На правах рукописи

ТЮРИН
Михаил Вячеславович

МЕТОДЫ ОБЕСПЕЧЕНИЯ ДОСТОВЕРНОСТИ ЭКСПЕРТНОЙ ОЦЕНКИ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ КОМПЛЕКСОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ В УСЛОВИЯХ НЕПОЛНОТЫ РЕТРОСПЕКТИВНОЙ ИНФОРМАЦИИ

05.13.15 – Вычислительные машины, комплексы
и компьютерные сети

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Москва – 2010

Работа выполнена на кафедре вычислительных машин, систем и сетей (каф. 304) Московского авиационного института (государственного технического университета).

Научный руководитель: Заслуженный деятель науки РФ,
доктор технических наук, профессор
БРЕХОВ Олег Михайлович

Официальные оппоненты: доктор физико-математических наук, профессор
МАРКОВ Александр Сергеевич

кандидат технических наук,
старший научный сотрудник
САЛЬМАН Леонид Абрамович

Ведущая организация: Институт Проблем Передачи Информации
им. А. А. Харкевича (ИППИ) РАН

Защита состоится "___" _____2010г. в 14 час. на заседании диссертационного совета Д 212.125.01 при Московском авиационном институте (техническом университете) по адресу: 125993, г.Москва, А-80, ГСП-3, Волоколамское шоссе, д.4.

С диссертацией можно ознакомиться в библиотеке МАИ.

Отзывы на автореферат в двух экземплярах, заверенные печатью, просим направлять по адресу: 125993, г.Москва, А-80, ГСП-3, Волоколамское шоссе, д.4., Ученый совет МАИ.

Автореферат разослан "___" _____ 2010г.

Ученый секретарь
диссертационного совета Д 212.125.01
кандидат технических наук А. В. Корнеенкова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

В настоящее время происходит бурное развитие технологий производства и применения вычислительных систем и компонентов. Это неизбежно приводит к интенсивному совершенствованию программных средств (ПС) вычислительных комплексов и компьютерных сетей (ВККС) и их широкому внедрению во все сферы человеческой деятельности. После введения в действие закона "О персональных данных" [№ 152-ФЗ от 27.07.2006г.] использование программных средств обработки и хранения персональных данных (ПС ПД ВККС) потребовало решения вопросов обеспечения достоверности экспертной оценки *устойчивости функционирования* (УФ) в соответствии с требованиями ФСТЭК и ФСБ России [Положение "Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" № 781 от 17.11.2007 г.].

Существующие методы обеспечения достоверности устойчивости функционирования программных средств вычислительных комплексов и компьютерных сетей обработки и хранения персональных данных [*Липаев В. В.* 1998.] в основе которых лежат элементы, аналогичные объекту исследования (Data Server - ОС Windows 2003 server, СУБД MS SQL server), наиболее часто применяемые для обработки и хранения персональных данных на предприятиях с численностью работников до 1000 человек, позволяют повысить достоверность экспертной оценки устойчивости функционирования ПС ПД ВККС на основе увеличения объемов накапливаемой ретроспективной информации (РИ). Выбор номенклатуры показателей устойчивости функционирования ПС ПД ВККС осуществляется в соответствии требованиям ФСТЭК и ФСБ России согласно ГОСТ 28195-89. В соответствии с этим стандартом, критерий устойчивости функционирования характеризуется набором метрик: $N_{во}$ - способность восстановления при ошибках; $N_{вс}$ - способность восстановления при сбоях оборудования; $N_{св}$ - реализация управления средствами восстановления. Эти метрики определяются набором оценочных элементов: вероятность безотказной работы - $P(t)$; среднее время восстановления после сбоев – $T_в$; функциональность ПО - $f_{ПО}$; показатель устойчивости – $K_у$. Набор значений оценочных элементов в метрике определяется с учетом информации, полученной при проведении различных испытаний, а также по результатам эксплуатации ПС, на основании ретроспективной информации, являющейся функцией показателей оценки ($\overline{w0_i}$) и их базовых значений (KB_i).

Существующие методы обеспечения достоверности устойчивости функционирования ПС ПД ВККС реализованы в различных программных средствах обеспечения достоверности экспертной оценки устойчивости функционирования, таких как сканнеры информационной безопасности: Nessus; Internet Security Scanner; XSpider, в которых используются *статистические методы* за счет постоянно обновляемых баз данных уязвимостей, а также средствах анализа рисков: CRAMM; COBRA; RA Software Tool, в которых используются *вероятностные методы* определения рисков за счет автоматизации

обработки статистики реализации угроз. Все перечисленные методы требуют большего количества *достоверной* ретроспективной информации отражающей состояние устойчивости функционирования ПС ПД ВККС, а также оценки методической погрешности. В случае неполноты ретроспективной информации существующие методы и средства не способны обеспечить необходимую достоверность экспертной оценки *устойчивости функционирования* ПС ПД ВККС в соответствии с требованиями ФСТЭК и ФСБ России.

Поэтому, решение задачи обеспечения достоверности экспертной оценки устойчивости функционирования ПС ПД ВККС на основе использования методов и средств работы с *неполными* сведениями является **актуальным** для современного этапа развития систем подобного назначения [Корченко А. Г. 2006].

Диссертация опирается на результаты работ ведущих российских и зарубежных ученых: Липаева В. В., Костогрызова А. И., Майерса Дж., Заде Л. А, Павлова В. В, Корченко А. Г., Леоненкова А. В, Бунича А. Л., Бахтадзе Н. Н., Дэвид Ф. Марка, Клемент МакГоуэна, Барри Боэма и других.

