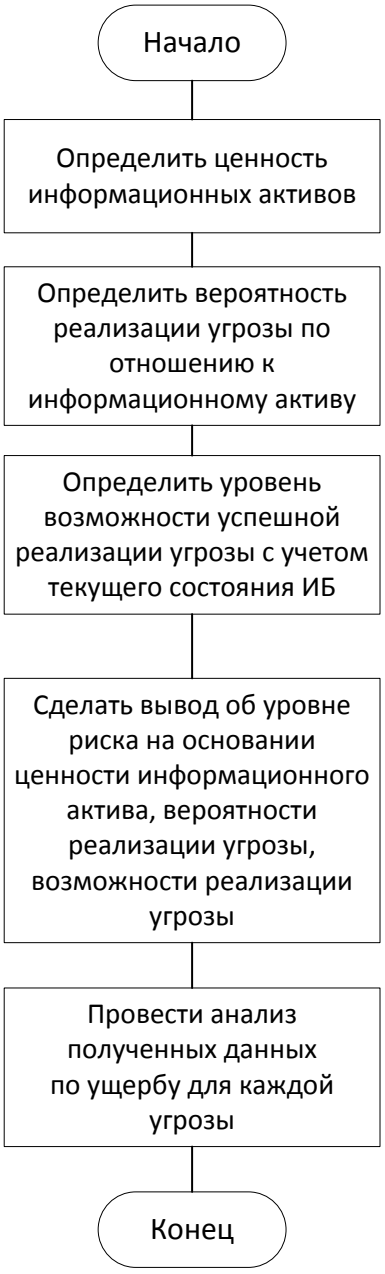


Рисунок 4 – Алгоритм качественной оценки ИБ

На первом шаге необходимо определить ценность информационных активов. Ценность актива можно определить по уровню критичности (последствиям) при нарушении характеристик безопасности (конфиденциальность, целостность, доступность) информационного актива.

На втором шаге необходимо определить вероятность реализации угрозы по отношению к информационному активу. Для оценки вероятности реализации угрозы может использоваться трехуровневая качественная шкала (низкая, средняя, высокая).

На третьем шаге необходимо определить уровень возможности успешной реализации угрозы с учетом текущего состояния ИБ, внедренных мер и средств защиты. Для оценки уровня возможности реализации угрозы также может использоваться трехуровневая качественная шкала (низкая, средняя, высокая). Значение возможности реализации угрозы показывает, насколько выполнимо успешное осуществление угрозы.

На четвертом шаге необходимо сделать вывод об уровне риска на основании ценности информационного актива, вероятности реализации угрозы, возможности реализации угрозы. Для определения уровня риска можно использовать пятибалльную или десятибалльную шкалу. При определении уровня риска можно использовать эталонные таблицы, дающие понимание, какие комбинации показателей (ценность, вероятность, возможность) к какому уровню риска приводят.

На последнем шаге необходимо провести анализ полученных данных по каждой угрозе и полученному для нее уровню риска. Часто группа анализа рисков оперирует понятием «приемлемый уровень риска». Это уровень риска, который компания готова принять (если угроза обладает уровнем риска меньшим или равным приемлемому, то она не считается актуальной). Глобальная задача при качественной оценке — снизить риски до приемлемого уровня.

После проведения оценки ИБ необходимо разработать меры безопасности, контрмеры и действия по каждой актуальной угрозе для снижения уровня риска.

1.5 Опыт применения экспертных систем для оценки ИБ

Экспертные системы могут применяться для оценки и анализа состояния информационной безопасности. На эту тему опубликован ряд научных работ. В [61] показаны преимущества использования ЭС для анализа и оценки ИБ:

- во-первых, появляется возможность решения сложных задач с привлечением нового, специально разработанного для этих целей математического аппарата (семантических сетей, фреймов, нечеткой логики);

- во-вторых, применение экспертных систем позволяет значительно повысить эффективность, качество и оперативность решений за счет аккумуляции знаний экспертов высшей квалификации;

- в-третьих, экспертные системы ориентированы на эксплуатацию широким кругом специалистов, общение с которыми происходит с использованием понятной им техники рассуждений и терминологии.

Использование экспертных систем способствует проведению анализа и оценки ИБ конкретными специалистами по защите информации в различных организациях без привлечения дополнительных и более квалифицированных кадров. В основе интеллектуального решения проблем лежит принцип воспроизведения знаний опытных специалистов-экспертов. Использование эвристик позволяет существенно сокращать количество альтернативных вариантов при поиске рационального решения нестандартных задач. Относительно несложные эвристики и знания многих экспертов могут быть представлены формально и реализованы с помощью ЭС. Основное предназначение ЭС состоит в том, что они выступают в качестве своеобразного помощника или усилителя интеллектуальной деятельности специалиста в конкретной предметной области.

В [62] показано, что экспертные системы используются для решения следующих задач ИБ:

— оценка рисков и составление модели угроз;

— антивирусное программное обеспечение;

— аудит информационной безопасности предприятия;

В частности, такие антивирусные средства, как ESET Threat Sense, Kaspersky, Dr.Web Katana используют в своей работе эвристический анализ. В данных продукта эвристический анализ представляет собой технологию обнаружения угроз, неопределяемых с помощью антивирусных баз. Эта технология позволяет находить объекты, которые подозреваются на заражение неизвестным вирусом или новой модификацией известного.

В работе [64] приведен пример разработки экспертной системы для оценки уровня ИБ для конкретного предприятия. В работе показано, что решение

поставленной задачи сводится к последовательной формализации угроз ИБ, ресурсов организации, оценки уровня ИБ, генерации вариантов мероприятий по обеспечению ИБ и выборе оптимального варианта обеспечения ИБ. Автором работы предложена модель классов, в которой угроза ИБ организации представляется в виде класса, содержащего имя, характеристику и объекты, которые в свою очередь обладают определяющими угрозу свойствами. Имя класса угроз содержит информацию, необходимую для определения данного класса угроз, и имеет уникальный идентификатор. Характеристика класса содержит общее описание угроз и обобщает участие объектов в нем. Такая структура позволяет описывать множество угроз и добавлять новые.

В то же время, существует ряд готовых промышленных решений, использующих экспертные системы для обеспечения информационной безопасности. К ним можно отнести, например, следующие системы [65].

CRAMM - инструментальное средство, реализующее одноименную методику, которая была разработана компанией BIS Applied Systems Limited по заказу британского правительства. Метод CRAMM позволяет производить анализ рисков и решать ряд других аудиторских задач: обследование информационной системы, проведение аудита в соответствии с требованиями стандарта BS 7799, разработка политики безопасности.

Данная методика опирается на оценки качественного характера, получаемые от экспертов, но на их базе строит уже количественную оценку. Метод является универсальным и подходит и для больших, и для малых организаций как правительственного, так и коммерческого сектора.

Digital Security Office 2006 – система управления информационными рисками и оценки соответствия системы управления ИБ международным, национальным и корпоративным стандартам в области информационной безопасности. Продукт состоит из системы анализа рисков ГРИФ и системы для оценки соответствия системы управления ИБ требованиям стандартов КОНДОР. Система ГРИФ позволяет построить приближенную модель информационной системы, содержащую наиболее критичные ресурсы и основные угрозы, и уязвимости, с

учетом вероятности их реализации. Полученная модель показывает наиболее уязвимые места ИС, уровень ущерба, к которому может привести каждая уязвимость, а также позволяет принять решение о том, какие контрмеры будут наиболее эффективны. В нем разработано гибкое и, несмотря на скрытый от пользователя сложнейший алгоритм, учитывающий более 100 параметров, максимально простое в использовании программное решение, основная задача которого дать возможность ИТ-менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе и эффективность существующей практики по обеспечению безопасности компании. Данный комплекс делает оценку рисков по различным информационным ресурсам, подсчитывает суммарный риск по ресурсам компании, а также ведет подсчет соотношения ущерба и риска и выдает недостатки существующей политики безопасности. В системе есть модуль управления рисками, который позволяет проанализировать все причины того значения риска, который получается после обработки алгоритмом занесенных данных. Здесь можно задать контрмеры, их стоимость и влияние на уровень риска.

Система КОНДОР включает в себя базы стандартов управления информационной безопасностью (ISO 17799:2000, ISO 17799:2005, ISO 27001, СТО БР ИББС-1.0-2006), представленных в виде перечня требований. Анализируя выполнение каждого требования, система, формируя отчёт, позволяет получить полную картину – какие положения стандартов выполняются, а какие нет. Также в системе предусмотрена возможность создавать свои базы требований, чтобы провести оценку соответствия, например, корпоративному стандарту безопасности. В отчете отражаются все положения политики безопасности, которые соответствуют и не соответствуют стандарту, а также существующий уровень риска невыполнения требований политики безопасности в соответствии со стандартом. Элементам, которые не выполняются, даются комментарии и рекомендации экспертов. По желанию специалиста, работающего с программой, могут быть выбраны генерация отчета, например, по какому-то одному или нескольким разделам стандарта ISO 17799, общий подробный отчет с комментариями, общий

отчет о состоянии политики безопасности без комментариев для представления руководству. Все варианты отчетов для большей наглядности сопровождаются диаграммами. КОНДОР дает возможность специалисту отслеживать вносимые на основе выданных рекомендаций изменения в политику безопасности, постепенно приводя ее в полное соответствие с требованиями стандарта. Существует возможность сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности. Данная система реализует метод качественной оценки рисков по уровневой шкале рисков: высокий, средний, низкий [65].

2 ПРОЕКТИРОВАНИЕ ЭКСПЕРТНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 Определение функций экспертной системы

Все функции экспертной системы можно разделить на основные и вспомогательные. Основные функции обеспечивают выполнение основных задач системы. Вспомогательные функции обеспечивают решение служебных задач: предоставление интерфейса, разграничение прав доступа, администрирование базы знаний. Дерево функций экспертной системы показано на рисунке 5.

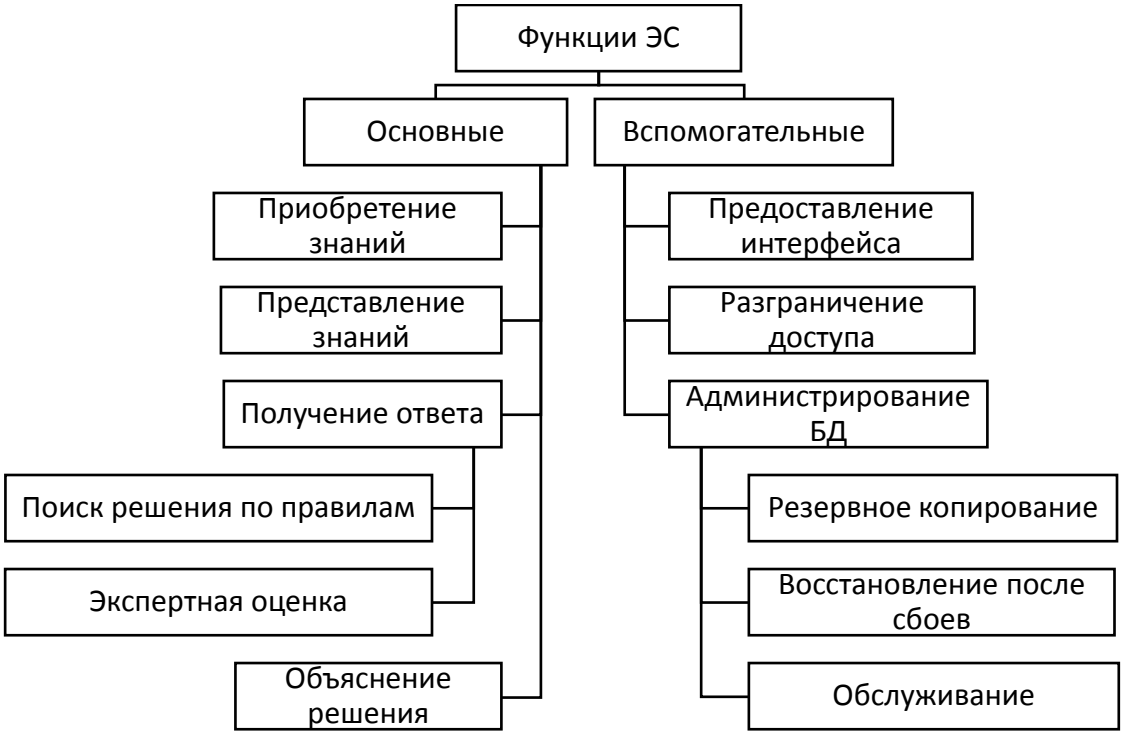


Рисунок 5 – Функции экспертной системы

К основным функциям экспертной системы относятся:

– приобретение знаний

– представление знаний;

– получение ответа;

– объяснение решения.

Функция приобретения знаний предполагает возможность ввод знаний в базу знаний экспертом. Выполнение данной функции предполагает: предоставление интуитивно-понятного интерфейса для эксперта; обеспечение ввода экспертных правил в базу знаний; обеспечение защиты от ошибок при вводе правил;

обеспечение сохранения введенных знаний в базе знаний; обеспечение возможности редактирования, добавления и удаления правил с сохранением целостности базы знаний.

Данная функция позволяет ввести в базу знания следующего характера:

– знания о симптомах различных инцидентов информационной безопасности. Инцидент информационной безопасности – это единичное событие информационной безопасности, которое может привести к угрозе информационной безопасности. Данные знания необходимы для идентификации угроз ИБ.

– знания о требованиях ИБ, например, указанных в СТР-К. Данные знания необходимы для проведения экспертной оценки состояния ИБ на предприятии.

– знания о методиках определения угроз, указанные, например, в [11]. Эти знания необходимы для определения наиболее актуальных для предприятия угроз и получения рекомендаций.

– другие необходимые знания для оценки ИБ или получения рекомендаций по улучшению состояния ИБ на предприятии.

Функция представления знаний предполагает использование такого формата хранения знаний, чтобы их можно было с минимальными потерями перевести с естественного языка на формализованный. При этом должны сохраниться связи между знаниями. Выполнение данной функции предполагает: перевод знаний эксперта в формализованные правила; обеспечение связей между правилами (знаниями); обеспечение целостности и непротиворечивости хранимых знаний.

Для реализации данной функции должны быть разработаны специальные информационные структуры.

Для того, чтобы экспертная система могла развиваться и дополняться новыми знаниями по различным областям, необходимо предусмотреть возможность администратору системы обеспечивать создание новых хранилищ знаний для каждой новой области (например, отдельное хранилище знаний для оценки по СТР-К, отдельное хранилище для оценки угроз и т.д.).

Функция получения ответа представляет собой формирование ответа на поставленный вопрос на основании экспертных правил. Для данной экспертной

системы ответ может заключаться в одном из двух значений: экспертный поиск решения проблемы по описанным правилам; экспертная оценка события или состояния ИБ по описанным требованиям.

Для реализации данной функции необходимо разработать алгоритмы поиска решения и формирования экспертной оценки.

Функция объяснения решения необходима для проверки правильности принятого решения, для получения промежуточных результатов рассуждений, для обоснования действий пользователей после получения экспертного решения. Для реализации данной функции также должны быть разработаны специальные алгоритмы и информационные структуры.

Вспомогательные функции должны обеспечивать работу основных функций.

Одной из главных вспомогательных функций является предоставление интерфейса пользователя, обеспечивающего навигацию между подсистемами системы. Интерфейс должен быть понятным, обеспечивать:

- минимальные затраты времени специалиста на работу с системой: минимизировать ручной ввод, минимизировать дублирование, обеспечить удобство переходов и контекстный поиск;

- учет профессиональных навыков пользователя: интерфейс должен быть привычным, для работы необходимо использовать стандартные элементы управления.

Функция разграничения доступа должна обеспечивать различный доступ для эксперта, пользователя и администратора системы. Различный доступ обеспечивается за счет аутентификации пользователей; кроме того, интерфейс для разных групп пользователей должен обеспечивать только возможность навигации по разрешенным пользователю подсистемам и массивам знаний.

Функция администрирования базы данных (базы знаний) заключается в выполнении стандартных операций по администрированию БД: выполнении резервного копирования, восстановления после сбоев, ведение журнала транзакций, возможность отката транзакций, выполнение операций корректного удаления записей и т.д.

Как следует из описания, описанные функции соответствуют модулям структуры типовой экспертной системы, изображенной на рисунке 1. Данное соответствие приведено в таблице 3.

Таблица 3 – Соответствие функций структуре ЭС

Элемент структуры типовой ЭС	Функция разрабатываемой ЭС
Модуль приобретения знаний	Функция приобретения знаний Функция представления знаний
Модуль логических выводов	Функция получения ответа Функция поиска решения
Модуль советов и объяснений	Функция объяснения решения
Пользовательский интерфейс	Вспомогательные функции

2.2 Описание функциональных модулей и обеспечивающих подсистем

Состав функциональных подсистем ЭС соответствует определенным для нее функциям. В экспертной системе должны присутствовать подсистемы:

– получения знаний;

– представления знаний;

– получения ответа (с объяснением решения).

Для описания взаимодействия пользователей с подсистемами ЭС можно построить диаграмму вариантов использования UML (рисунок 6).

С разрабатываемой системой могут работать три группы пользователей:

– Эксперты: занимаются вводом знаний в экспертную систему, могут участвовать в проверке знаний ЭС;

– Администраторы: занимаются обеспечением представления знаний в требуемых форматах, обеспечением предоставления новых хранилищ для знаний;

– Пользователи: получают ответы (решения) от экспертной системы.

ЭС состоит из следующих функциональных подсистем:

– подсистема получения знаний, позволяющая эксперту внести в базу знаний необходимые знания в удобном для него виде (выполнить обучение системы).

Подсистема может быть дополнена модулем проверки знаний, которую выполняют как эксперт, так и администратор системы.

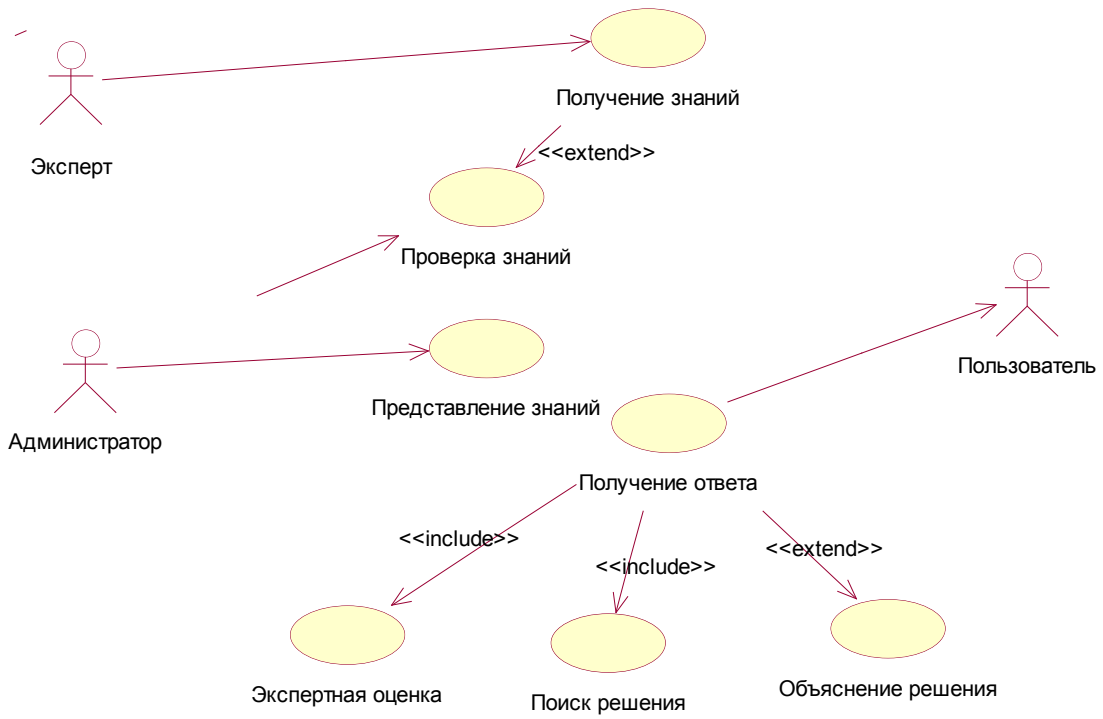


Рисунок 6 – Диаграмма вариантов использования ЭС

– подсистема представления знаний, позволяющая создать новые хранилища знаний, организовать новое обучение системы, ввести необходимые данные для последующей обработки знаний. Работа с данной подсистемой выполняется администратором ЭС;

– подсистема получения ответа от ЭС пользователем. В результате запроса или по итогам ответов на вопросы системы пользователь должен получить ответ на поставленный вопрос. Подсистема использует модули поиска решения или экспертной оценки, а также может использовать модуль объяснения решения (по требованию пользователя).

К обеспечивающим подсистемам относятся:

– подсистема управления пользователями (назначение ролей, определение прав доступа, назначение паролей);

– подсистема обслуживания базы знаний (резервирование, восстановление, ведение журнала транзакций).

Схема взаимодействия программных модулей показана на рисунке 7.

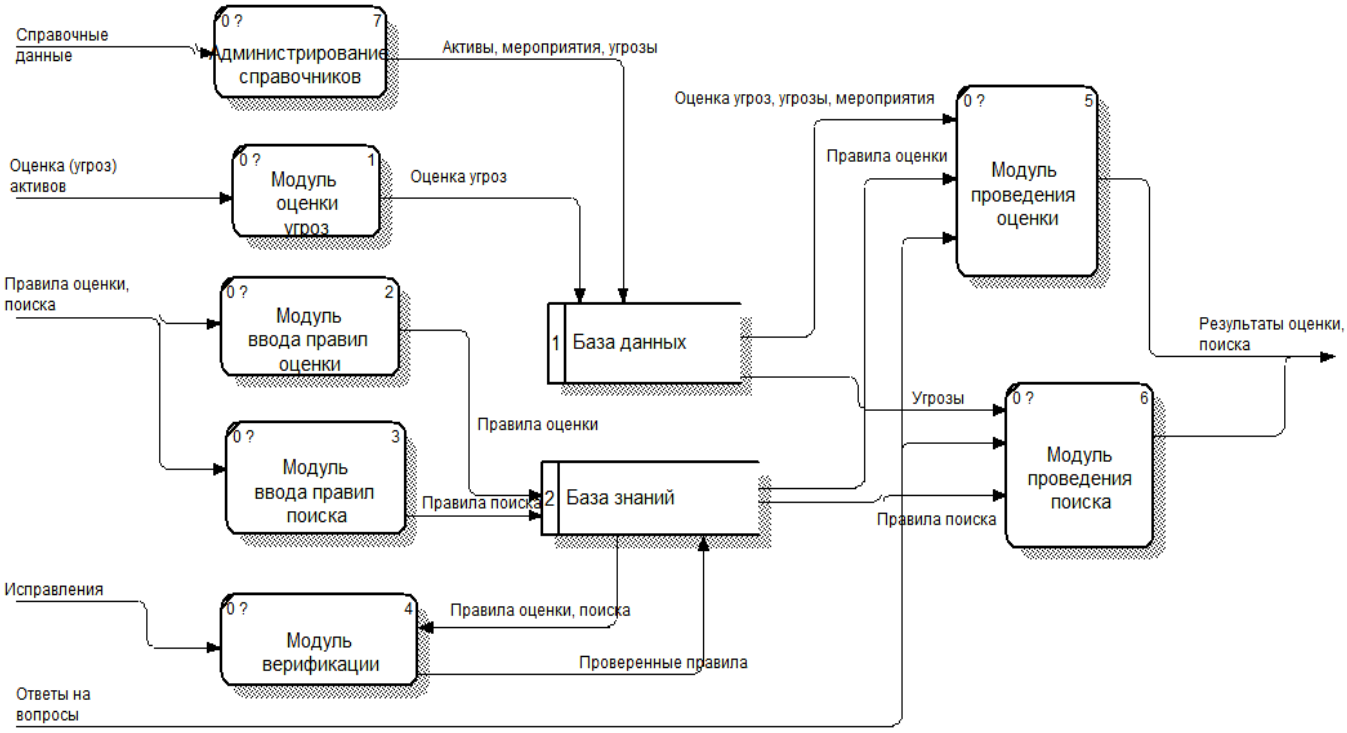


Рисунок 7 – Схема взаимодействия модулей

Как видно из рисунка, структуру программного решения составляют следующие модули:

– Модуль оценки угроз. Эксперту предлагается перечень активов, он выставляет количественную оценку угроз для данного актива.

– Модуль ввода экспертных правил. Модуль предоставляет интерфейс для ввода экспертных правил оценки, преобразования введенных правил во внутренний формат хранения, сохранения правил.

– Модуль ввода правил поиска. Модуль предоставляет интерфейс для ввода правил экспертного поиска, преобразования введенных правил во внутренний формат, сохранения правил.

– Модуль верификации. Модуль выполняет проверку введенных правил на полноту и непротиворечивость.

– Модуль администрирования БД. Группа модулей для ведения справочников, управления данными.

– Модуль проведение оценки. Модуль предоставляет интерфейс для ответа на вопросы и сохранения ответов для дальнейшей обработки. Так же модуль включает

в себя процедуру обработки оценки, формирующая результат по ответам пользователя на вопросы.

– Модуль проведения поиска. Модуль предоставляет интерфейс для ответа на вопросы и сохранения ответов для дальнейшей обработки. Так же модуль включает в себя процедуру обработки ответов пользователя, формирующая результат по ответам пользователя на вопросы.

Большинство модулей реализованы как методы соответствующих классов, как показано на рисунке 10.

2.3 Описание методики обучения экспертной системы

Обучением экспертной системы может заниматься только эксперт. Его изначальная работа – внести в базу знаний все знания, касающиеся всех известных на момент обучения ЭС угроз. Для этих целей эксперт использует информацию с сайта ФСТЭК России. Как следует из информации, представленной на сайте, обновление перечня угроз или их описания происходит не чаще 1 раза в месяц. Следовательно, внесение изменений в базу знаний достаточно несколько раз в год (в зависимости от сложности информационной системы предприятия).

Для обучения экспертной системы используется метод получения знаний извне (от эксперта) в режиме диалога.

Экспертная система в сфере информационной безопасности может быть использована для проведения двух видов процедур:

– поиск решения поставленной проблемы;

– определение соответствия поставленной цели.

Первый тип процедур может применяться, например, для поиска уровня информационной безопасности, соответствующего данной системе.

В этом случае для заполнения базы знаний необходимо воспользоваться правилами «Если – то», составляющими дерево решений. Особенность такого подхода состоит в том, что каждый следующий вопрос зависит от ответа на предыдущий. В результате цепочка вопросов и ответов должна привести к единственному правильному решению. Примером подобной реализации может служить система диагностики неполадок Windows.

Для реализации подобной системы, эксперт должен ввести в базу знаний правила продукций, состоящие из следующих компонентов (рисунок 8).

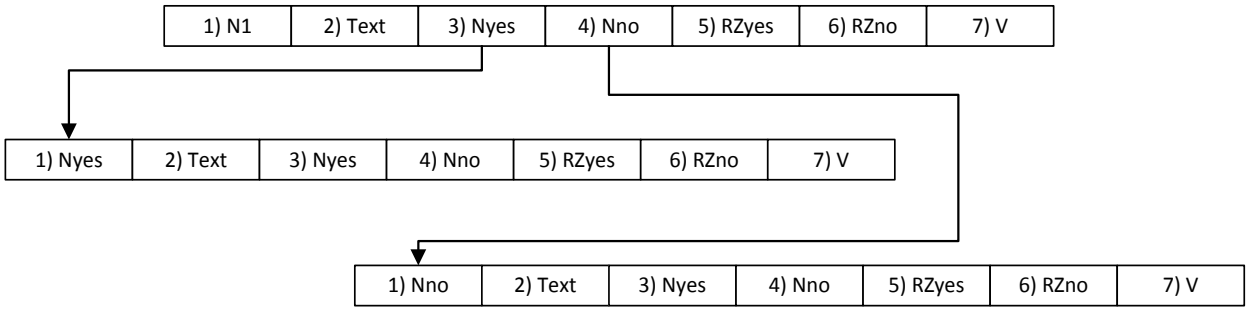


Рисунок 8 – Структура правила

1) Номер вопроса;

2) Текст вопроса, который будет задан пользователю;

3) Номер вопроса, к которому необходимо перейти при положительном ответе пользователя на вопрос;

4) Номер вопроса, к которому необходимо перейти при отрицательном ответе на вопрос;

5) Промежуточный или итоговый вывод при положительном ответе на вопрос;

6) Промежуточный или итоговый вывод при отрицательном ответе на вопрос;

7) Вес вопроса: при получении противоречивых результатов, какова вероятность того, что ответ именно на данный вопрос является верным решением.

В результате ввода знаний должно получиться дерево решений, пример которого показан на рисунке 9. Данный пример показывает только общий принцип организации дерева, очевидно, что в дереве таким образом может быть организовано сколь угодно много вопросов.

Ввод продукционных правил в базу знаний экспертом возможен с помощью двух подходов: снизу и сверху.

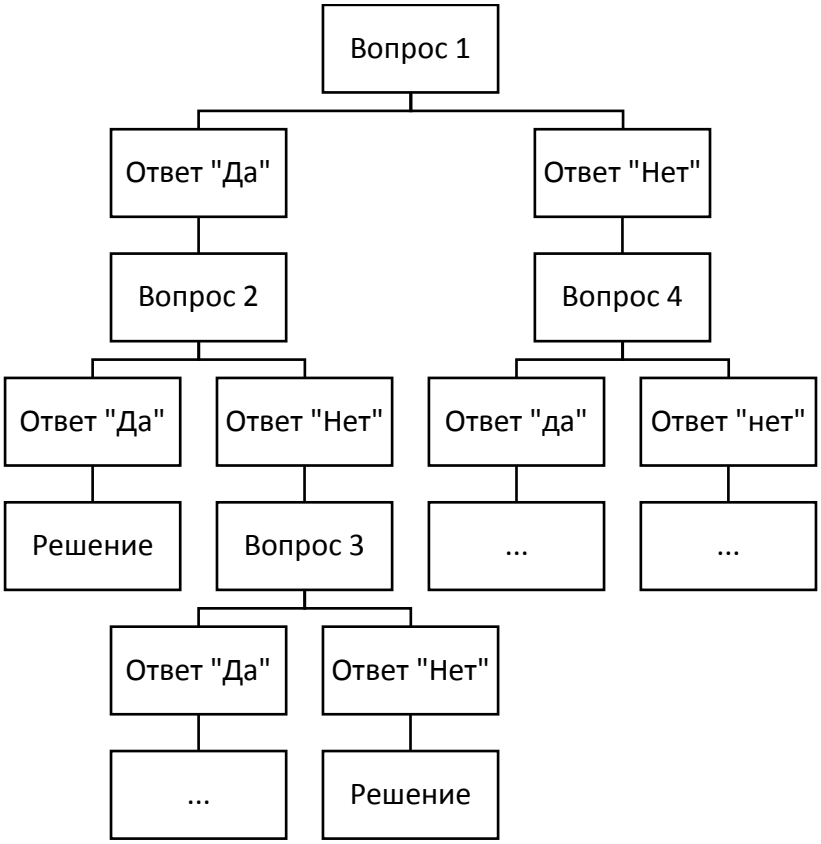


Рисунок 9 – Пример дерева решений

При подходе снизу необходимо выполнить следующие действия:

– определить перечень идентифицируемых событий, например, инцидентов ИБ;

– определить правила, соответствующие данному событию (симптомы, характерные для данного уровня);

– определить общие правила для группы событий (общие симптомы для уровня);

– составить дерево правил (симптомов);

– для каждого правила (симптома) сформулировать все компоненты правила и ввести его в базу знаний.

При подходе сверху необходимо выполнить следующие действия:

– определить перечень всех симптомов, возможных для данного уровня ИБ;

– выбрать наиболее общие симптомы и поставить их на верхний уровень дерева;

– для каждой ветки получившегося дерева снова определить наиболее общие симптомы из оставшихся и поставить их на следующий уровень дерева; данный пункт повторять пока есть симптомы;

– в полученном дереве для каждого правила (симптома) сформулировать все компоненты правила и ввести его в базу знаний.

Данные методы касаются первоначального наполнения базы знаний. Для добавления правил в базу знаний достаточно будет только ввести новые правила, согласовав их с ветками уровнем выше и ниже.

При большом количестве правил может возникнуть коллизия, то есть рассогласованность правил, когда в результате действий пользователя при одинаковых ответах на вопросы будут выдаваться различные ответы. В то же время при хаотичном добавлении правил возможны ситуации, когда одна или несколько веток не ведут к каким-либо результатам. Поэтому следующей процедурой после наполнения (модернизации) базы знаний при обучении экспертной системы является проверка (верификация) базы знаний.

Процедура верификации может выполняться в два этапа:

– автоматическая проверка. Для реализации данной проверки необходим специальный программный модуль, который будет проверять наличие/отсутствие безрезультатных веток, проходить каждую ветку для определения, единственный ли результат получается в конце прохода.

– проверка экспертом. Данная проверка должна проводиться экспертом в тестовом режиме, когда эксперт проверяет правильность выводов, сделанных экспертной системой на основе правил в базе знаний.

Второй вид процедур – определение соответствия поставленной цели – можно использовать при проведении аудитов информационной безопасности. Аудит информационной безопасности позволяет определить, обеспечивается ли безопасность информационных ресурсов предприятия. При проведении аудита сравнивается состояние информационной безопасности предприятия с определенным стандартом, например, описанным в СТР-К.

Для проведения аудитов в базе знаний экспертной системы должны храниться факторы (требования) оценки состояния информационной безопасности, экспертная оценка значимости этих факторов, а также результаты, соответствующие различным сочетаниям значений факторов.

При проведении аудита пользователь должен указать для каждого требования его выполнение на проверяемом предприятии (или степень выполнения), а экспертная система должна выдать количественную оценку соответствия информационной безопасности предприятия требованиям, а также рекомендации по повышению ее эффективности. Для этого эксперт должен занести в базу знаний правила, состоящие из следующих компонентов: вопрос, задаваемый пользователю; оцениваемое требование ИБ; вес вопроса; результат при положительном ответе; результат при отрицательном ответе.

Для заполнения базы знаний правилами эксперт должен выполнить следующие действия:

– Определить основные угрозы информационной безопасности;

– Определить для каждой угрозы уязвимости, через которые может быть реализована данная угроза;

– Определить для каждой уязвимости требования информационной безопасности, выполнение которых обеспечит минимизацию угроз;

– Определить для каждого требования его вес, то есть значимость для данной уязвимости;

– Определить перечень рекомендаций при невыполнении данного требования (или часть рекомендаций).

– Сформировать для каждого требования правила и ввести их в базу знаний.

Таким образом, сформулированные правила разного типа позволят выполнять различные процедуры (процедуры поиска решения и процедуры экспертной оценки).

2.4 Проектирование модели данных ЭС

Как видно из вышеописанного, разрабатываемая система должна работать как с системой правил (база знаний), так и с фактографической информацией

(информация об информационных активах, угрозах и т.д.) Поэтому одной из особенностей данной экспертной системы является объединение в одной информационной базе базы данных и базы знаний.

В соответствии с правилами, определенными в предыдущем пункте, в информационной базе должна храниться информация:

1) Классифицирующая угрозы, требования и мероприятия при возникновении угроз, определяющая мероприятия для каждой угрозы. Эта информация используется при проведении экспертной оценки информационной безопасности.

2) Классифицирующая инциденты информационной безопасности, информационные активы, подвергавшиеся инцидентам, стоимостную характеристику активов. Эта информация необходима для проведения экспертного поиска инцидента и экспертной оценки угроз.

3) Блок информации, организованной в виде продукционных правил, представляющий «базу знаний» в составе информационной базы.

Разрабатываемая экспертная систем должна работать в сфере информационной безопасности. Поэтому в модели данных должны присутствовать справочники, содержащие перечень возможных угроз и перечень возможных требований информационной безопасности. Для хранения данной информации используются таблицы со следующей структурой (таблица 4, 5).

Таблица 4 – Структура таблицы «Угрозы»

Поле	Тип данных	Назначение
Код	Числовой	Уникальный идентификатор
Наименование	Гекстовый	Наименование угрозы

Таблица 5 – Структура таблицы «Требования»

Поле	Тип данных	Назначение
Код	Числовой	Уникальный идентификатор
Наименование	Гекстовый	Наименование требования

Текст требования	Текстовый	Полный текст требования

Помимо требований информационной безопасности в нормативных документах описываются мероприятия, которые необходимо выполнить при возникновении той или иной угрозы. Поэтому в информационной базе необходимо иметь перечень мероприятий, проводимых для обеспечения ИБ (таблица 6).

Таблица 6 – Структура таблицы «Мероприятия»

Поле	Тип данных	Назначение
Код	Числовой	Уникальный идентификатор
Наименование	Текстовый	Наименование мероприятия

Одной из функций разрабатываемой экспертной системы должна стать идентификация инцидентов информационной безопасности с помощью процедуры экспертного поиска. Для унификации данной процедуры необходимо ввести в информационную базу таблицу «Инциденты». При этом каждому инциденту необходимо поставить в соответствие перечень мероприятий, которые выполняются при возникновении инцидента (таблицы 7, 8).

Таблица 7 – Структура таблицы «Инциденты»

Поле	Тип данных	Назначение
Код	Числовой	Уникальный идентификатор
Наименование	Текстовый	Наименование инцидента
Вид угрозы	Ссылка «Угрозы»	Какой угрозе соответствует инцидент

Таблица 8 – Структура таблицы «Соответствующие мероприятия»

Поле	Тип данных	Назначение
Инцидент	Ссылка «Инцидент»	Какому инциденту соответствует
Мероприятие	Ссылка «Мероприятия»	Мероприятие

Поскольку экспертная система должна постоянно пополняться новыми знаниями, эти знания должны быть разбиты по рассматриваемым вопросам (или темам). Для этого необходимо иметь список тем (таблица 9), по которым может происходить экспертный поиск или экспертную оценку.

Таблица 9 – Структура таблицы «Темы»

Поле	Тип данных	Назначение
Код	Числовой	Уникальный идентификатор
Наименование	Текстовый	Наименование темы

Для хранения правил экспертной системы необходимо использовать таблицы со структурой, определенной в предыдущем параграфе. При этом необходимо использовать отдельную таблицу для хранения правил поиска (таблица 10) и правил оценки (таблица 11).

Таблица 10 – Структура таблицы «Правила поиска»

Поле	Тип данных	Назначение
Код	Числовой	Уникальный идентификатор
Наименование	Текстовый	Наименование правила
Текст вопроса	Текстовый	Текст вопроса правила
Вопрос Да	Ссылка «Правила поиска»	Ссылка на следующий вопрос (правило) при ответе «Да»
Вопрос «Нет»	Ссылка «Правила поиска»	Ссылка на следующий вопрос (правило) при ответе «Нет»
Результат «Да»	Ссылка «Инциденты»	Какой инцидент предполагается при ответе «Да»
Результат «Нет»	Ссылка «Инциденты»	Какой инцидент предполагается при ответе «Нет»
Вес	Числовой	Вес вопроса (0..1)

Таблица 11 – Структура таблицы «Правила оценки»

Поле	Тип данных	Назначение
Код	Числовой	Уникальный идентификатор
Наименование	Текстовый	Наименование правила
Текст вопроса	Текстовый	Текст вопроса правила
Требование	Ссылка «Требования»	На соответствие какому требованию вопрос
Результат «Да»	Строка	Рекомендации при ответе «Да»
Результат «Нет»	Строка	Рекомендации при ответе «Нет»
Вес	Числовой	Вес вопроса (0..1)
Угроза	Ссылка «Угроза»	Какая угроза возможна при невыполнении требования

Каждый факт проведения экспертной оценки или экспертного поиска должны фиксироваться в информационной базе для дальнейшего анализа. Поэтому в базе необходимы таблицы «Экспертный поиск» и «Экспертная оценка» для хранения результатов выполнения данных процедур (таблицы 12, 14). С данными таблицами, содержащими общую информацию о проведенных процедурах, должны быть ассоциированы таблицы, содержащие информацию о заданных вопросах и полученных ответах (таблицы 13, 15). Эта информация необходима для выполнения процедуры объяснения решения.

Таблица 12 – Структура таблицы «Экспертный поиск»

Поле	Тип данных	Назначение
Номер	Числовой	Уникальный идентификатор
Дата	Дата	Дата проведения поиска
Тема	Ссылка «Тема»	Тема поиска

Результат	Ссылка «Инциденты»	Идентифицируемый в результате поиска инцидент

Таблица 13 – Структура таблицы «Правила поиска»

Поле	Тип данных	Назначение
Текст вопроса	Строка	Задаваемый вопрос
Ответ	Булево	Ответ пользователя
Вопрос	Ссылка «Правила поиска»	Ссылка на правило вопроса

Таблица 14 – Структура таблицы «Экспертная оценка»

Поле	Тип данных	Назначение
Номер	Числовой	Уникальный идентификатор
Дата	Дата	Дата проведения поиска
Тема	Ссылка «Тема»	Тема поиска

Таблица 15 – Структура таблицы «Правила оценки»

Поле	Тип данных	Назначение
Текст вопроса	Строка	Задаваемый вопрос
Ответ	Булево	Ответ пользователя
Вопрос	Ссылка «Правила поиска»	Ссылка на правило вопроса

Для выполнения количественной оценки информационной безопасности необходимо иметь перечень информационных активов предприятия и оценку ущерба от потенциальных угроз для этого актива. Эта информация должна храниться в таблицах «Активы» и «Ущерб от угроз» (таблицы 16-17).

Таблица 16 – Структура таблицы «Активы»

Поле	Тип данных	Назначение

Код	Числовой	Уникальный идентификатор
Наименование	Текстовый	Наименование правила
Ценность	Числовой	Оценка ценности актива

Таблица 17 – Структура таблицы «Ущерб от угроз»

Поле	Тип данных	Назначение
Актив	Ссылка «Актив»	Для какого актива оценен ущерб
Угроза	Ссылка «Угрозы»	От какой угрозы оценен ущерб
Ущерб	Числовой	Оценка ущерба

Для реализации экспертной системы в объектно-ориентированной среде необходимо создать объектно-ориентированную модель данных. Модель данных в виде диаграммы классов показана на рисунке 10.

Классы «Мероприятия», «Инциденты», «Угрозы», «Требования», «Темы», «Активы», «Правила поиска» и «Правила оценки» являются наследниками класса «Справочник» и наследуют его атрибуты «Код» и «Наименование». Классы «Правила поиска» и «Правила оценки» должны иметь методы «Проверка», позволяющие оценить правильность занесенных данных. Класс «Соответствующие мероприятия» является частью класса «Инциденты», то есть связаны отношением композиции. Класс «Ущерб от угроз» также является частью класса «Активы».

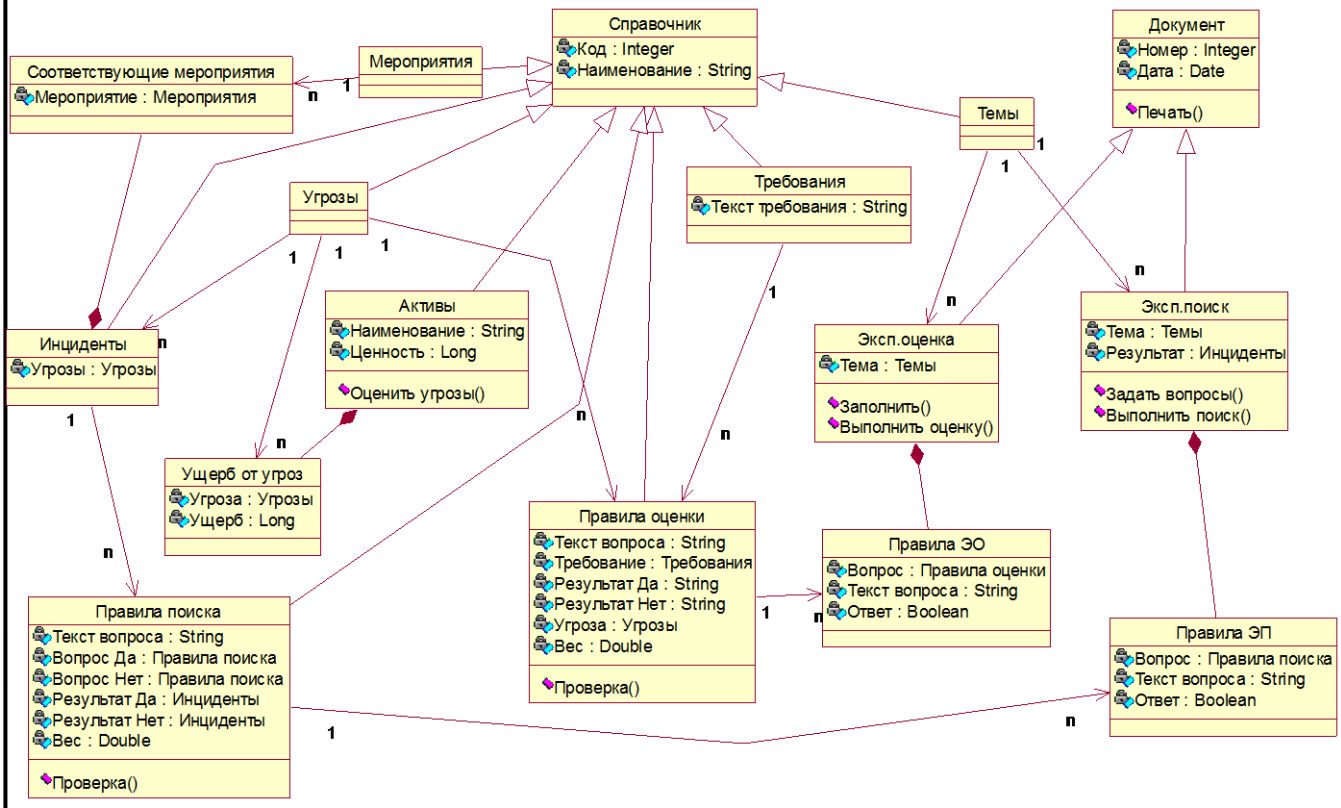


Рисунок 10 – Диаграмма классов

Классы «Эксп.оценка» и «Эксп.поиск» являются наследниками класса «Документ» и наследуют его атрибуты «Номер» и «Дата», а также метод «Печать». Кроме того, у классов «Эксп.оценка» и «Эксп.поиск» есть методы «Заполнить», «Выполнить оценку», «Задать вопрос» и «Выполнить поиск», реализующие собственно алгоритмы экспертной оценки и экспертного поиска. Классы «Правила ЭО» и «Правила ЭП» являются частью классов «Эксп.оценка» и «Эксп.Поиск» соответственно и связаны с ними отношениями композиции.

Классы «Правила оценки» и «Правила поиска» организованы в соответствии со структурой правил, приведенной в п.2.3. Это означает, что каждому правилу соответствует один вопрос и два альтернативных набора вариантов – если ответ «Да» и если ответ «Нет». Так как правил для каждой процедуры можно задать сколь угодно много, то соответственно и вопросов пользователю будет задано столько же, сколько задано правил.

2.5 Описание алгоритмов работы ЭС

Наиболее сложными алгоритмами в экспертной системе являются алгоритмы, имитирующие работу эксперта, то есть дающие ответы на поставленные

пользователем вопросы. Одним из таких алгоритмов является алгоритм обхода дерева решений при идентификации событий.

При обходе дерева система задает первый вопрос. В зависимости от ответа проверяется, если в поле «Вопрос да» или «Вопрос нет» записано значение, означающее конец поиска (например, пусто), значит это последний вопрос и выводится решение, записанное в полях «Результат да» или «Результат нет» соответственно. Если в полях «Вопрос да» или «Вопрос нет» записана ссылка на следующий вопрос, то система переходит к этому вопросу. Блок-схема алгоритма обхода дерева показана на рисунке 11.

Другим алгоритмом, обеспечивающим экспертную работу, является алгоритм оценки соответствия системы информационной безопасности требованиям нормативных документов. Для этого эксперт вводит в систему вопросы, определяет рекомендации по устранению недостатков. После этого, отвечая на вопросы системы, пользователь получает рекомендации и количественную оценку соответствия требованиям.

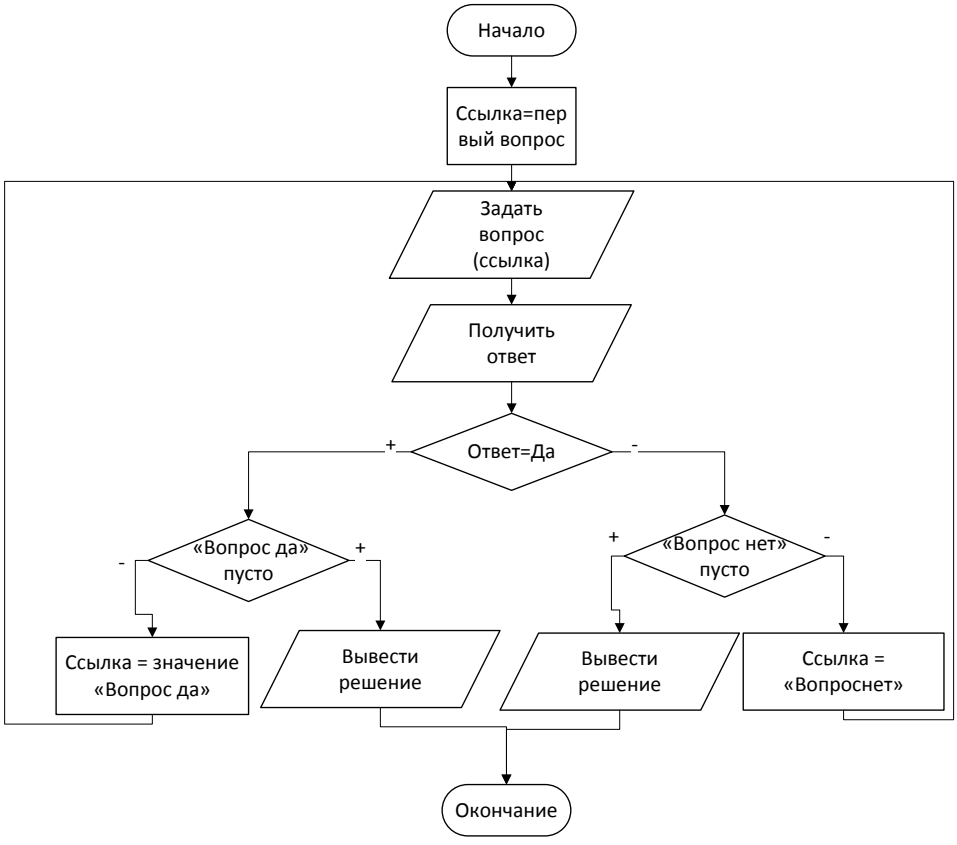


Рисунок 11 – Блок-схема алгоритма экспертного поиска

Для оценки соответствия системы информационной безопасности, программа поочередно задает вопросы, занесенные экспертом в базу данных. Если пользователь отвечает отрицательно на какой-то из вопросов, рекомендации, соответствующие этому вопросу, добавляются в общий перечень рекомендаций, количество отрицательных ответов увеличивается на 1. Кроме того, угроза, соответствующая данному вопросу, заносится в отдельную таблицу с соответствующим весом. После того, как все вопросы заданы, таблицу необходимо сгруппировать по типу угроз, подсчитав для каждого типа общий вес, а затем отсортировать таблицу по убыванию веса. Затем выводится список рекомендаций, количественна оценка соответствия, наиболее вероятная угроза. Блок-схема показана на рисунке 12.

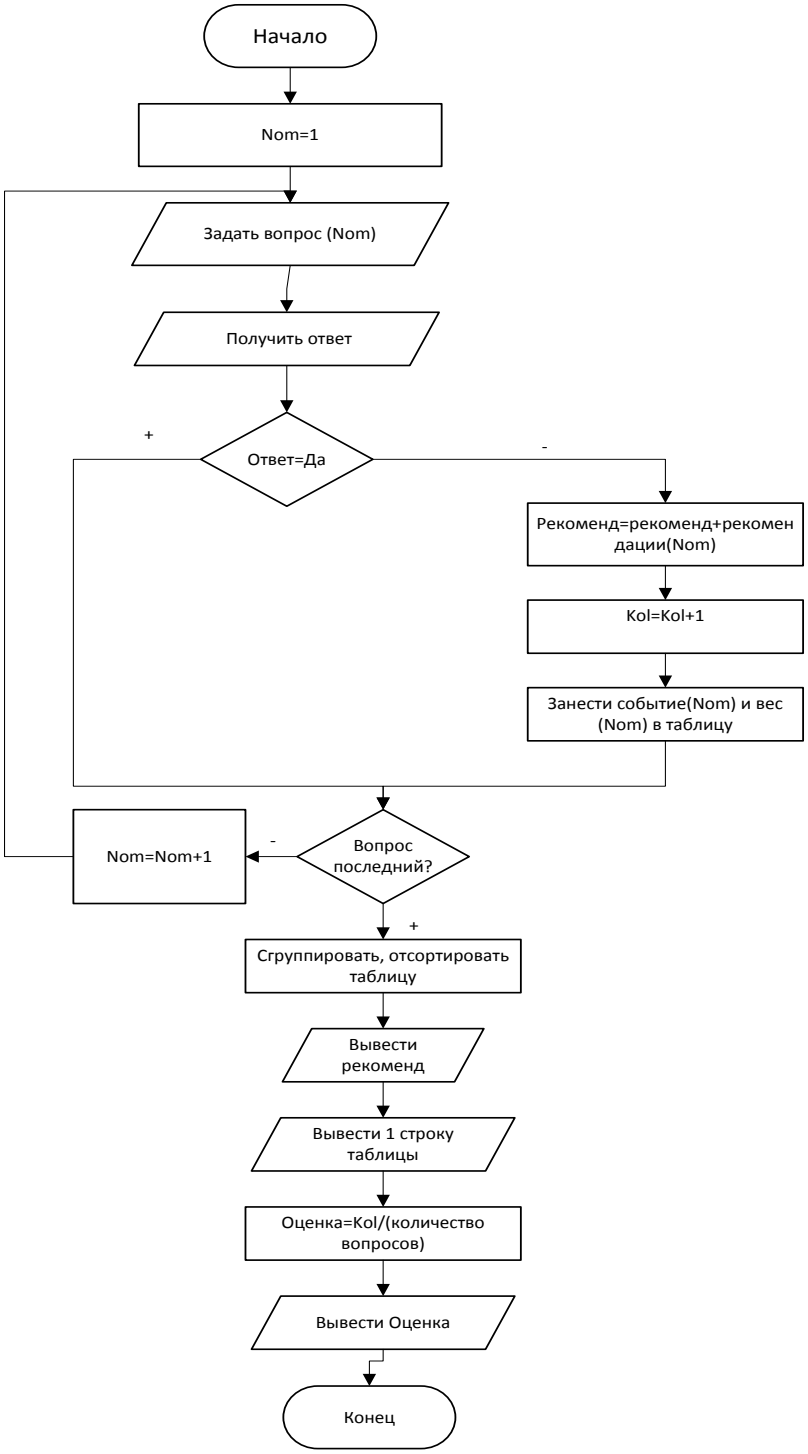


Рисунок 12 – Блок-схема алгоритма экспертной оценки

Предложенные алгоритмы по занесенным в базу правилам могут производить экспертный поиск (например, определение уровня информационной безопасности) и экспертную оценку (оценку соответствия состояния системы информационной безопасности требованиям методики определения угроз безопасности информации в ИС).

2.6 Определение прав доступа

В соответствии с диаграммой вариантов использования, с программой должны работать следующие типы пользователей:

- эксперт: выполняет ввод правил оценки и правил поиска;

- пользователь: принимает решения с помощью экспертной системы. Пользователи могут быть двух типов: пользователи, выполняющие оценку угроз и аудиторы, выполняющие оценку состояния информационной безопасности;

- администратор, осуществляющий администрирование справочников системы и организацию хранилища для новых знаний.

Схема работы с программой рассмотрена на диаграмме вариантов использования. Для того, чтобы определить структуру программы, необходимо определить основные процедуры (модули) программы.

На рисунке 13 показано разграничение прав доступа к основным модулям программы и их взаимодействие.

Как видно из рисунка, структуру программного решения составляют следующие модули:

- Оценка угроз. Эксперту предлагается перечень активов, он выставляет количественную оценку угроз для данного актива.

- Расчет оценки. Процедура расчета рассчитывает экспертную оценку угроз на основании оценок, введенных различными экспертами.

- Ввод экспертных правил. Модуль предоставляет интерфейс для ввода экспертных правил оценки, преобразования введенных правил во внутренний формат хранения, сохранения правил.

- Ввод правил поиска. Модуль предоставляет интерфейс для ввода правил экспертного поиска, преобразования введенных правил во внутренний формат, сохранения правил.

– Верификация. Модуль выполняет проверку введенных правил на полноту и непротиворечивость.

– Администрирование БД. Группа модулей для ведения справочников, управления данными.

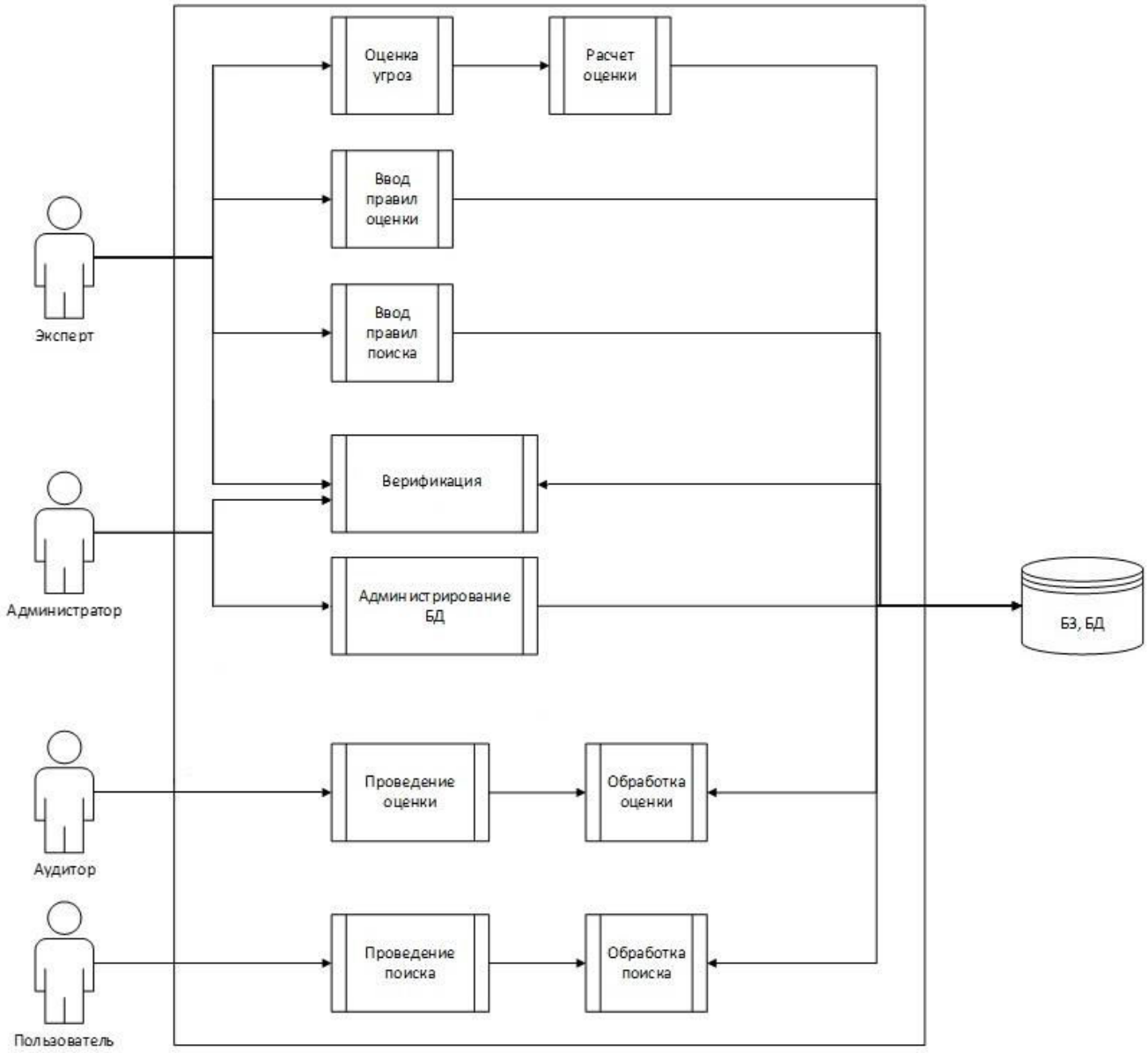


Рисунок 13 – Разграничение прав доступа

– Проведение оценки. Модуль предоставляет интерфейс для ответа на вопросы и сохранения ответов для дальнейшей обработки.

– Обработка оценки. Процедура формирования результата по ответам пользователя на вопросы.

– Проведение поиска. Модуль предоставляет интерфейс для ответа на вопросы и сохранения ответов для дальнейшей обработки.

– Обработка оценки. Процедура формирования результата по ответам пользователя на вопросы.

2.7 Подготовка и ввод экспертных правил

2.7.1 Особенности использования методических документов при реализации ЭС.

Для оценки состояния ИБ на предприятии в исходных данных работы используются два документа: «Методика определения угроз безопасности информации в информационных системах. Утверждена ФСТЭК России в 2015 г.» [8] и Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), утвержден приказом Гостехкомиссии России от 30.08.02 [14].

Документ [14] не содержит конкретных правил для выявления угроз ИБ на предприятии. В документе содержатся требования к безопасности. При этом оценивая выполнение данных требований, можно выявить перечень актуальных угроз для предприятия. Таким образом, используя [14], можно составить правила для выявления (оценки) угроз. Реализация данных правил выполнена в справочнике «Правила оценки».

В документе [8] приведена методика определения уровня защищенности информационной системы предприятия. Под уровнем защищенности понимается исходная защищенность информационной системы, обусловленная заданными при проектировании структурно-функциональными характеристиками и условиями ее функционирования. Уровень проектной защищенности определяется на основе анализа проектных структурно-функциональных характеристик. Оценку этих характеристик можно преобразовать в правила, используемые для оценки уровня защищенности. Реализация данных правил выполнена в справочнике «Правила поиска».

Также в документе [8] приведена методика количественной оценки выявленных угроз:

УБИj = [вероятность реализации угрозы (Pj)* степень ущерба (Xj)]

То есть для каждой выявленной угрозы необходимо определить вероятность ее реализации и ущерб от ее реализации.

Выявление угроз выполняется с помощью документа [14]. Для количественной оценки ущерба необходимо, чтобы ЭС не только выявляла и оценивала угрозы, но и

определяла количественный ущерб от их реализации. Для этого в документе «Экспертная оценка», который использует правила выявления угроз по СТР-К, добавлен модуль, который для каждой выявленной угрозы определяет вероятность ее возникновения. Поскольку в базе данных ЭС содержится информация об информационных активах предприятия и стоимости их ущерба, то ЭС может рассчитать этот показатель для каждого актива и по каждой угрозе. Реализация данного расчета выполнена в документе «Экспертная оценка», работа которого приведена ниже.

2.7.2 Разработка и ввод правил

Правила поиска для оценки состояния ИБ по методике определения угроз безопасности информации в информационных системах [8] показана на рисунке 14.

Код	Н	П...	Текст вопроса	Вопрос да	Вопро...	Результат да	Результат нет
000...	1	✔	Информационная система имеет структуру АРМ?	4	2	Высокий	
000...	10		ИС имеет файл-серверную архитектуру?	15	11	Низкий	
000...	11		ИС основана на одноранговой сети?	15	12	Средний	
000...	12		ИС строится на основе "тонкого клиента"?	15	13	Высокий	
000...	13		Для работы используются центра обработки данных?	14	14	Низкий	
000...	14		Испольуются системы с удаленным доступом пользователей?	15	15	Низкий	
000...	15		Используются разные типы операционных систем?	16	16	Средний	
000...	16		Используются прикладные программы, независимые от ОС?	17	17	Средний	
000...	17		Используются выделенные каналы связи?	18	18	Средний	
000...	18		ИС взаимодействует с иными ИС?	20	19	Низкий	
000...	19		Невзаимодействующая с другими ИС система?	20	20	Средний	
000...	2		Информационная система является локальной?	4	3	Средний	
000...	20		ИС является неподключенной к сетям общего пользования?	23	21	Высокий	
000...	21		ИС подключена к сетям общеко пользования через выделенную инфраструктуру?	22	23	Средний	
000...	22		ИС подключена к сетям общего пользования?	23	23	Низкий	
000...	23		Имеется контрольная зона размещения технических средств?	24	26		Низкий
000...	24		Технические средства расположены в пределах одной контролируемой зоны?	26	25	Высокий	
000...	25		Технические средства расположены в пределах нескольких контрольных зон	26	26	Средний	
000...	26		Режим обработки информации однопользовательский?	27	27	Высокий	Низкий
000...	27		Разграничиваются ли права доступа к ИС?	28	28	Средний	Низкий
000...	28		Режим разделения функций по управлению ИС без разделения?	32	29	Низкий	
000...	29		Рабочие места для администрирования ИС выделены в отдельный домен?	32	30	Средний	
000...	3		Используется распределенная информационная система?	4	4	Низкий	
000...	30		Для разделения функций по управлению ИС используются различные сетевые ад...	32	31	Низкий	
000...	31		Для администрирования выделены отдельные каналы?	32	32	Средний	
000...	32		Информационная система сегментирована?			Средний	Низкий

Рисунок 14 – Правила поиска по методике ФСТЭК

Данная методика выбрана потому, что в ней есть раздел, в котором указаны конкретные параметры, по которым можно оценить уровень защищенности информационной системы – высокий, низкий или средний. По соответствию этим параметрам составлены вопросы (правила) для ввода в ЭС.

При вводе правил в справочник, вопрос, стоящий в корне дерева, должен быть помечен флагом «Первый».

Эти правила поиска следующую структуру:

1. ЕСЛИ (Информационная система имеет структуру АРМ?) ТО (Высокий, перейти к 4) ИНАЧЕ (перейти к 2)
2. ЕСЛИ (Информационная система является локальной?) ТО (Средний, перейти к 4) ИНАЧЕ (перейти к 3)
3. ЕСЛИ (Используется распределенная информационная система?) ТО (Низкий, перейти к 4) ИНАЧЕ (перейти к 4)
4. ЕСЛИ (Используется технология виртуализации?) ТО (Низкий, перейти к 5) ИНАЧЕ (перейти к 5)
5. ЕСЛИ (Используются системы с технологиями беспроводного доступа?) ТО (Низкий, перейти к 6) ИНАЧЕ (перейти к 8)
6. ЕСЛИ (Используются системы, реализующие облачные вычисления?) ТО (Низкий, перейти к 7) ИНАЧЕ (перейти к 7)
7. ЕСЛИ (Используются системы с мобильными устройствами?) ТО (Низкий, перейти к 8) ИНАЧЕ (перейти к 8)
8. ЕСЛИ (Используются ГРИД-системы?) ТО (Низкий, перейти к 9) ИНАЧЕ (перейти к 9)
9. ЕСЛИ (Используются суперкомпьютерные системы?) ТО (Низкий, перейти к 10) ИНАЧЕ (перейти к 10)
10. ЕСЛИ (ИС имеет файл-серверную архитектуру?) ТО (Низкий, перейти к 15) ИНАЧЕ (перейти к 11)
11. ЕСЛИ (ИС основана на одноранговой сети?) ТО (Средний, перейти к 15) ИНАЧЕ (перейти к 12)
12. ЕСЛИ (ИС строится на основе "тонкого клиента"?) ТО (Высокий, перейти к 15) ИНАЧЕ (перейти к 13)
13. ЕСЛИ (Для работы используются центра обработки данных?) ТО (Низкий, перейти к 14) ИНАЧЕ (перейти к 14)

Полный перечень правил представлен в приложении Б.

Перевод из таблицы справочника в правила экспертной системы выполняются с помощью следующего программного кода:

```
СтрокаТабличнойЧасти = ЭлементыФормы.Правила.ТекущиеДанные;
если строкатабличнойчасти.ответ=истина тогда
 если значениезаполнено(строкатабличнойчасти.вопрос.вопросда) тогда
        нс=правила.Добавить();
        нс.Вопрос=строкатабличнойчасти.вопрос.вопросда;

нс.ТекстВопроса=строкатабличнойчасти.вопрос.вопросда.текствопроса;
конецесли;
результат=строкатабличнойчасти.вопрос.результатДа;
 иначеесли строкатабличнойчасти.ответ=ложь тогда
        если значениезаполнено(строкатабличнойчасти.вопрос.вопроснет)
тогда
        нс=правила.Добавить();
        нс.Вопрос=строкатабличнойчасти.вопрос.вопроснет;

нс.ТекстВопроса=строкатабличнойчасти.вопрос.вопроснет.текствопроса;
  конецесли;
  результат=строкатабличнойчасти.вопрос.результатнет;
конецесли;
```

Программа должна подсчитать процентное соотношение каждого результата и вывести общее решение. В результате работы правил системе ИБ предприятия должен быть присвоен уровень – Высокий, Средний или Низкий.

Для подготовки правил оценки угроз по СТР-К необходимо определить оцениваемые угрозы, требования для минимизации угрозы, рекомендации при невыполнении требования, важность (вес) требования. Также эксперт подготавливает вопрос для проверки выполнения данного требования. Эти данные можно оформить в виде таблицы (таблица 18).

Таблица 18 – Правила оценки состояния ИБ

Угроза	Требование	Вопрос	Рекомендовано	Вес
Вирусная угроза	Наличие антивирусной программы	Установлена ли антивирусная программа на всех СВТ?	Предотвращение внедрения в автоматизированные системы вирусов	90

Продолжение таблицы 18

	Сертификация СЗИ	Средства защиты информации сертифицированы по требованиям безопасности?	Использование сертифицированных средств защиты информации	0
Несанкционированный доступ	Наличие перечня требований конфиденциального характера	Есть ли в организации Перечень сведений конфиденциального характера?	Документальное оформление перечня сведений конфиденциального характера с учетом ведомственной и отраслевой специфики этих сведений	0
	Удаление временных файлов	Выполняется ли удаление временных файлов после сеанса работы?	По окончании обработки защищаемой информации или при передаче управления другому лицу пользователь обязан произвести стирание временных файлов на несъёмных носителях	0
Несанкционированный доступ	Защищенное размещение экранов	Размещены ли экраны в местах, защищенных от несанкционированного просмотра?	Размещение дисплеев и других средств отображения информации, исключающее несанкционированный просмотр информации	0

	Наличие системы допуска	Существует ли разрешительная система допуска пользователей к информации?	Реализация разрешительной системы допуска пользователей к информации и связанным с ее использованием работами	5

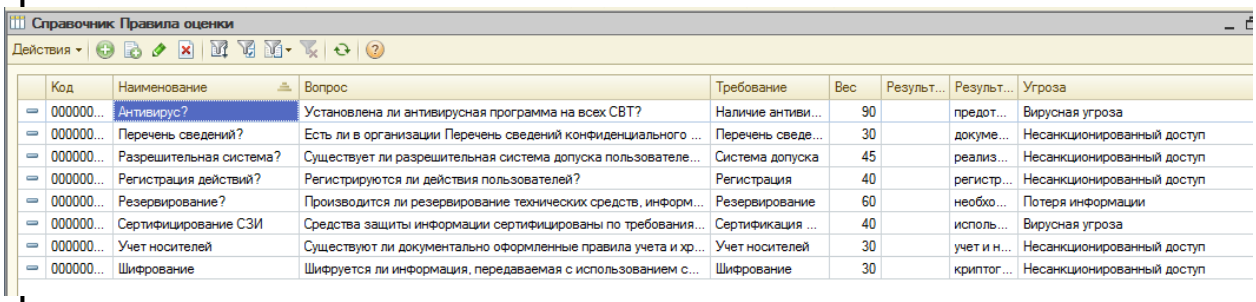
Продолжение таблицы 18

Несанкционированный доступ	Регистрация действий пользователей	Регистрируются ли действия пользователей?	Регистрация действий пользователей АС и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц	0
	Ведение учета носителей и хранения информации	Существуют ли документально оформленные правила учета и хранения носителей информации?	Учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену	0
Несанкционированный доступ	Шифрование информации, передаваемой по КС	Шифруется ли информация, передаваемая с использованием сети Интернет?	Криптографическое преобразование информации, обрабатываемой и передаваемой средствами	0

			вычислительной техники и связи	
Потеря информации	Резервное копирование информации	Производится ли резервирование технических средств, информации, носителей информации?	Необходимое резервирование технических средств и дублирование массивов и носителей информации	0

Данные правила сформированы в соответствии с СТР-К [14]. Поскольку в данном документе не определены конкретные методики оценки, то общие рекомендации преобразованы в правила.

Эти данные заносятся в справочник «Правила оценки» (рисунок 15).


Справочник Правила оценки

Действия

Код	Наименование	Вопрос	Требование	Вес	Результ...	Результ...	Угроза
000000...	Антивирус?	Установлена ли антивирусная программа на всех СВТ?	Наличие антиви...	90		предот...	Вирусная угроза
000000...	Перечень сведений?	Есть ли в организации Перечень сведений конфиденциального ...	Перечень сведе...	30		докуме...	Несанкционированный доступ
000000...	Разрешительная система?	Существует ли разрешительная система допуска пользователе...	Система допуска	45		реализ...	Несанкционированный доступ
000000...	Регистрация действий?	Регистрируются ли действия пользователей?	Регистрация	40		регистр...	Несанкционированный доступ
000000...	Резервирование?	Производится ли резервирование технических средств, информ...	Резервирование	60		необхо...	Потеря информации
000000...	Сертифицирование СЗИ	Средства защиты информации сертифицированы по требования...	Сертификация ...	40		исполь...	Вирусная угроза
000000...	Учет носителей	Существуют ли документально оформленные правила учета и хр...	Учет носителей	30		учет и н...	Несанкционированный доступ
000000...	Шифрование	Шифруется ли информация, передаваемая с использованием с...	Шифрование	30		криптог...	Несанкционированный доступ

Рисунок 15 – Правила оценки

Эти правила с помощью программы интерпретируются в следующие правила:

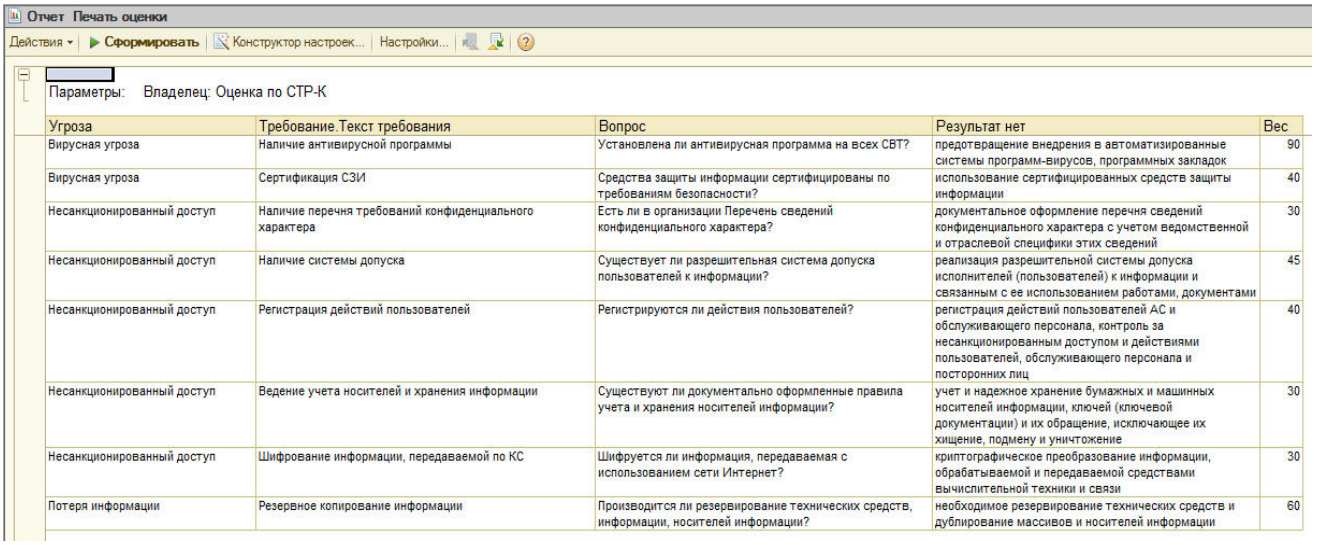
1. ЕСЛИ <Установлена ли антивирусная программа на всех СВТ> ТО <Нет угрозы> ИНАЧЕ <Угроза «Вирусная угроза» с вероятностью 90%>

2. ЕСЛИ <Есть ли в организации Перечень сведений конфиденциального характера? > ТО <Нет угрозы> ИНАЧЕ <Угроза «Несанкционированный доступ» с вероятностью 30%>

3. ЕСЛИ <Существует ли разрешительная система допуска пользователей к информации?> ТО <Нет угрозы> ИНАЧЕ <Угроза «Несанкционированный доступ» с вероятностью 45%>

И так далее в соответствии с таблицей 15.

Перевод из таблицы справочника в правила экспертной системы выполняются с помощью программного кода.



Отчет Печать оценки

Действия | Сформировать | Конструктор настроек... | Настройки...

Параметры: Владелец: Оценка по СТР-К

Угроза	Требование.Текст требования	Вопрос	Результат нет	Вес
Вирусная угроза	Наличие антивирусной программы	Установлена ли антивирусная программа на всех СВТ?	предотвращение внедрения в автоматизированные системы программ-вирусов, программных закладок	90
Вирусная угроза	Сертификация СЗИ	Средства защиты информации сертифицированы по требованиям безопасности?	использование сертифицированных средств защиты информации	40
Несанкционированный доступ	Наличие перечня требований конфиденциального характера	Есть ли в организации Перечень сведений конфиденциального характера?	документальное оформление перечня сведений конфиденциального характера с учетом ведомственной и отраслевой специфики этих сведений	30
Несанкционированный доступ	Наличие системы допуска	Существует ли разрешительная система допуска пользователей к информации?	реализация разрешительной системы допуска исполнителей (пользователей) к информации и связанным с ее использованием работами, документами	45
Несанкционированный доступ	Регистрация действий пользователей	Регистрируются ли действия пользователей?	регистрация действий пользователей АС и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц	40
Несанкционированный доступ	Ведение учета носителей и хранения информации	Существуют ли документально оформленные правила учета и хранения носителей информации?	учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение	30
Несанкционированный доступ	Шифрование информации, передаваемой по КС	Шифруется ли информация, передаваемая с использованием сети Интернет?	криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи	30
Потеря информации	Резервное копирование информации	Производится ли резервирование технических средств, информации, носителей информации?	необходимое резервирование технических средств и дублирование массивов и носителей информации	60

Рисунок 16 – Отчет «Печать оценки»

Для верификации правил используется отчет «Печать оценки», сравнив результат которого с исходной таблицей эксперт может проверить корректность данных (рисунок 16).

Как видно из рисунка, правила оценки по СТР-К введены корректно.

В результате работы с правилами, система оценивает процентное соотношение угроз, получая тем самым вероятность возникновения каждой угрозы. Затем для каждой угрозы определяется набор активов, которые подвержены угрозам. Для каждого актива определяется ущерб от угроз как произведение стоимости актива на вероятность угрозы. Такой метод оценки угроз приведен в [8]. Результат работы программы показан в следующем пункте.

3 РЕАЛИЗАЦИЯ ЭКСПЕРТНОЙ СИСТЕМЫ ИБ

3.1 Выбор средств реализации экспертной системы

Как было показано в 1 главе настоящей работы, для разработки экспертной системы можно использовать специальные средства программирования (использующие логические языки) или средства программирования общего назначения (использующие процедурные или объектно-ориентированные языки). В [68] приведены плюсы и минусы подобных подходов и сделан вывод о том, что выбор инструмента разработки зависит от требуемого результата и изначальных навыков (предпочтений) разработчика.

В то же время в [69] сказано, что экспертная система может быть реализована на любом современном языке программирования.

Для выбора инструмента разработки экспертной системы необходимо проанализировать преимущества и недостатки каждого из типов языков программирования применительно к разработке системы оценки информационной безопасности. При этом необходимо учесть следующие моменты:

– С помощью разрабатываемой системы необходимо выполнять не только экспертные процедуры, но и формализованные расчеты (при выполнении количественной оценки угроз, например). Поэтому разрабатываемая система должна содержать как алгоритмы логических решений, так и алгоритмы расчетов.

– Для выполнения оценки угроз необходимо иметь перечень информационных активов и оценку их стоимости. Поэтому в информационной базе необходимо иметь не только логические правила (база знаний), но и фактические данные (база данных). Таким образом, разрабатываемое приложение должно работать или с двумя базами, или с одной объединенной, используя как средства логического поиска, так и средства запросов к базам данных.

– С разрабатываемой системой должны работать эксперты и простые пользователи, поэтому она должна иметь удобный интерфейс и средства разграничения доступа.

Сравнение языков общего назначения и специальных языков для реализации ЭС приведены в таблице 19.

Таблица 19 – Сравнение языков реализации ЭС

Тип языка	Преимущества	Недостатки
Общего назначения	– возможность работать с правилами и данными, реализованными в реляционной или объектно-ориентированной БД – возможность выполнять экспертные процедуры и фактографические расчеты – возможность реализации удобного интерфейса	– отсутствие встроенных механизмов экспертных логических выводов – необходимость разработки алгоритмов выполнения логических процедур
Специальные	– наличие встроенного механизма выполнения экспертных процедур – возможность обработки большого числа правил	– отсутствие возможности реализации удобного интерфейса – сложности при работе с фактографическими базами данных

Для экспертной системы информационной безопасности такие преимущество специальных средств разработки как возможность обработки большого числа правил не столь актуально, поскольку используемые методики оценки ИБ не оперируют слишком большим числом правил. В остальном преимущество на стороне языков общего назначения.

На текущий момент времени есть огромное количество инструментальных средств, позволяющих разрабатывать прикладные программы. Среди этих решений можно выделить платформу «1С: Предприятие 8.2», с одной стороны, как на наиболее удобную систему решения прикладных задач, а с другой стороны, как на

наиболее распространенную в РФ программу разработки офисных приложений. В то же время в [70] приведен пример реализации экспертной системы на платформе 1С:Предприятие.

Опыт внедрения прикладных решений на платформе «1С: Предприятие 8.2» показывает, что платформа 1С позволяет решать задачи различной направленности — от автоматизации одного рабочего места до создания АИС масштаба холдинга [66].

Прикладные программные решения «1С» разрабатываются для автоматизации предприятий малого и среднего бизнеса, государственных и бюджетных учреждений, некоммерческих организаций (НКО) и индивидуальных частных предпринимателей, образовательных учреждений.

Платформу «1С: Предприятие 8» нельзя назвать программным обеспечением (ПО), готовым к эксплуатации конечными пользователями: для работы необходимы также прикладные решения — конфигурации, разработанные на ее основе.

Данный подход позволяет компаниям различных форм собственности и отраслевой направленности автоматизировать свои бизнес-процессы с применением единой технологической платформы «1С: Предприятие 8».

Технологическая платформа «1С: Предприятие 8» обладает большой гибкостью, что позволяет применять систему программ «1С: Предприятие 8» в самых разных областях.

В состав системы «1С: Предприятие» включен программный модуль «Конфигуратор», он отвечает за:

- настройку системы на различные виды учета;
- реализацию произвольной методологии учета;
- организацию справочников и документов произвольной структуры;
- настройку внешнего вида форм ввода информации;
- настройку поведения и алгоритмов работы системы в различных ситуациях;
- возможность создания печатных форм документов и отчетов;
- возможность представления информации в виде диаграмм;
- быстрое изменение конфигурации с помощью «конструкторов».

Конфигуратор позволяет не только изменять элементы типовой конфигурации, но и создать собственную конфигурацию «с нуля».

Программное обеспечение 1С содержит разнообразные средства для связи с другими программами и аппаратными средствами: средства импорта и экспорта информации через текстовые файлы, файлы формата DBF и XML, сохранение печатных форм в форматах MS Excel и HTML, возможность экспорта данных в «Диспетчер контактов для малого бизнеса» «MS Office».

Наличие единой технологической платформы и общей методологии позволяет создавать такие решения на базе выпускаемых фирмой «1С» тиражных прикладных решений, добавляя в них только необходимые отличия, учитывающие специфику отрасли или конкретного предприятия. Это обеспечивает:

– высокую скорость создания и внедрения решений за счет максимального использования апробированной функциональности и методологии, реализованных в типовых конфигурациях;

– низкую стоимость отраслевых прикладных решений — затраты на их создание существенно ниже, чем затраты на разработку программы «с нуля».

Таким образом, принимая во внимание все вышесказанное, было принято решение об использовании в качестве системы разработки платформы «1С:Предприятие 8.2».

Выбор платформы разработки повлиял на составление технического задания. При определении функций разрабатываемой системы сразу делался прогноз о возможности реализации этих функций на платформе «1С:Предприятие» и возможного использования тех или иных прикладных объектов платформы для более полной и быстрой реализации закладываемых в систему функций. Таким образом, на этапе составления технического задания у разработчика уже есть представление, как примерно будет реализована эта функция на платформе разработки, но без детализации.

«1С:Предприятие 8» поддерживает 5 видов СУБД: файловый вариант самой 1С; IBM DB2; MS SQL; Oracle BD; PostgreSQL.

Каждая из этих СУБД имеет ограничения при работе с 1С: в СУБД PostgreSQL сильно уменьшается производительность в режиме интенсивной работы, система как можно чаще требуется реиндексерование; DB2 чувствительная к регистру строковых значений при сравнении, а также в ней существенно снижается производительность от использования подзапросов в условии соединения; на работу СУБД Oracle DB очень сильное влияние оказывает статистика планов запроса 1С. Наименьшее число ограничений накладывается на использование MS SQL, поэтому для реализации системы будет использоваться именно она.

В качестве языка программирования выбирается встроенный язык 1С как наиболее понятный и наилучшим образом использующий объекты конфигурации 1С.

3.2 Разработка интерфейса ЭС

Интерфейс разработанной экспертной системы обусловлен принятыми в системе 1С:Предприятие шаблонами форм и их поведением. Поскольку для системы необходимо разграничить доступ к объектам в зависимости от роли пользователя (эксперт, пользователь, администратор), то и меню необходимо организовать в соответствии с правами пользователей.

Права доступа к объектам и содержание меню программы необходимо задать в соответствии с таблицей (таблица 20).

Таблица 20 – Права доступа к объектам программы

Роль пользователя	Объект	Права доступа
Эксперт	Справочник «Правила оценки»	Добавление, редактирование
	Справочник «Правила поиска	Добавление, редактирование
	Справочник «Активы»	Добавление, редактирование
	Справочник «Мероприятия»	Добавление, редактирование
	Справочник «Инциденты»	Добавление, редактирование
	Справочник «Требования»	Добавление, редактирование
	Справочник «Угрозы»	Добавление, редактирование

	Отчеты	Использование
Пользователь	Документ «Экспертный поиск»	Создание, чтение

Продолжение таблицы 20

Аудитор	Документ «Экспертная оценка»	Создание, чтение
	Справочник «Активы»	Чтение
	Отчеты	Использование
Администратор	Все объекты	Полный доступ

В соответствии с таблицей, проектируется меню системы. Наиболее полными правами обладает Администратор, поэтому в качестве базового интерфейса строится интерфейс администратора. На рисунке 17 приведены для сравнения меню интерфейса «Администратор» и меню интерфейса «Пользователь».

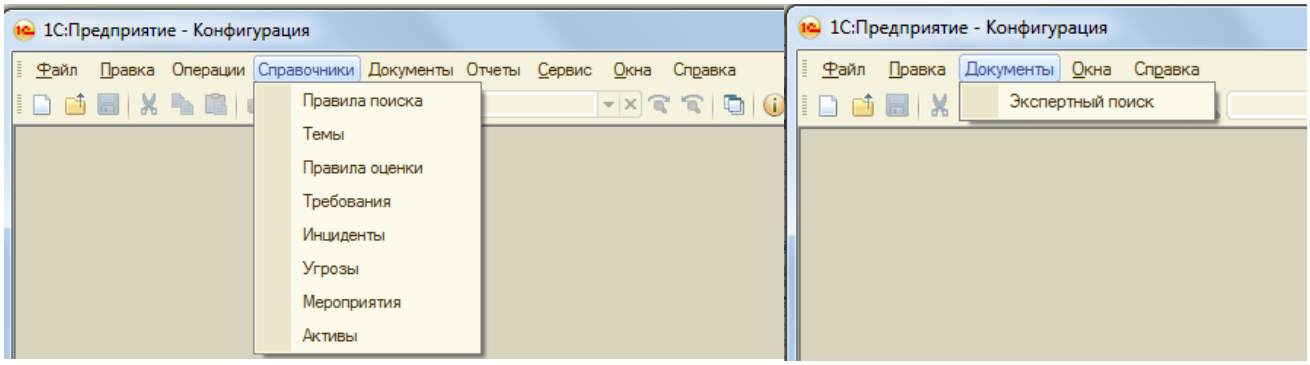


Рисунок 17 – Меню интерфейсов «Администратор» и «Пользователь»

Следуя принципам системы 1С:Предприятие, в меню программы выделяются пункты «Справочники», «Документы» и «Отчеты». Объекты имеют схожий интерфейс, поскольку строятся на основе встроенных шаблонов форм.

Интерфейсные формы справочников системы приведены на рисунках 15-20.

Справочники «Мероприятия» и «Угрозы» представляют собой обычные списки возможных мероприятий и угроз соответственно. Поэтому их формы имеют простой интерфейс (рисунок 18).

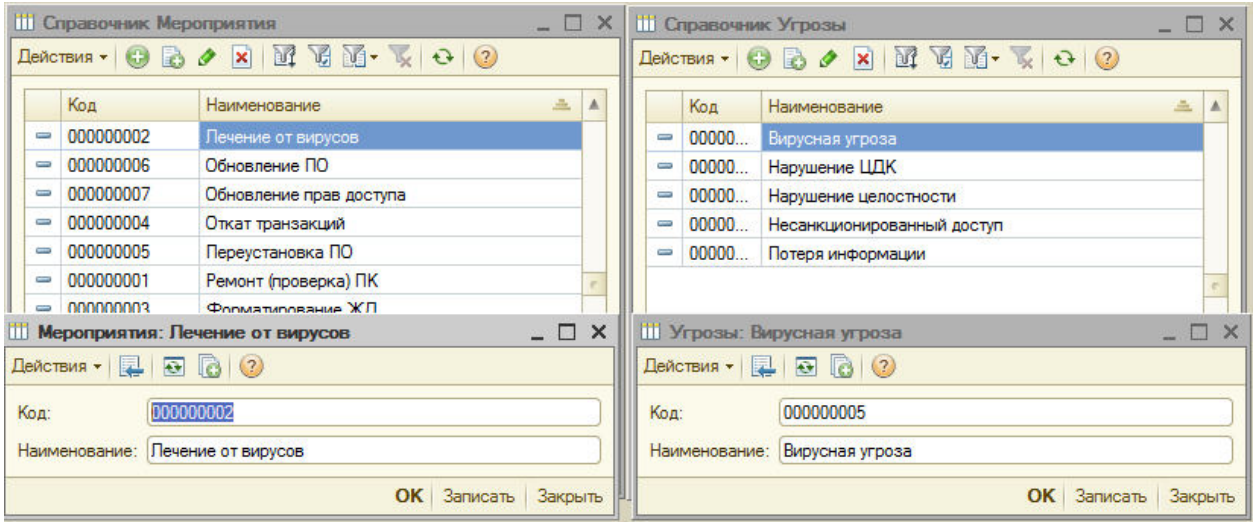


Рисунок 18 – Интерфейс справочников «Мероприятия» и «Угрозы»

Форма справочника «Требования» содержит поля для ввода краткой и полной форм требований ИБ (рисунок 19).

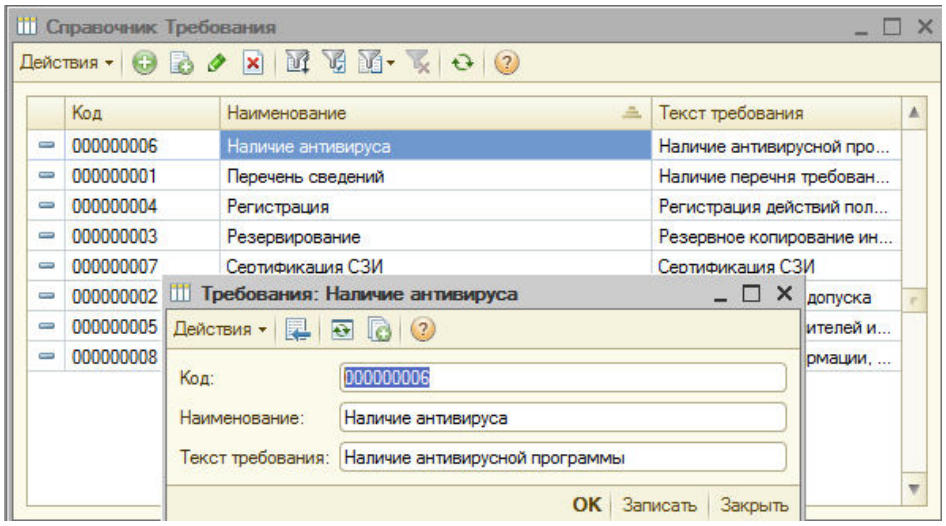


Рисунок 19 – Интерфейс справочника «Требования»

Интерфейс справочника «Активы» позволяет вводить в справочник не только перечень активов, но и привязывать к ним непосредственно угрозы, возможные для этого актива, и ущерб от них. Ущерб должен вноситься экспертом (рисунок 20).

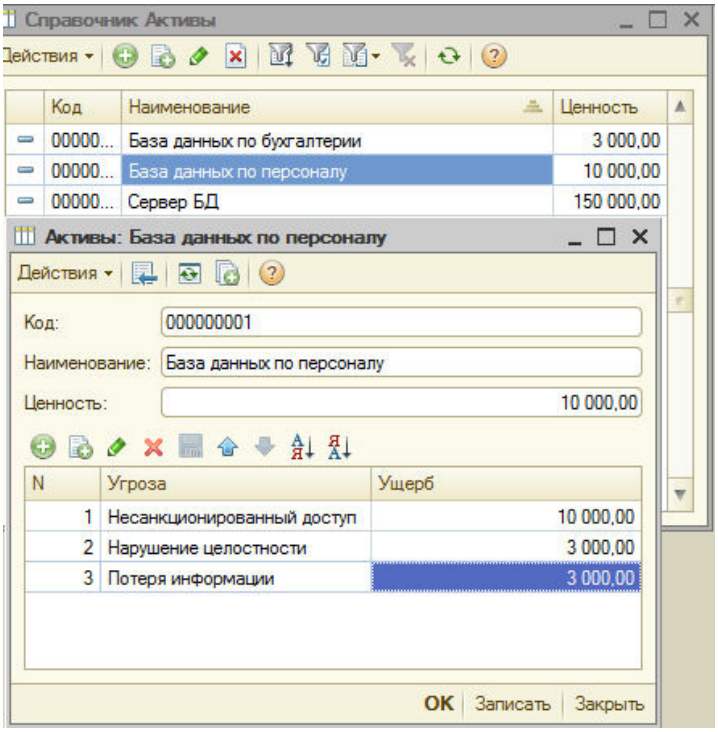


Рисунок 20 – Интерфейс справочника «Активы»

Более сложный интерфейс имеют справочники «Правила оценки» и «Правила поиска». Данные справочники заполняются экспертом, поэтому для форм минимизирован ручной ввод информации.

Справочник «Правила оценки» может заполняться для оценок по различным нормативным документам. Для этого в поле «Родитель» указывается, к оценке по какой методике относится правило.

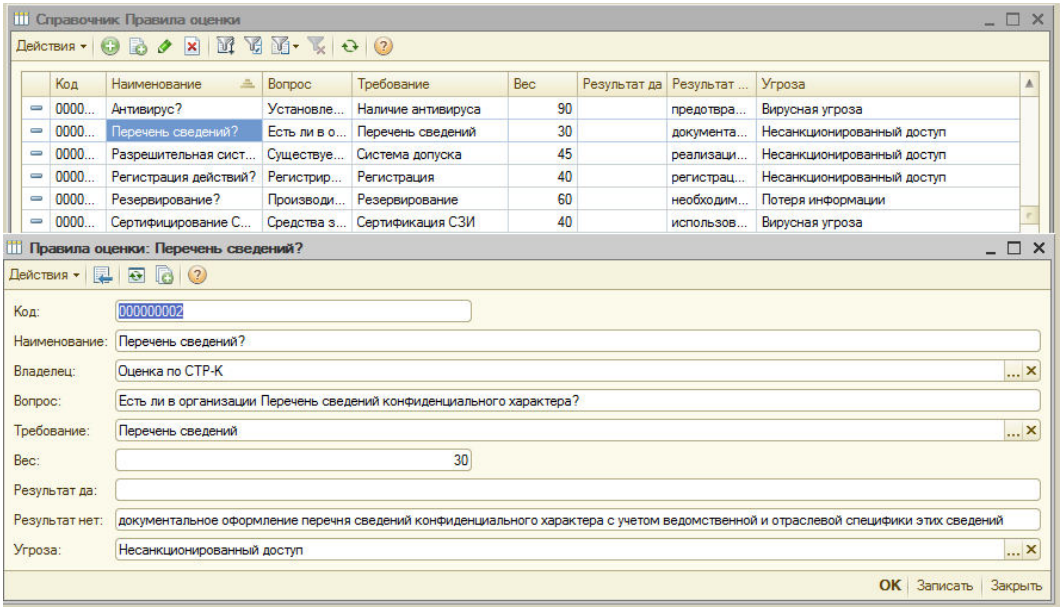


Рисунок 21 – Интерфейс справочника «Правила оценки»

В справочнике указывается краткое наименование правила, текст правила, требование, проверяемое этим правилом, угроза, возникающая при несоблюдении правила, рекомендации при несоблюдении правила (рисунок 21).

Справочник «Правила поиска» (рисунок 22) имеет схожий интерфейс; поскольку поиск может производиться по различным категориям, тип поиска, к которому относится данное правило, указывается в поле «Владелец». Если этот вопрос при проведении поиска должен задаваться первым, выставляется флаг «Первый». Далее справочник заполняется в соответствии с правилами, указанными на рисунке 7.

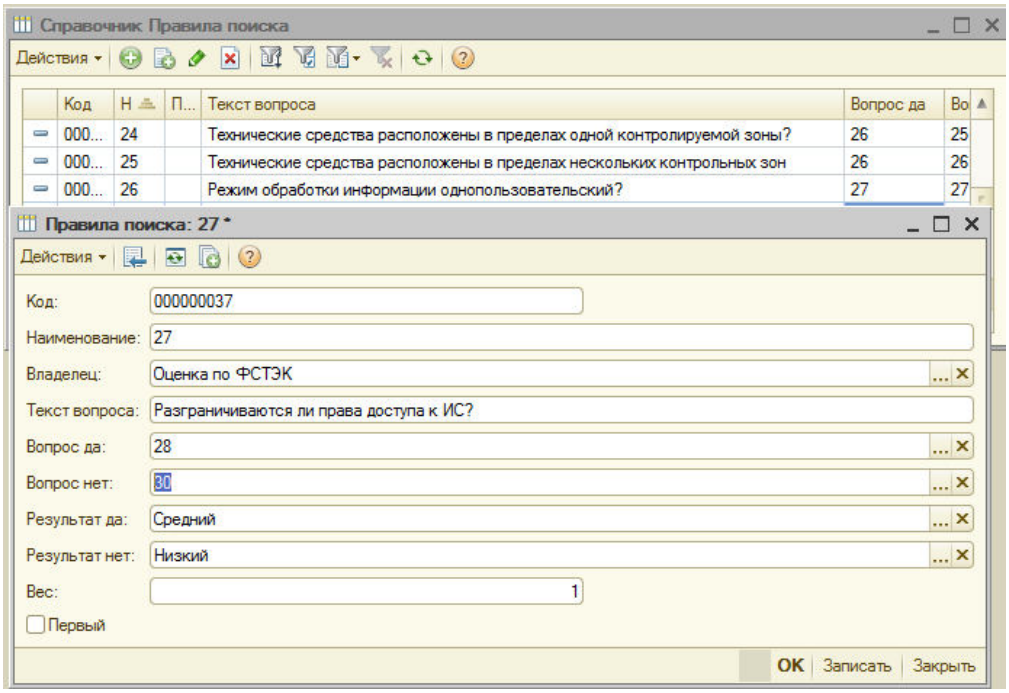


Рисунок 22 – Интерфейс справочника «Правила поиска»

3.3 Результаты работы системы

В качестве результатов работы системы рассмотрим пример выполнения оценки ИБ по ответам, указанным пользователем. Для оценки работы системы покажем последовательно работу документа «Экспертный поиск». В этом случае пользователь формирует документ отвечает на вопросы экспертной системы в следующем порядке:

1) Формирует новый документ, выбирает тему «Оценка по ФСТЭК» и нажимает кнопку «Начать». При этом в табличной части сразу появится первый вопрос по этой теме.

2) Пользователь отвечает на вопрос, после чего система задает следующий вопрос, при этом следующий вопрос зависит от предыдущего. Результаты ответов на вопросы показаны на рисунке 23.

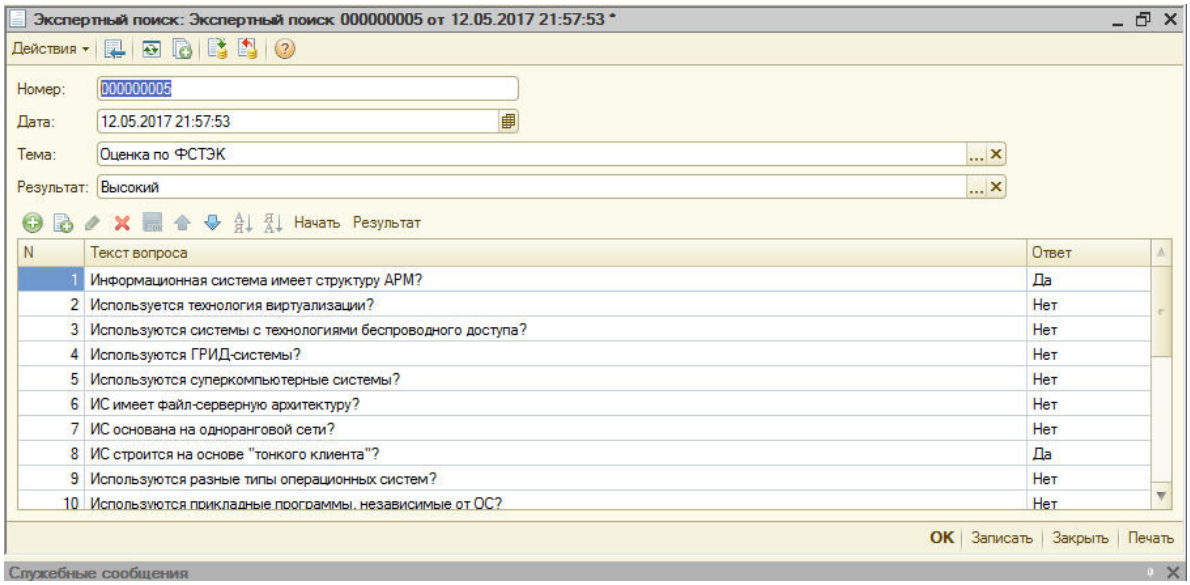


Рисунок 23 – Результаты поиска

3) После ответа на последний вопрос по нажатию кнопки «Результат» в поле «Результат» появляется результат работы, то есть оценка ИБ.

4) Если уровень оценки ИБ по методике определения угроз безопасности информации в ИС соответствует низкому или среднему, то пользователю предлагается перейти к шагу 2, то есть оценке угроз (рисунок 24).

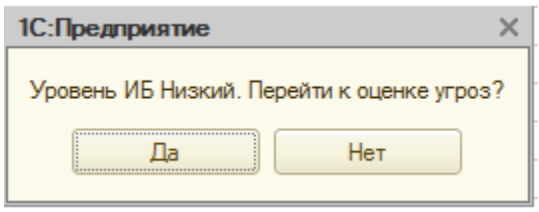


Рисунок 24 – Переход к оценке угроз

4) Если пользователь отказывается оценить угрозы, он может продолжить работу с документом. При нажатии кнопки «Печать» пользователь получает объяснение решения, в котором отображаются промежуточные «возможные» результаты на каждом шаге (рисунок 25).

№	Текст вопроса	Ответ	Промежуточный результат	Вес
1	Информационная система имеет структуру АРМ?	Да	Высокий	1
2	Используется технология виртуализации?	Нет		1
3	Используются системы с технологиями беспроводного доступа?	Нет		
4	Используются ГРИД-системы?	Да	Низкий	
5	Используются суперкомпьютерные системы?	Да	Низкий	
6	ИС имеет файл-серверную архитектуру?	Да	Низкий	
7	Используются разные типы операционных систем?	Да	Средний	
8	Используются прикладные программы, независимые от ОС?	Нет		
9	Используются выделенные каналы связи?	Нет		
10	ИС взаимодействует с иными ИС?	Нет		
11	Невзаимодействующая с другими ИС система?	Да	Средний	
12	ИС является неподключенной к сетям общего пользования?	Нет		
13	ИС подключена к сетям общего пользования через выделенную инфраструктуру?	Да	Средний	
14	ИС подключена к сетям общего пользования?	Да	Низкий	
15	Имеется контрольная зона размещения технических средств?	Нет	Низкий	
16	Имеется контрольная зона размещения технических средств?	Нет	Низкий	

Результат Низкий

Рисунок 25 – Объяснение результатов поиска

Если пользователь согласен перейти к оценке угроз, формируется документ «Экспертная оценка», тема оценки – «Оценка по СТР-К». Пользователь дает ответы на вопросы, показанные на рисунке 26.

Метод расчета ущерба по каждой угрозе, а также полного ущерба от реализации угроз взят из методики определения угроз безопасности информации в информационных системах ФСТЭК.

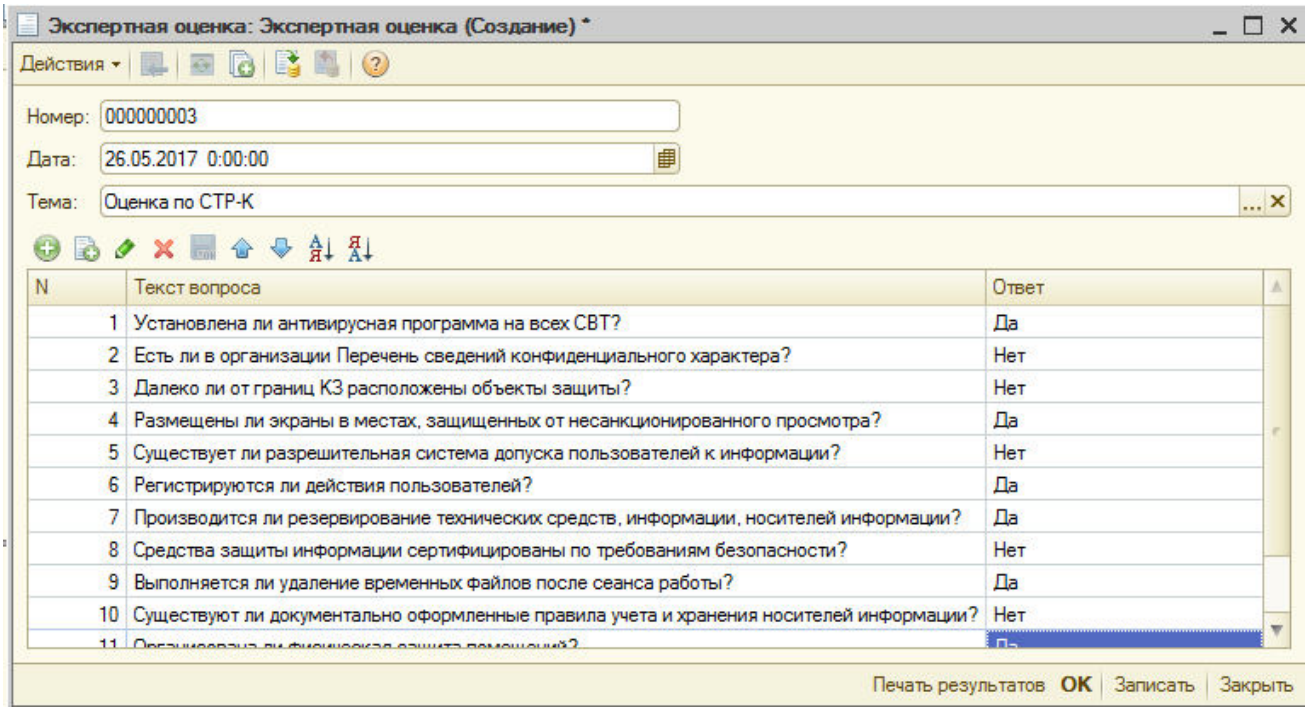
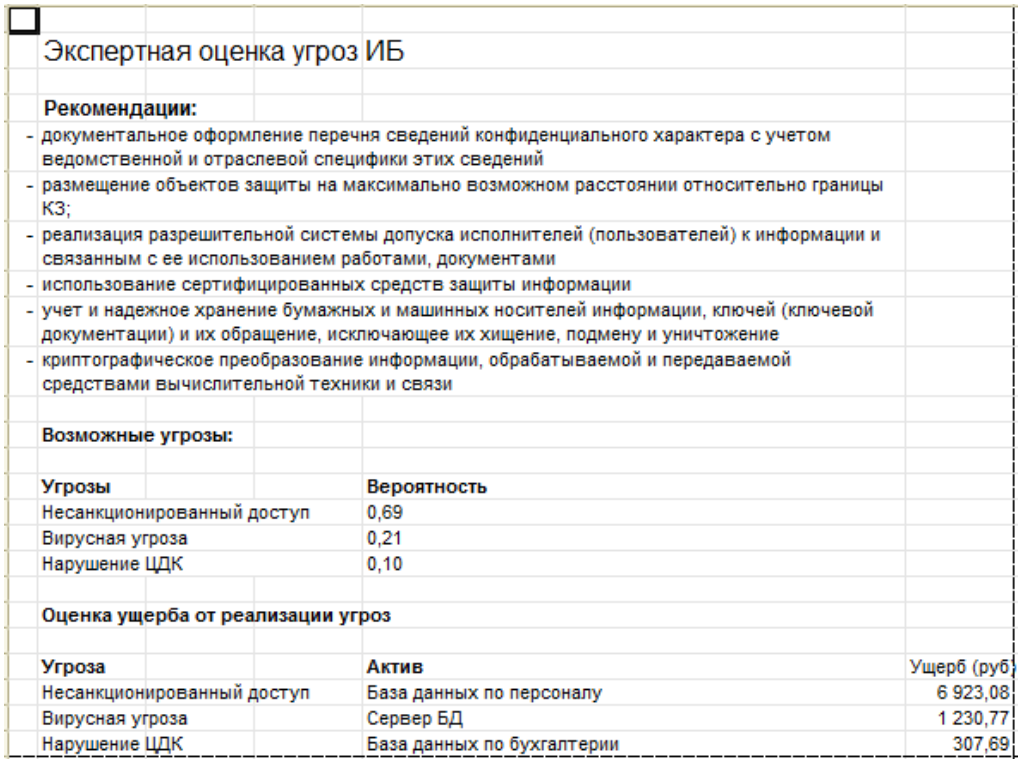


Рисунок 26 – Проверка экспертной оценки

Результаты оценки можно получить после ответа на все вопросы, нажав кнопку «Печать». В сформировавшемся отчете приведены рекомендации по текущему состоянию ИБ, выявлены возможные угрозы и активы, подвергающиеся данной угрозе, оценен ущерб от угроз (рисунок 27).



Экспертная оценка угроз ИБ

Рекомендации:

- документальное оформление перечня сведений конфиденциального характера с учетом ведомственной и отраслевой специфики этих сведений
- размещение объектов защиты на максимально возможном расстоянии относительно границы КЗ;
- реализация разрешительной системы допуска исполнителей (пользователей) к информации и связанным с ее использованием работами, документами
- использование сертифицированных средств защиты информации
- учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение
- криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи

Возможные угрозы:

Угрозы	**Вероятность**
Несанкционированный доступ	0,69
Вирусная угроза	0,21
Нарушение ЦДК	0,10

Оценка ущерба от реализации угроз

Угроза	**Актив**	Ущерб (руб)
Несанкционированный доступ	База данных по персоналу	6 923,08
Вирусная угроза	Сервер БД	1 230,77
Нарушение ЦДК	База данных по бухгалтерии	307,69

Рисунок 27 – Отчет по экспертной оценке

В отчете выводится количественная оценка информационной безопасности, выведенная по методике ФСТЭК.

Как видно из приведенных примеров, разработанная система работает корректно. В примерах приведены тестовые данные и правила для осуществления поиска, и оценки. Система позволяет эксперту ввести сколь угодно сложные правила для более точной работы экспертной системы.

ЗАКЛЮЧЕНИЕ

В работе выполнялась разработка экспертной системы информационной безопасности.

Экспертные системы предназначены для использования знаний профессионалов-экспертов в определенных предметных областях. Разработанная экспертная система хранит и использует знания в области информационной безопасности.

На сегодняшний день разработаны определенные методики и рекомендации в области информационной безопасности, однако разобраться с ними может только профессионал. Поэтому использование профессиональных знаний эксперта возможно посредством экспертной системы.

Целью данной работы является разработка экспертной системы информационной безопасности. Для достижения поставленной цели были решены следующие задачи:

1) Исследованы возможности и структуру экспертных систем, проанализированы модели данных, используемых в экспертных системах. В результате анализа определено, что наиболее удобной моделью данных для разрабатываемой системы является система продукционных правил. Определено также, что в состав экспертной системы должны входить такие функциональные блоки, как база знаний, интерфейс, модули приобретения знаний, логических выводов и объяснений.

2) Изучены методы оценки информационной безопасности. Изучены алгоритмы качественной и количественной оценки ИБ. Выполнен анализ моделей угроз ИБ.

3) Определен функциональный состав разрабатываемой экспертной системы. Система должна выполнять функции приобретения знаний, представления знаний, получения ответа, поиска решения, объяснения решения, вспомогательные функции.

4) Спроектирована объектно-ориентированная модель данных разрабатываемой системы. В качестве среды реализации выбрана система 1С:Предприятие 8.3. Выбор обусловлен с одной стороны тем, что это наиболее удобная система решения прикладных задач, а с другой стороны тем, что это наиболее популярная в РФ программу разработки офисных приложений.

5) Реализована экспертная система. Для системы реализован пользовательский интерфейс, реализована модель данных как набор справочников и документов. В выбранной среде программирования реализованы алгоритмы обработки информации для проведения экспертной оценки.

6) Сформированы и введены правила оценки экспертной безопасности на предприятии. Правила сформированы на основании методик оценки ИБ, предложенных ФСТЭК РФ. Выполнена проверка системы, реализован контрольный пример.

Реализованная система может быть использована для оценки ИБ на предприятии. Огромным преимуществом данной системы является возможность легко пополнять базу знаний, вводить правила по другим методикам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями от 25 ноября, 27 декабря 2009 г.) // Собр. Законодательства Российской Федерации. – 2006. – ст.1–25.

2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» // Собр. Законодательства Российской Федерации. – 2006. – ст.1–18.

3. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]: указ, утвержденный Президентом Российской Федерации В. В. Путиным 5 декабря 2016 г., № 646. Доступ из справ.-правовой системы «Гарант».

4. Концепция национальной безопасности Российской Федерации [Электронный ресурс]: указ Президента РФ от 10 января 2000 года № 24. Доступ из справ.-правовой системы «Гарант».

5. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства РФ от 01.11.2012 №1119. Доступ из справ.-правовой системы «Гарант».

6. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: утвержден приказом № 21 от 18.02.2013 г. Доступ из справ.-правовой системы «Гарант».

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008 г.[10]

8. Методика определения угроз безопасности информации в информационных системах. Утверждена ФСТЭК России в 2015 г. [11]

9. Об утверждении порядка проведения классификации информационных систем персональных данных [Электронный ресурс]: утвержден приказом №

55/86/20 Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 г. Доступ из справ.-правовой системы «Гарант».

10. Требования к средствам антивирусной защиты. [Электронный ресурс]: утвержден приказом № 28 от 20.03.12 г. Доступ из справ.-правовой системы «Гарант».

11. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. [Электронный ресурс]: утвержден приказом № 27 от 12.03.12 г. Доступ из справ.-правовой системы «Гарант».

12. Требования к системам обнаружения вторжений [Электронный ресурс]: утвержден приказом № 638 от 06.12.11. Доступ из справ.-правовой системы «Гарант».

13. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утвержден Заместителем директора ФСТЭК России от 25.12.06 г.

14. Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), утвержден приказом № 282 Гостехкомиссии России от 30.08.02.

15. Руководящий документ «Автоматизированные системы Защита от несанкционированного доступа к информации», утвержден решением Гостехкомиссии России от 20.03.1992 г.

16. Андрианов В.В. Обеспечение информационной безопасности бизнеса / С.Л. Зефиров, В.Б. Голованов, Н.А. Голдуев. – М.: Альпина Паблишерз, 2011. – 338 с.

17. Вишняков, С.М. Угрозы и защищенность объектов системами комплексной безопасности / С. М. Вишняков // Системы безопасности. – 2008. – № 2. – С. 30-39.

18. Воронин, В.В. Технология интеграции продукционных экспертных систем в клиент-серверное окружение / В.В. Воронин, П.Н. Семченко. – Хабаровск:

Издательство Тихоокеанского гос. университета, 2014. – 141 с.

19. Гвоздева, Г.В. Проектирование информационных систем / Г.В. Гвоздева, Б.А Баллод. – Ростов н/Д.: Феникс, 2013 - 508 с.

20. Грибунин, В. Г. Комплексная система защиты информации на предприятии: учебное пособие – М.: «Академия», 2013. – 416 с.

21. Головчинер, М.Н. Интеллектуальные информационные системы, Курс лекций. – Томск: ТГУ, 2015. – 97 с.

22. Ездаков, А.Л. Экспертные системы САПР: учебное пособие – М.: ИД ФОРУМ, 2013. – 160 с.: ил.; 60х90 1/16.

23. Заляжных, В.А. Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем / В.А. Заляжных, А.В. Гирик. – СПб: Университет ИТМО, 2014. – 136 с.

24. Исаев, Г.Н. Проектирование информационных систем: учебное пособие – М.: Омега– Л, 2013. – 55 с.

25. Казиев, В.М. Введение в анализ, синтез и моделирование систем: учебное пособие – Интернет-Университет Информационных Технологий, 2014. – 126 с.

26. Кузин, А.В. Базы данных / А.В. Кузин, С.В. Левонисова. – М.: Академия, 2012. – 317 с.

27. Защита информации / под ред. В.П. Мельникова. – М: Академия, 2014. – 44 с.

28. Никаноров, И. Ю., Сравнение и анализ моделей представления знаний в экспертных системах / И. Ю. Никоноров, Д. Г. Васёв, А. А. Филимонова // Научные исследования: от теории к практике – 2015. – №5. – 90 с.

29. Потапов, А.С. Технологии искусственного интеллекта: моногр. / А.С. Потапов – СПб: СПбГУ ИТМО, 2010. – 221 с.

30. Торокин, А.А. Инженерно-техническая защита информации: учебное пособие. – М.: Гелиос АРВ, 2005. – 72 с.

31. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: моногр. / В.Ф. Шаньгин – М: Инфра-М, 2010. – 148 с.

32. Информационная безопасность: учеб. / ред. В.И. Ярочкин – 2-е изд., – М.:

Академический Проект, 2014. – 544 с.

33. Методика оценки рисков информационной безопасности. [Электронный ресурс] : доклад / П.В. Плетнев, В.М. Белов. – М., 2013. – Режим доступа : http://cyberleninka.ru/

34. Созинова, Е.Н. Применение экспертных систем для анализа и оценки информационной безопасности/ Е.Н. Созинова // Молодой ученый. – 2011. – №10. – С. 64-66.

35. Болтунов, А.И. Применение экспертных систем для решения задач информационной безопасности / А. И. Болтунов, Л. Н. Кротов // Международный научно-исследовательский журнал. – 2016. – № 9 (51) Часть 2. – С. 9-12.

36. Лаборатория Касперского [Электронный ресурс] : офиц. сайт. – 25.10.2001 Режим доступа : http://www.kaspersky.ru. – 14.04.2009

37. Королева, Н.А. Экспертная система поддержки принятия решений по обеспечению информационной безопасности организации : автореф. дис. на соискание ученой степени кандидата наук / Н.А. Королева. – Тамбов: Изд-во ТГУ, 2006. –28 с.

38. Гончаров, Д. И. Технологии интеграции «1С:Предприятия 8.2» / Д.И. Гончаров, Е. Ю. Хрусталева. – СПб.: 1С-Паблишинг, 2014. – 273 с.

39. Радченко, М.Г. 1С: Предприятие 8.1. Практическое пособие разработчика : моногр. / М.Г. Радченко. – СПб.: 1С-Паблишинг, 2013. – 322 с.

40. Джарратано, Д. Экспертные системы: принципы разработки и программирование / Д. Джарратано, Г. Райли. – 4-е изд. – пер. с англ. – М.: И.Д. Вильямс, 2007. – 1152 с.

41. Шориков, А.Ф. Компьютерная экспертная система бизнес-планирования / А.Ф. Шориков, Е.В. Буценко, В.Г. Крылов // Прикладная информатика. – 2016. – №5. – С. 8–18.

42. Ахаев, А.В. Алгоритмы и программные средства построения экспертных систем выбора программных продуктов на примере «1С:Предприятие 8» / А.В. Ахаев, И.А. Ходашинский // Информатика и системы управления. – 2013. – №4(38) – С. 36–42.

ПРИЛОЖЕНИЕ А

Техническое задание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Полное наименование системы

Полное наименование системы: «Разработка экспертной системы для анализа и оценки информационной безопасности».

1.2 Наименование предприятия разработчика и заказчика системы, их реквизиты

Заказчик: Амурский государственный университет.

Реквизиты предприятия заказчика:

1. Юридический адрес: 675027, Амурская область, г. Благовещенск, Игнатьевское шоссе, 21.
2. Телефон: 394-530
3. Сайт: www.amursu.ru
4. E-mail ВУЗа: master@amursu.ru

Разработчик: Козулин Сергей Викторович – студент 553ОМ группы факультета математики и информатики Амурского государственного университета.

1.3 Перечень документов, на основании которых разрабатывается экспертная система информационной безопасности

Используемые документы, на основании которых создается ЭС:

- Федеральный закон от 27 июля 2006 года №149 «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года №152 «О персональных данных» в редакции от 05.04.2013 г.;
- Перечень сведений конфиденциального характера, утвержденный Указом Президента РФ от 06.03.1997 №188;

- Постановление Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года №55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный №11462);

- Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России);

- Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России);

- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом О персональных данных»;

- Постановление Правительства «Об утверждении положения об особенностях обработки персональных данных без использования средств автоматизации» от 15.09.2008г. № 687;

- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных от 21 февраля 2008 г. № 149/6/6-622.

- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) от 30 августа 2002 г.

1.4 Плановые сроки начала и окончания работ

Начало работ: 01.09.2016

Окончание работ: 04.06.2017

Продолжение ПРИЛОЖЕНИЯ А

Техническое задание

1.5 Сведения об источниках и порядке финансирования работ

Экспертная система является учебной, выполняется без привлечения каких либо финансовых средств извне.

1.6 Порядок оформления и предъявления заказчику результатов разработки экспертной системы информационной безопасности

Система передается в виде функционирующего комплекса на базе средств вычислительной техники Заказчика и Исполнителя в установленные сроки. Приемка системы осуществляется Заказчиком.

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1 Назначение системы

Разрабатываемая экспертная система информационной безопасности предназначена для предотвращения разглашения, утечки и несанкционированного доступа к источникам конфиденциальной информации, предотвращения ущерба за счет хищения информации, предотвращения нарушений работы технических средств обеспечения производственной деятельности, включая средства информатизации.

Данная экспертная система информационной безопасности позволит:

- своевременно выявлять и устранять угрозы информационным ресурсам предприятия; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам предприятия, нарушения его нормального функционирования и развития.

- создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия;

- эффективное пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности;

Продолжение ПРИЛОЖЕНИЯ А

Техническое задание

- создание условий для максимального возможного возмещения и локализации наносимого ущерба неправомерными действиями юридических и физических лиц, для ослабления негативного влияния последствий нарушения безопасности.

2.1 Назначение системы

- своевременно выявлять и устранять угрозы информационным ресурсам предприятия; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам предприятия, нарушения его нормального функционирования и развития.

- создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия;

- эффективное пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности;

- создание условий для максимального возможного возмещения и локализации наносимого ущерба неправомерными действиями юридических и физических лиц, для ослабления негативного влияния последствий нарушения безопасности

2.2 Цели создания системы

Главной целью экспертной системы информационной безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов Заказчика от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты,

утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта.

Другой целью системы информационной безопасности является повышение качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов.

Продолжение ПРИЛОЖЕНИЯ А

Техническое задание

3 ТРЕБОВАНИЯ К СИСТЕМЕ

3.1 Требования к системе в целом

3.1.1 Требования к структуре и функционированию системы

Разрабатываемая система должна состоять из следующих компонент:

1. База знаний - база данных, содержащая правила, вопросы и ответы.
2. Модуль приобретения знаний – данный модуль нужен для заполнения базы знаний.
3. Модуль логических выводов - этот модуль необходим в ЭС для формирования решения поставленной задачи.
4. Модуль взаимодействия с пользователем – этот модуль представляет собой пользовательский интерфейс, который необходим для правильной и удобной передачи ответов пользователю, а также для осуществления манипуляций с базой знаний эксперту.
5. Модуль советов и объяснений – нужен для объяснения решения задачи.

3.1.2 Требования к персоналу

Пользователям системы будут являться сотрудники предприятия.

Для работы с системой пользователю необходимо иметь базовые навыки работы с персональным компьютером и ОС Windows в том числе.

При этом весь персонал системы обязан до начала эксплуатации системы ознакомиться с эксплуатационной документацией (руководство пользователя).

3.1.3 Требования к надежности

Разработанная экспертная система информационной безопасности должна обеспечивать достаточно высокую степень отказоустойчивости.

3.1.3.1 Состав и количественные значения показателей надежности для системы в целом

Надежность системы в целом определяется надежностью функционирования ее компонентов, а также надежностью обеспечивающих технических и программных средств:

- технические средства;

Продолжение ПРИЛОЖЕНИЯ А

Техническое задание

– серверы, рабочие станции, сетевое аппаратное обеспечение;

– сетевые кабельные соединения, устройства бесперебойного питания;

программные средства:

– системное программное обеспечение, установленное на серверах и рабочих станциях;

– прикладное программное обеспечение, установленное на серверах и рабочих станциях.

Надежность системы также зависит от следующих факторов:

– условий эксплуатации системы;

– соблюдения организационных и организационно-технических мероприятий, регламентных работ по эксплуатации системы.

Для системы устанавливаются следующие количественные значения показателей надежности:

– режим работы системы в целом - 5 дней в неделю 12 часов в сутки

– допустимое максимальное временя восстановления работоспособности при любых сбоях и отказах не должно превышать 4-х часов. В это значение входит разворачивание и настройка специального ПО на сервере, а также восстановление данных с использованием последней резервной копии. В указанное время не входит решение проблем с техническим обеспечением и инсталляция операционной системы;

– общее допустимое времени простоя в месяц не должно превышать 8-ми часов, включая проведение сервисных и регламентных работ.

Количественные значения показателей надежности должны быть уточнены по результатам опытной эксплуатации системы.

Для поддержания указанных показателей надежности система должна обеспечивать возможность формирования архивных копий БД (дампов). При этом должны поддерживаться следующие операции:

– автоматическое присваивание уникальных семантических имен архивным копиям;

– восстановление БД из архивных копий в случае необходимости;

– ведение протоколов выполнения заданий формирования и восстановления архивных копий.

3.1.4.2 Перечень аварийных ситуаций

При разработке системы необходимо учитывать возможность возникновения следующих аварийных ситуаций:

– сбой общего или специального программного обеспечения;

– выход из строя части КТС;

– сбои или выход из строя активного накопителя на жестком магнитном диске;

– ошибки персонала при работе с подсистемой;

– импульсные помехи, сбои или прекращение электропитания.

3.1.4.3 Требования к надежности технических средств и программного обеспечения

Надежность системы должна обеспечиваться:

- использованием технических средств повышенной отказоустойчивости и их структурным резервированием;

– защитой технических средств по электропитанию путем использования источников бесперебойного питания;

– дублированием носителей информационных массивов.

Назначенные сроки службы, среднее время наработки на отказ не устанавливаются, а определяются в соответствии с заявленными производителями характеристиками выбранных технических средств.

3.1.5 Требования к безопасности

Продолжение ПРИЛОЖЕНИЯ А

Техническое задание

Программно-аппаратные средства Системы должны обеспечивать безопасность обслуживающего персонала при эксплуатации, техническом обслуживании и ремонте с учетом требований ГОСТ 21552-84, ГОСТ 25861-83.

Электробезопасность должна соответствовать требованиям ГОСТ 12.1.030-81, ГОСТ 12.2.003, ГОСТ 12.2.007.0-75.

Силовые кабельные комплексы технических средств системы должны отвечать требованиям «Правил устройств электроустановок» (ПУЭ).

3.1.6 Требования к эргономике и технической эстетике

Разрабатываемая экспертная система дожна соответствовать требования эргономики и технической эстетики. Система должна создаваться с учетом обеспечения максимального удобства и и комфорта для пользователей. Для этого необходимо предусмотреть применение интуитивно понятного пользователю интерфейса с использованием понятной для пользователя терминологии.

Создаваемое ПО ориентированно на пользователя, владеющего навыками работы в операционной системе Windows XP, Windows 7, 8, 10. Интерфейс программы должен быть интуитивно понятен и разработан с учетом группировки элементов по смысловым признакам. Интерфейс требует от пользователя минимум

действий, а вся вводимая информация контролируется, что делает ввод ошибочных данных маловероятным.

3.1.7 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

Требования к эксплуатации, техническому обслуживанию, ремонту и хранению системы включают в себя предоставление инструкций, методических и нормативных материалов по использованию и эксплуатации информационной системы. Технические средства системы должны быть установлены так, чтобы обеспечивалась их безопасная эксплуатация и техническое обслуживание. Для сопровождения технических средств в процессе эксплуатации необходимо

привлечение специалистов по обслуживанию компьютерной и оргтехники.

Устройство хранения данных дожно быть защищено от внешних физических воздействий.

3.1.8 Требования к защите информации от несанкционированного доступа

Экспертная система информационной безопасности должна соответствовать требованиям к защите информации от несанкционированногоо доступа. Система должна иметь разграничения прав доступа к данным в соответствии с функциями

пользователя, контроль правильной работы и разграничение прав должен осуществляется пользователями системы.

3.1.9 Требования по сохранности информации при авариях

После аварийного выхода из программы следует средствами СУБД проверить БД на наличие ошибок, и в случае обнаружения таковых по возможности исправить их. Ущерб программному обеспечению в случае аварийного выхода маловероятен, но при возникновении проблем рекомендуется переустановить систему без файла инициализации.

3.1.10 Требования по стандартизации и сертификации

В соответствии с требованиями по стандартизации и сертификации при проектировании, создании экспертной системы информационной безопасности и оформлении документации следует учесть следующие стандарты:

ГОСТ 7.1-2003 – «Библиографическое описание документа. Общие требования и правила составления»;

ГОСТ 19.001-77 – «ЕСПД. Общие положения»;

ГОСТ 19.004-80 – «ЕСПД. Термины и определения»;

ГОСТ 19.004-80 – «ЕСПД. Виды программ и программных документов»;

ГОСТ 19.101-77 – «ЕСПД. Стадии разработки»;

ГОСТ 19.103-77 – «ЕСПД. Обозначение программ и программных документов»;

ГОСТ 19.104-78 – «ЕСПД. Основные надписи»;

ГОСТ 19.105-78 – «ЕСПД. Требования к программным документам, выполненным печатным способом»;

ГОСТ 19.402-78 – «ЕСПД. Описание программы»;

ГОСТ 19.502-78 – «Описание применения. Требования к содержанию и оформлению»;

ГОСТ 19.505-79 – «Руководство оператора. Требования к содержанию и оформлению»;

ГОСТ 19.508-79 – «Руководство по техническому обслуживанию. Требования к содержанию и оформлению»;

ГОСТ 24.301-80 – «Общие требования к выполнению текстовых документов»;

ГОСТ ИСО/МЭК 15408-2-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности;

ГОСТ ИСО/МЭК 15408-3-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности

информационных технологий. Часть 3. Требования доверия к безопасности;

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения;

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения;

ГОСТ Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической зашиты информации;

3.2 Требования к функциям, выполняемым системой

3.2.1 Перечень подлежащих решению задач

Разрабатываемая система должна решать следующие задачи:

Продолжение ПРИЛОЖЕНИЯ А

Техническое задание

1. Своевременно выявлять и устранять угрозы информационным ресурсам предприятия; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам предприятия, нарушения его нормального функционирования и развития.

2. Создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия;

3. Эффективное пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности;

4. Создание условий для максимального возможного возмещения и локализации наносимого ущерба неправомерными действиями юридических и физических лиц, для ослабления негативного влияния последствий нарушения безопасности

3.2.2 Временной регламент реализации каждой функции

Обработка данных и выполнение функций в системе должны происходить в интерактивном режиме. Допускается естественная задержка в обработке данных при выполнении функции, связанная с большим объемом обрабатываемых данных.

3.2.3 Требования к качеству реализации каждой функции, формы выходной информации, характеристики достоверности

Качество реализации функций должно обеспечивать полное выполнение входящих в их состав операций и задач и гарантировать корректную с точки зрения предметной области обработку данных и представление результатов.

3.2.4 Перечень и критерии отказа

Отказом является невозможность корректного выполнения функции или завершения операции с успешным признаком. Критерием отказа является нарушение выполнения функциональности экспертной системы.

3.3 Требования к видам обеспечения

3.3.1 Требования к математическому обеспечению

Продолжение ПРИЛОЖЕНИЯ А

Техническое задание

Выполнение стандартных математических функций с использованием бесплатных или имеющихся в наличии программных и технических средств.

3.3.2 Требования к метрологическому обеспечению

Требования к метрологическому обеспечению не предъявляются.

3.3.3 Требования к информационному обеспечению

Информационное обеспечение представляет собой совокупность входных и выходных потоков данных. Наиболее важным компонентом информационного обеспечения является база данных системы. В ней содержится информация, необходимая для формирования выходных данных. Информация, поступающая в БД, должна быть полной, правдивой и непротиворечивой.

3.3.4 Требования к лингвистическому обеспечению

Требования к лингвистическому обеспечению также предполагают использование единого логически понятного интерфейса для пользователей. Ввод

и вывод данных должен производиться в удобном формате на русском или английском языке.

3.3.5 Требования к программному обеспечению

Разрабатываемая система не накладывает жестких ограничений на программные средства клиентских станций.

На клиентской стороне обязательно наличие пакета офисных программ (для работы с генерируемыми документами). Операционная система Windows начиная с 7 версии.

3.3.6 Требования к техническому обеспечению

Требования к техническим средствам клиентских рабочих станций – минимальны. Предложенная архитектура обеспечит работоспособность системы на любой клиентской платформе.

Требования к техническим характеристикам ПК:

– процессор от Intel Pentium IV 2,4 ГГц и выше;

– объем оперативной памяти 2 Гб;

– дисковая система 120 Гб;

– сетевой адаптер – 100 Мбит/с.

3.3.7 Требования к организационному обеспечению

Для работы с экспертной системой информационной безопасности необходимо разработать руководство пользователя, внести изменения в организационную документацию, скорректировать должностные инструкции работников.

3.3.8 Требования к методическому обеспечению

Требования к методическому обеспечению не предъявляются.

4 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

4.1 Перечень стадий и этапов работ по созданию системы

Этапы, которые необходимо выполнить по созданию экспертной системы:

1 этап – Исследование предметной области, выделение объекта автоматизации. По окончании данного этапа будут разработаны контекстные диаграммы, диаграммы потоков данных и другие схемы.

2 этап – Составление технического задания: выяснение требований заказчика к разрабатываемой системе, определение технических и программных средств, необходимых для реализации проекта, уточнение функций системы.

3 этап – Проектирование экспертной системы информационной безопасности:

4 этап – Программная реализация экспертной системы информационной безопасности;

5 этап – Согласование созданной экспертной системы информационной безопасности с требованиями заказчика, учет всех полученных замечаний и указаний;

6 этап - Составление документации (разработка рабочей документации на систему);

7 этап – Внедрение системы: установка и настройка программно-аппаратных средств, выявление и устранение неполадок.

4.2 Сроки выполнения

Продолжение ПРИЛОЖЕНИЯ А

Техническое задание

На разработку экспертной системы информационной безопасности отводится срок с сентября 2016 по июнь 2017.

4.3 Состав организации исполнителя работ

Все виды работ выполняются студентом 553ОМ группы Амурского Государственного университета Козулиным Сергеем Викторовичем.

4.4 Вид и порядок экспертизы технической документации

Вид и порядок экспертизы технической документации определяет Заказчик в одностороннем порядке.

4.5 Программа обеспечения надежности

Требования по обеспечению надежности указаны в п.4.1.4 данного технического задания.

4.6 Программа метрологического обеспечения

Программой метрологического обеспечения в соответствии с п. 4.3.8 данного технического задания может являться любое стороннее средство, удовлетворяющее заявленному требованию к метрологическому обеспечению.

5 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

5.1 Виды, состав, объем и методы испытания

В процессе приемки проекта экспертной системы информационной безопасности должен быть проведены следующие действия:

– анализ выполненной работы;

– проверка соответствия проекта поставленной задаче и обеспечения выполнения поставленных требований;

– корректировка системы по результатам;

– определение достоинств и недостатков разработанной системы.

5.2 Общие требования приемки работ по стадиям

Сдача-приёмка работ производится поэтапно, в соответствии с рабочей программой и календарным планом. Сдача-приемка осуществляется комиссией, в состав которой входят представители Заказчика. Приемка ИС осуществляется в при-

сутствии представителей Исполнителя. По результатам приемки подписывается акт приемочной комиссии.

Все создаваемые в рамках настоящей работы программные изделия передаются Заказчику, как в виде готовых модулей, так и в виде исходных кодов, предоставленных в электронной форме на стандартном машинном носителе.

5.3 Статус приемной комиссии

Кафедра информационных и управляющих систем Амурского государственно-

го университета.

6 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

6.1 Перечень подлежащих разработке документов

Состав и содержание документации должны соответствовать требованиям ГОСТ 34.201-89 и нормативно-технических документов (комплекса стандартов и руководящих документов на экспертной системы и единой подсистемы программной документации).

Документация на разрабатываемую систему должна включать:

– эксплуатационную документацию, предназначенную для использования при эксплуатации системы;

– описание программного продукта;

– руководство пользователя;

– техническое задание;

6.2. Перечень документов на машинных носителях

Документация из пункта 8.1 должна быть представлена на машинных носителях.

Продолжение ПРИЛОЖЕНИЯ А

Техническое задание

7 ИСТОЧНИКИ РАЗРАБОТКИ

7.1 Документы и информационные материалы, на основании которых разрабатывается техническое задание

Техническое задание разработано в соответствии с Комплексом стандартов и руководящих документов на экспертной системы с использованием следующих нормативно-технических документов:

– ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем»;

– ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3

– ГОСТ Р ИСО/МЭК ТО 24762 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения»

– ГОСТ Р ИСО/МЭК 12207-99 «Процессы жизненного цикла программных средств»;

ПРИЛОЖЕНИЕ Б

Структурированные правила поиска

14. ЕСЛИ (Информационная система имеет структуру АРМ?) ТО (Высокий, перейти к 4) ИНАЧЕ (перейти к 2)
15. ЕСЛИ (Информационная система является локальной?) ТО (Средний, перейти к 4) ИНАЧЕ (перейти к 3)
16. ЕСЛИ (Используется распределенная информационная система?) ТО (Низкий, перейти к 4) ИНАЧЕ (перейти к 4)
17. ЕСЛИ (Используется технология виртуализации?) ТО (Низкий, перейти к 5) ИНАЧЕ (перейти к 5)

18. ЕСЛИ (Используются системы с технологиями беспроводного доступа?) ТО (Низкий, перейти к 6) ИНАЧЕ (перейти к 8)
19. ЕСЛИ (Используются системы, реализующие облачные вычисления?) ТО (Низкий, перейти к 7) ИНАЧЕ (перейти к 7)
20. ЕСЛИ (Используются системы с мобильными устройствами?) ТО (Низкий, перейти к 8) ИНАЧЕ (перейти к 8)
21. ЕСЛИ (Используются ГРИД-системы?) ТО (Низкий, перейти к 9) ИНАЧЕ (перейти к 9)
22. ЕСЛИ (Используются суперкомпьютерные системы?) ТО (Низкий, перейти к 10) ИНАЧЕ (перейти к 10)
23. ЕСЛИ (ИС имеет файл-серверную архитектуру?) ТО (Низкий, перейти к 15) ИНАЧЕ (перейти к 11)
24. ЕСЛИ (ИС основана на одноранговой сети?) ТО (Средний, перейти к 15) ИНАЧЕ (перейти к 12)
25. ЕСЛИ (ИС строится на основе "тонкого клиента"?) ТО (Высокий, перейти к 15) ИНАЧЕ (перейти к 13)
26. ЕСЛИ (Для работы используются центра обработки данных?) ТО (Низкий, перейти к 14) ИНАЧЕ (перейти к 14)

Продолжение ПРИЛОЖЕНИЯ Б

Структурированные правила поиска

27. ЕСЛИ (Используются системы с удаленным доступом пользователей?) ТО (Низкий, перейти к 15) ИНАЧЕ (перейти к 15)
28. ЕСЛИ (Используются разные типы операционных систем?) ТО (Средний, перейти к 16) ИНАЧЕ (перейти к 16)
29. ЕСЛИ (Используются прикладные программы, независимые от ОС?) ТО (Средний, перейти к 17) ИНАЧЕ (перейти к 17)
30. ЕСЛИ (Используются выделенные каналы связи?) ТО (Средний, перейти к 18) ИНАЧЕ (перейти к 18)

31. ЕСЛИ (ИС взаимодействует с иными ИС?) ТО (Низкий, перейти к 20) ИНАЧЕ (перейти к 19)
32. ЕСЛИ (Невзаимодействующая с другими ИС система?) ТО (Средний, перейти к 20) ИНАЧЕ (перейти к 20)
33. ЕСЛИ (ИС является неподключенной к сетям общего пользования?) ТО (Высокий, перейти к 23) ИНАЧЕ (перейти к 21)
34. ЕСЛИ (ИС подключена к сетям общего пользования через выделенную инфраструктуру??) ТО (Средний, перейти к 22) ИНАЧЕ (перейти к 23)
35. ЕСЛИ (ИС подключена к сетям общего пользования?) ТО (Низкий, перейти к 23) ИНАЧЕ (перейти к 23)
36. ЕСЛИ (Имеется контрольная зона размещения технических средств?) ТО (перейти к 24) ИНАЧЕ (Низкий, перейти к 26)
37. ЕСЛИ (Технические средства расположены в пределах одной контролируемой зоны?) ТО (Высокий, перейти к 26) ИНАЧЕ (перейти к 25)
38. ЕСЛИ (Технические средства расположены в пределах нескольких контрольных зон) ТО (Средний, перейти к 26) ИНАЧЕ (перейти к 26)
39. ЕСЛИ (Режим обработки информации однопользовательский?) ТО (Высокий, перейти к 27) ИНАЧЕ (Низкий, перейти к 27)

Продолжение ПРИЛОЖЕНИЯ Б

Структурированные правила поиска

40. ЕСЛИ (Разграничиваются ли права доступа к ИС?) ТО (Средний, перейти к 28) ИНАЧЕ (Низкий, перейти к 28)
41. ЕСЛИ (Режим разделения функций по управлению ИС без разделения?) ТО (Низкий, перейти к 32) ИНАЧЕ (перейти к 29)
42. ЕСЛИ (Рабочие места для администрирования ИС выделены в отдельный домен?) ТО (Средний, перейти к 32) ИНАЧЕ (перейти к 30)

43. ЕСЛИ (Для разделения функций по управлению ИС используются различные сетевые адреса?) ТО (Низкий, перейти к 32) ИНАЧЕ (перейти к 31)
44. ЕСЛИ (Для администрирования выделены отдельные каналы?) ТО (Средний, перейти к 32) ИНАЧЕ (перейти к 32)
45. ЕСЛИ (Информационная система сегментирована?) ТО (Средний) ИНАЧЕ (Низкий)
46. ЕСЛИ (Информационная система имеет структуру АРМ?) ТО (Высокий, перейти к 4) ИНАЧЕ (перейти к 2)
47. ЕСЛИ (Информационная система является локальной?) ТО (Средний, перейти к 4) ИНАЧЕ (перейти к 3)
48. ЕСЛИ (Используется распределенная информационная система?) ТО (Низкий, перейти к 4) ИНАЧЕ (перейти к 4)
49. ЕСЛИ (Используется технология виртуализации?) ТО (Низкий, перейти к 5) ИНАЧЕ (перейти к 5)
50. ЕСЛИ (Используются системы с технологиями беспроводного доступа?) ТО (Низкий, перейти к 6) ИНАЧЕ (перейти к 8)
51. ЕСЛИ (Используются системы, реализующие облачные вычисления?) ТО (Низкий, перейти к 7) ИНАЧЕ (перейти к 7)
52. ЕСЛИ (Используются системы с мобильными устройствами?) ТО (Низкий, перейти к 8) ИНАЧЕ (перейти к 8)

Продолжение ПРИЛОЖЕНИЯ Б

Структурированные правила поиска

53. ЕСЛИ (Используются ГРИД-системы?) ТО (Низкий, перейти к 9) ИНАЧЕ (перейти к 9)
54. ЕСЛИ (Используются суперкомпьютерные системы?) ТО (Низкий, перейти к 10) ИНАЧЕ (перейти к 10)

55. ЕСЛИ (ИС имеет файл-серверную архитектуру?) ТО (Низкий, перейти к 15) ИНАЧЕ (перейти к 11)
56. ЕСЛИ (ИС основана на одноранговой сети?) ТО (Средний, перейти к 15) ИНАЧЕ (перейти к 12)
57. ЕСЛИ (ИС строится на основе "тонкого клиента"?) ТО (Высокий, перейти к 15) ИНАЧЕ (перейти к 13)
58. ЕСЛИ (Для работы используются центра обработки данных?) ТО (Низкий, перейти к 14) ИНАЧЕ (перейти к 14)
59. ЕСЛИ (Используются системы с удаленным доступом пользователей?) ТО (Низкий, перейти к 15) ИНАЧЕ (перейти к 15)
60. ЕСЛИ (Используются разные типы операционных систем?) ТО (Средний, перейти к 16) ИНАЧЕ (перейти к 16)
61. ЕСЛИ (Используются прикладные программы, независимые от ОС?) ТО (Средний, перейти к 17) ИНАЧЕ (перейти к 17)
62. ЕСЛИ (Используются выделенные каналы связи?) ТО (Средний, перейти к 18) ИНАЧЕ (перейти к 18)
63. ЕСЛИ (ИС взаимодействует с иными ИС?) ТО (Низкий, перейти к 20) ИНАЧЕ (перейти к 19)
64. ЕСЛИ (Невзаимодействующая с другими ИС система?) ТО (Средний, перейти к 20) ИНАЧЕ (перейти к 20)
65. ЕСЛИ (ИС является неподключенной к сетям общего пользования?) ТО (Высокий, перейти к 23) ИНАЧЕ (перейти к 21)

Продолжение ПРИЛОЖЕНИЯ Б

Структурированные правила поиска

66. ЕСЛИ (ИС подключена к сетям общего пользования через выделенную инфраструктуру??) ТО (Средний, перейти к 22) ИНАЧЕ (перейти к 23)
67. ЕСЛИ (ИС подключена к сетям общего пользования?) ТО (Низкий, перейти к 23) ИНАЧЕ (перейти к 23)

68. ЕСЛИ (Имеется контрольная зона размещения технических средств?) ТО (перейти к 24) ИНАЧЕ (Низкий, перейти к 26)
69. ЕСЛИ (Технические средства расположены в пределах одной контролируемой зоны?) ТО (Высокий, перейти к 26) ИНАЧЕ (перейти к 25)
70. ЕСЛИ (Технические средства расположены в пределах нескольких контрольных зон) ТО (Средний, перейти к 26) ИНАЧЕ (перейти к 26)
71. ЕСЛИ (Режим обработки информации однопользовательский?) ТО (Высокий, перейти к 27) ИНАЧЕ (Низкий, перейти к 27)
72. ЕСЛИ (Разграничиваются ли права доступа к ИС?) ТО (Средний, перейти к 28) ИНАЧЕ (Низкий, перейти к 28)
73. ЕСЛИ (Режим разделения функций по управлению ИС без разделения?) ТО (Низкий, перейти к 32) ИНАЧЕ (перейти к 29)
74. ЕСЛИ (Рабочие места для администрирования ИС выделены в отдельный домен?) ТО (Средний, перейти к 32) ИНАЧЕ (перейти к 30)
75. ЕСЛИ (Для разделения функций по управлению ИС используются различные сетевые адреса?) ТО (Низкий, перейти к 32) ИНАЧЕ (перейти к 31)
76. ЕСЛИ (Для администрирования выделены отдельные каналы?) ТО (Средний, перейти к 32) ИНАЧЕ (перейти к 32)
77. ЕСЛИ (Информационная система сегментирована?) ТО (Средний) ИНАЧЕ (Низкий)

ПРИЛОЖЕНИЕ В

Руководство пользователя

1. Разработка руководства пользователя

1.1 Разработка руководства пользователя – администратора

К функциям администратора относятся администрирование БД и верификация правил ЭС.

Администрирование БД – это в первую очередь администрирование справочников. Справочники заполняются в следующем порядке:

1) Справочник «Активы»: администратором заполняются только общие сведения об активе (рисунок 28), оценку угроз выполняет эксперт.

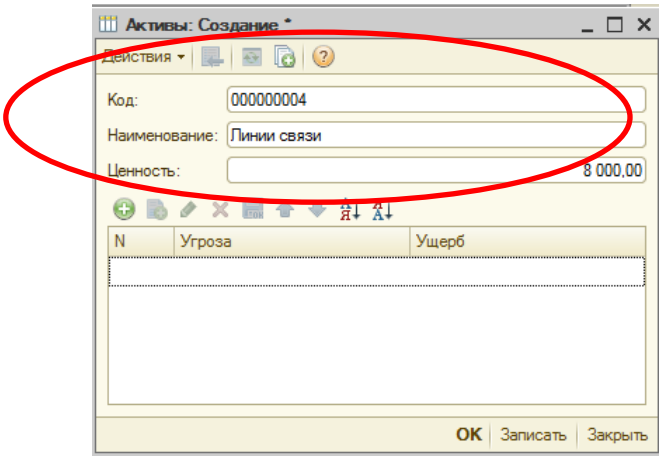


Рисунок 28 – Заполнение справочника «Активы» администратором

В информационную базу необходимо занести следующие типы активов:

– информация/данные;
– аппаратные средства;
– программное обеспечение, включая прикладные программы;
– оборудование для обеспечения связи;
– программно-аппаратные средства;
– документы;
– другие активы.

Продолжение ПРИЛОЖЕНИЯ В

Руководство пользователя

Ценность актива складывается из:

– первоначальной стоимости актива,

– стоимости его обновления или воссоздания.

2) Справочник «Угрозы» заполняется в соответствии с ГОСТ Р ИСО/МЭК ТО 13335-3-2007 [29], в котором определены все типичные угрозы.

3) Справочники «Мероприятия» и «Требования» заполняются в соответствии с Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К) [14]. Экранные формы справочников показаны на рисунках 15-16.

4) Справочник «Темы» заполняется по требованию эксперта при внесении в базу нового пакета правил для оценки ИБ или поиска решений.

Остальные справочники администратор может редактировать, удалять помеченные объекты, но он не отвечает за содержание этих справочников. То же касается и других объектов экспертной системы.

1.2 Разработка руководства пользователя – эксперта

К основным функциям эксперта относятся:

- оценка угроз активам предприятия;
- ввод экспертных правил;
- верификация правил.

Для выполнения первой функции эксперту предоставляется справочник «Активы», уже частично заполненный администратором. Эксперт открывает справочник и для каждого актива проставляет возможные угрозы и количественную (денежную) оценку ущерба (рисунок 29).

Продолжение ПРИЛОЖЕНИЯ В

Руководство пользователя

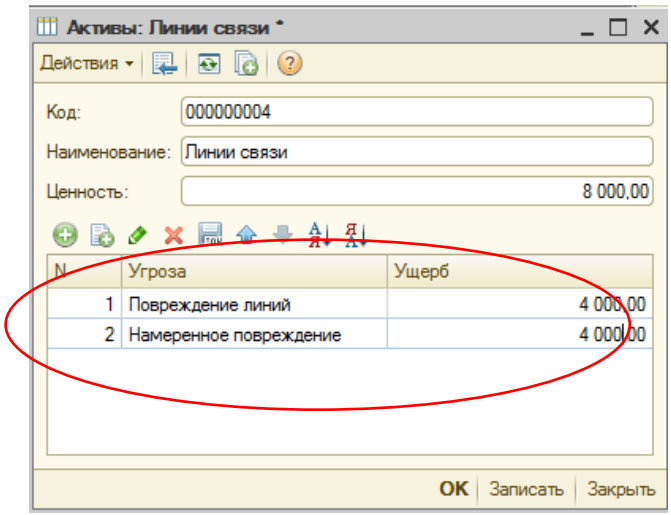


Рисунок 29 – Заполнение справочника «Активы» экспертом

Для ввода экспертных правил эксперт заполняет справочники «Правила оценки» и «Правила поиска».

Правила оценки состояния информационной безопасности на предприятии составляются в соответствии с определенной методикой, например, изложенной в СТР-К. Перед заполнением справочника «Правила оценки» эксперт должен убедиться, что заполнены справочники «Темы», «Требования», «Угрозы». В случае нехватки данных в последних двух справочниках эксперт может внести необходимые данные.

Для внесения новых правил оценки (поиска) эксперт должен зайти в справочник «Темы» и выбрать тематику оценки (поиска) (рисунок 30). Выбрав нужную тему, эксперт нажимает кнопку «Перейти» и открывает справочник с соответствующими правилами. При этом в справочнике отбираются только правила, соответствующие данной теме.

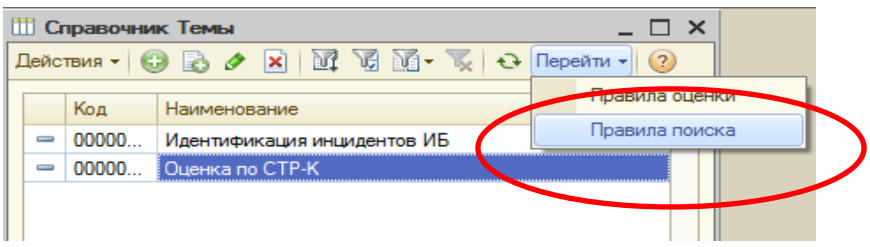


Рисунок 30 – Открытие справочника «Правила оценки»

Продолжение ПРИЛОЖЕНИЯ В

Руководство пользователя

В справочнике «Правила оценки» (рисунок 31) эксперт заносит:

- в поле «Наименование» - краткое наименование вопроса;

- в поле «Владелец» автоматически выставляется тема правила;

- в поле «Вопрос» - полный текст вопроса, который будет задан пользователю (аудитору) при выполнении экспертной оценки;

- в поле «Требование» выбирается из соответствующего справочника требование, которое оценивает данное правило;

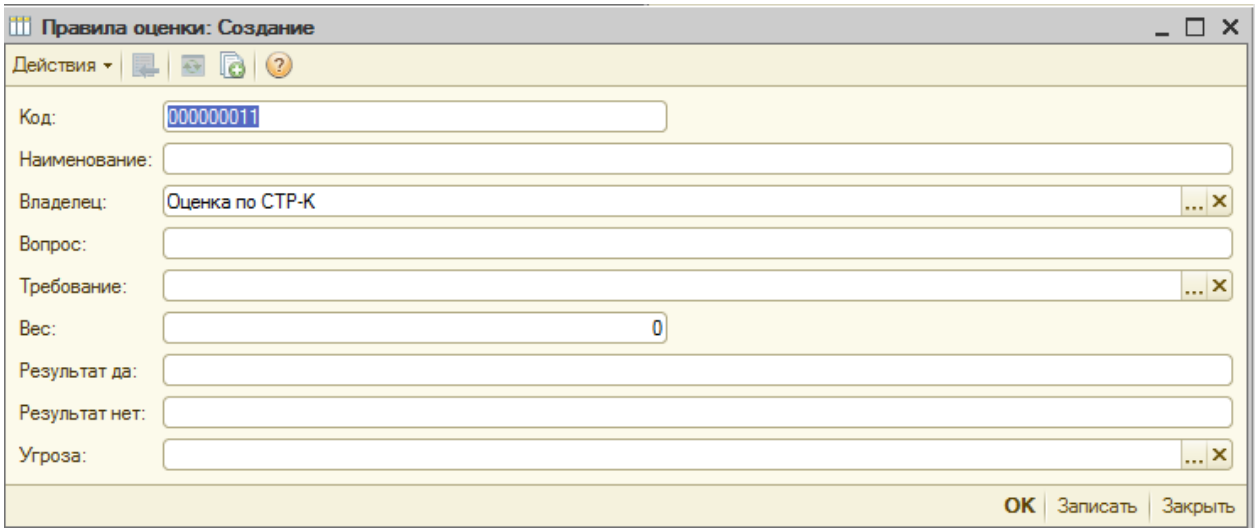


Рисунок 31 – Форма справочника «Правила оценки»

- в поле «Вес» указывается, насколько данное правило оценивает соответствие требованию: при наличии нескольких правил по одному требованию они могут быть неравнозначны;

- в поле «Результат Да» записываются рекомендации, которые даются пользователю, если ответ на вопрос положительный;

- в поле «Результат Нет» записываются рекомендации, которые даются пользователю, если ответ на вопрос отрицательный;

- в поле «Угроза» эксперт выбирает из справочника угрозу, оцениваемую данным требованием.

Продолжение ПРИЛОЖЕНИЯ В

Руководство пользователя

Для работы с правилами поиска для идентификации инцидентов ИБ, эксперт должен сперва заполнить справочник «Инциденты». Справочник «Инциденты» заполняется после заполнения справочника «Угрозы», поскольку имеет ссылки на элементы этого справочника. В справочнике перечисляются возможные и произошедшие инциденты ИБ и их связь с угрозами ИБ (рисунок 18).

В справочнике «Правила поиска», который также должен быть открыт из справочника «Темы», эксперт заносит правила для идентификации инцидентов ИБ. В справочник заносятся (рисунок 32):

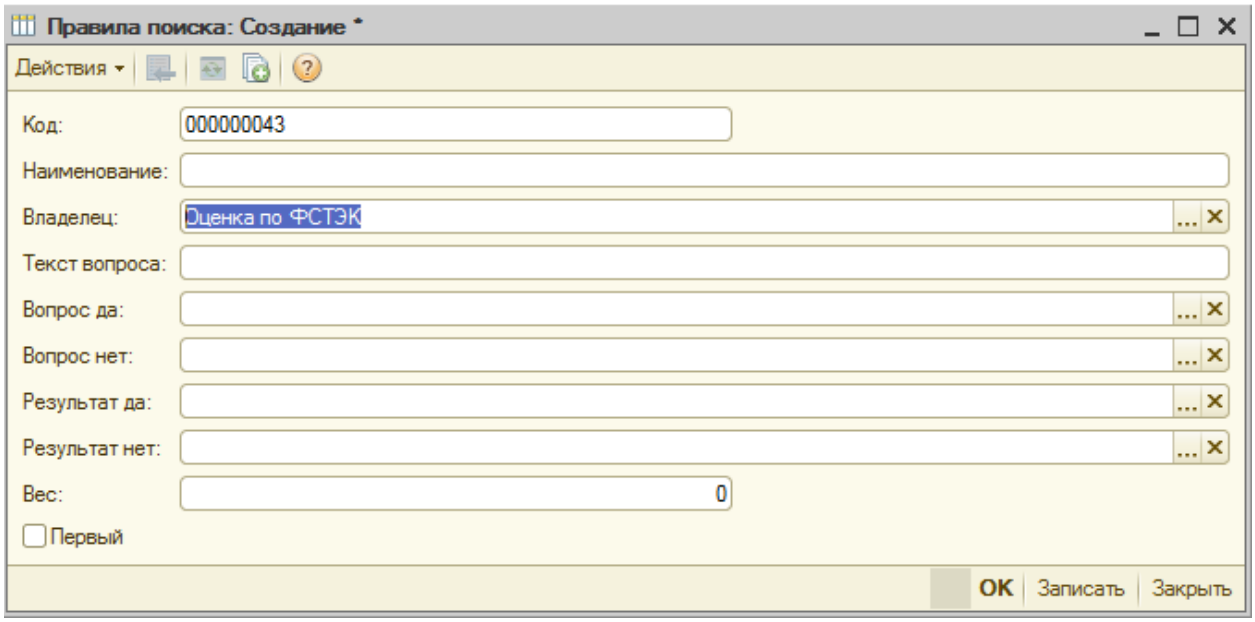


Рисунок 32 – Форма справочника «Правила поиска»

- в поле «Наименование» - краткое наименование правила;

- в поле «Владелец» автоматически выставляется тема правила;

- в поле «Вопрос» - полный текст вопроса, который будет задан пользователю при выполнении поиска;

- в поле «Вопрос Да» указывается вопрос, который будет следующим задан пользователю при ответе «Да» на текущий вопрос. В данное поле выбирается значение из этого же справочника;

Продолжение ПРИЛОЖЕНИЯ В

Руководство пользователя

- в поле «Вопрос Нет» указывается вопрос, который будет следующим задан пользователю при ответе «Нет» на текущий вопрос. В данное поле выбирается значение из этого же справочника;

- в поле «Результат Да» указывается результат, который соответствует ответу «Да» на текущий вопрос. В данное поле выбирается значение из справочника «Инциденты»;

- в поле «Результат Нет» указывается результат, который соответствует ответу «Нет» на текущий вопрос. В данное поле выбирается значение из справочника «Инциденты»;

- в поле «Вес» указывается, насколько точно данный вопрос идентифицирует указанный инцидент;

- в поле «Первый» ставится флаг, если данный вопрос должен быть задан первым. В одной теме может быть только один вопрос, помеченный этим флагом.

Если в полях «Вопрос Да» и «Вопрос Нет» одновременно ничего не указывается, то считается, что данный вопрос последний, поэтому для такого вопроса должны быть обязательно заполнены оба поля «Результат Да» и «Результат Нет».

Поскольку при занесении нового элемента справочника используются уже имеющиеся элементы справочника, то перед заполнением справочника рекомендуется сперва составить дерево поиска, а заполнение справочника начинать «снизу».

Для проверки получившегося дерева используется отчет «Обход дерева», доступный из меню «Отчеты». Работа отчета будет показана в п. 3.6 «Результаты работы системы».

1.3 Разработка руководства пользователя, аудитора

Аудитор выполняет функции экспертной оценки состояния системы ИБ на предприятии. Для этого он использует правила экспертной оценки, составленные экспертом. Работа производится в 2 этапа:

1) Общая оценка состояния;

2) В случае низкой или средней оценки – оценка угроз.

Для выполнения первого этапа аудитор формирует документ «Экспертный поиск» (рисунок 33). Порядок работы с документом следующий:

- Пользователь выбирает тему «Оценка по ФСТЭК» в поле «Тема»;

- Пользователь нажимает кнопку «Начать», после этого в табличном поле «Текст вопроса» появляется первый вопрос;

- Пользователь отвечает на вопрос, выбирая в поле «Ответ» значения «Да» или «Нет» из выпадающего списка.

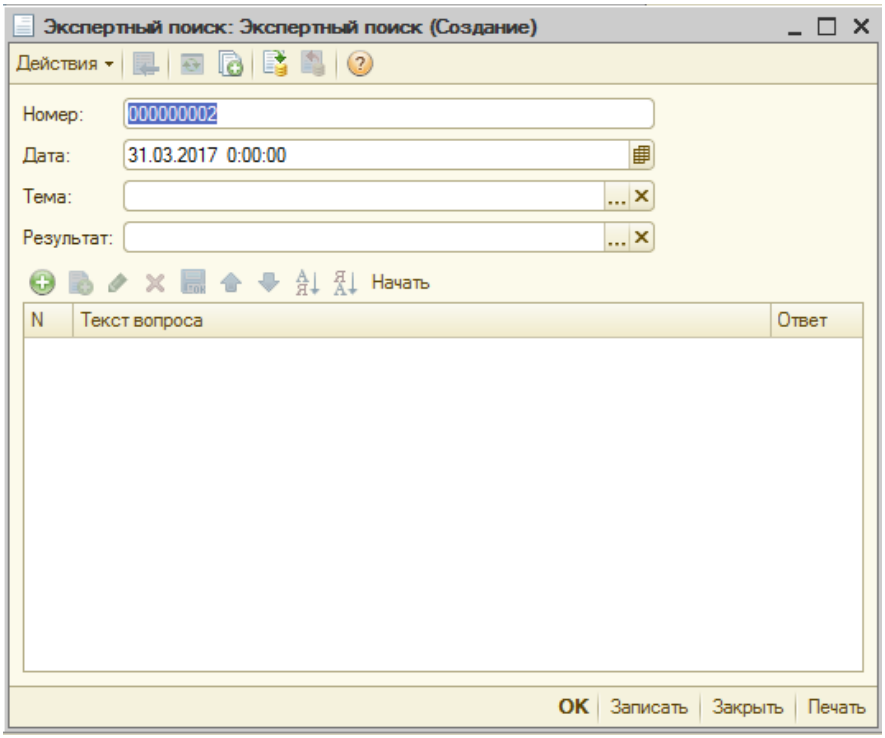


Рисунок 33 – Форма документа «Экспертный поиск»

- После ответа на каждый вопрос в табличном поле «Текст вопроса» появляется новый вопрос. После ответа на последний вопрос результат поиска появляется в поле «Результат».

– После проведения поиска можно распечатать результаты поиска, которые объясняют полученный результат (выполняя функцию объяснения). Результаты поиска будут показаны в п.3.6 «Результаты работы системы».

Продолжение ПРИЛОЖЕНИЯ В

Руководство пользователя

Для выполнения второго этапа пользователю предлагается перейти к оценке угроз. Открывается новый документ, в котором:

– Выбирается тема в поле «Тема» из соответствующего справочника. Для проведения оценки состояния ИБ аудитором выбирается «Оценка по СТР-К»;

– После выбора темы автоматически заполняется табличная часть документа. В табличное поле «Текст вопроса» вносятся все вопросы по данной теме оценки.

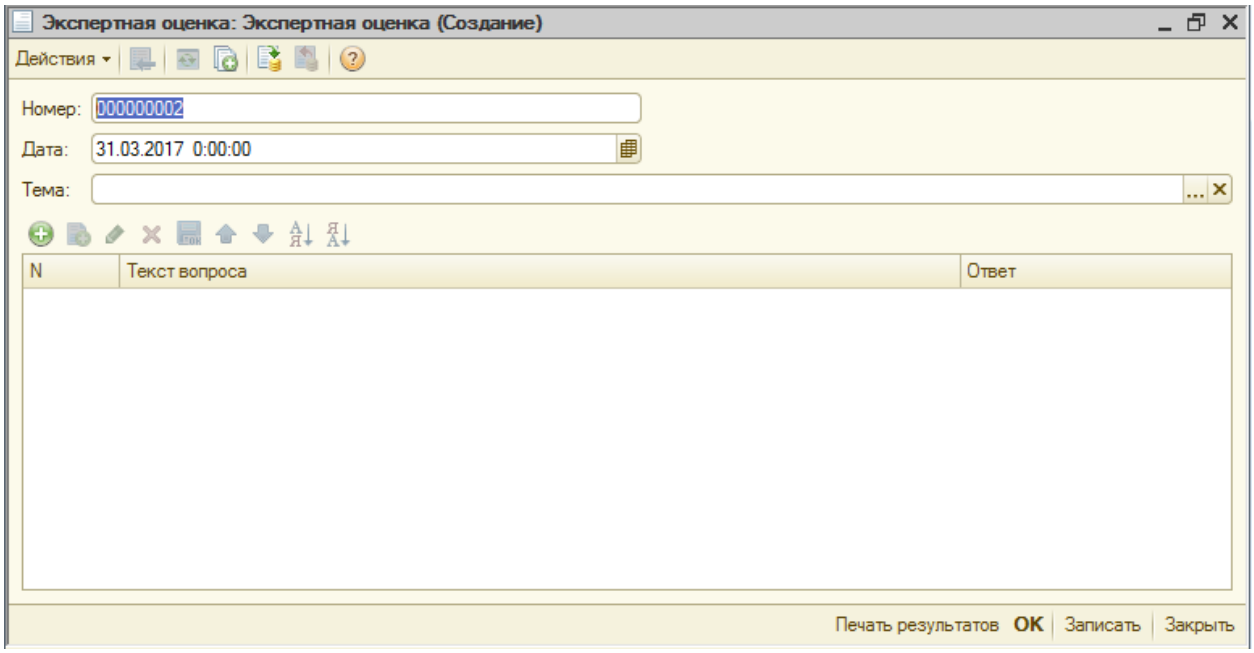


Рисунок 34 – Форма документа «Экспертная оценка»

– Пользователь отвечает на каждый вопрос, выбирая из выпадающего списка в поле «Ответ» значения «Да» или «Нет».

– После ответа на все вопросы пользователь нажимает кнопку «Печать результатов», после чего открывается страница с результатами оценки. Данная страница будет показана в п.3.5 «Результаты работы системы».