Научная задача диссертационного исследования состоит в обеспечении достоверности экспертизы устойчивости функционирования ПС ПД ВККС в условиях неполноты ретроспективной информации, на ранних стадиях жизненного цикла.

Цель диссертации состоит в разработке методов и рекомендаций по обеспечению достоверности экспертизы устойчивости функционирования программных средств вычислительных комплексов и компьютерных сетей обработки и хранения персональных данных (ПС ПД ВККС), в условиях неполноты ретроспективной информации на ранних стадиях жизненного цикла.

Задачи исследования.

1. Анализ существующих методов и средств обеспечения достоверности экспертизы устойчивости функционирования ПС ПД ВККС.
2. Разработка метода согласования экспертных оценок устойчивости функционирования ПС ПД ВККС на основе принципов нечеткой логики, позволяющего учитывать особенности применяемых методов экспертизы при анализе УФ на ранних стадиях жизненного цикла.
3. Разработка метода сокращения издержек экспертизы УФ на ранних стадиях жизненного цикла ПС ПД ВККС.
4. Разработка рекомендаций по автоматизации метода согласования экспертных оценок УФ в условиях неполноты ретроспективной информации о влиянии деструктивных воздействий, с учетом особенностей применяемых методов экспертизы на ранних стадиях ЖЦ, на основе программного средства.

Методы исследования. При выполнении работы использовался математический аппарат теории надежности, общей теории погрешностей, теории нечетких множеств, теории принятия решений, а также принципы и алгоритмы нечеткого вывода.

На защиту выносятся.

- Метод согласования экспертных оценок устойчивости функционирования ПС ПД ВККС на основе методов и средств нечеткой логики.

- Метод оптимизации стратегий экспертной оценки УФ на ранних стадиях жизненного цикла ПС ПД ВККС в условиях неполноты ретроспективной информации об устойчивости функционирования ПС ПД ВККС, на основе сокращения издержек в исходном описании объекта и угроз.
- Рекомендации по автоматизации метода согласования экспертных оценок устойчивости функционирования ПС ПД ВККС в условиях неполноты ретроспективной информации на основе системы нечеткого моделирования.

Научная новизна. Научная новизна и теоретическая значимость диссертационной работы состоит в следующем:

1. Разработан *метод* согласования экспертных оценок устойчивости функционирования ПС ПД ВККС в условиях неполноты ретроспективной информации на основе принципов нечеткой логики, определяющий взаимосвязь угроз информационной безопасности с учетом степени их взаимного влияния;
2. Разработан метод оптимизации выбранных стратегий экспертизы УФ на ранних стадиях жизненного цикла в условиях неполноты ретроспективной информации. В основе этого метода лежит процесс нахождения предельного функционала средних издержек, значения которого выражают в виде поправок к результатам экспертных оценок устойчивости функционирования ПС ПД ВККС.
3. Разработаны рекомендации по автоматизации метода согласования экспертных оценок устойчивости функционирования в условиях неполноты ретроспективной информации на ранних стадиях жизненного цикла, на основе среды программирования MATLAB, способные сократить время принятия решения экспертами об устойчивости функционирования ПС ПД ВККС в условиях неполноты ретроспективной информации, на ранних стадиях жизненного цикла.

Практическая значимость работы заключается:

- В повышении достоверности экспертизы устойчивости функционирования ПС ПД ВККС с 68 % - до 90 % в условиях неполноты ретроспективной информации за счет применения разработанного метода *согласования экспертных оценок* устойчивости функционирования на основе принципов нечеткой логики.
- В снижении издержек организации процессов и работ по обеспечению достоверности экспертизы устойчивости функционирования ПС ПД ВККС на ранних стадиях жизненного цикла почти на 30 %, в сравнении с применением вероятностной модели и почти на 40 %, в сравнении с применением статистической модели оценки устойчивости функционирования, за счет оптимизации стратегий управления экспертизой.
- В повышении производительности работ по проведению экспертизы устойчивости функционирования ПС ПД ВККС за счет автоматизации метода согласования экспертных оценок на основе внедрения программного средства, созданного в среде нечеткого моделирования MATLAB, способного сократить время проведения экспертизы устойчивости функционирования ПС ПД ВККС почти на 50 %, и тем самым уменьшив затраты по административному управлению вдвое.

Реализация и внедрение. Методы и рекомендации по обеспечению достоверности экспертной оценки устойчивости функционирования программных средств вычислительных комплексов и компьютерных сетей обработки и хранения

персональных данных (ПС ПД ВККС) реализованы и внедрены на предприятии ЗАО "Управляющая Холдинговая компания "Королевский трубный завод". Внедрение производилось на базе финансовой ПС ПД ВККС предприятия, под целевую задачу модернизации с помощью программных комплексов MATLAB и BPWin 4.1.

Достоверность полученных результатов подтверждается сравнением итогов анализа устойчивости функционирования финансовой ПС ПД ВККС предприятия ЗАО "Управляющая Холдинговая компания "Королевский трубный завод" полученных в результате применения разработанных методов и рекомендаций, и результатов аудита, ранее проведенного сторонней организацией, что зафиксировано в Протоколах проверки и Акте приемки-сдачи работ.

Апробация работы. Основные результаты диссертационной работы обсуждались на кафедральной научно-технической конференции "Разработка методов анализа устойчивости функционирования вычислительных комплексов и компьютерных сетей на основе применения CALS – технологий" (Москва, МАИ, 5 июня 2006 г.).

Публикации. По основным результатам исследований опубликовано 7 печатных работ, 3 из которых - в реферируемых изданиях, рекомендованных ВАК.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения и четырех приложений. Общий объем работы составляет 142 страниц, в том числе приложения представлены на 28 страницах. Работа содержит 37 рисунков и 36 таблиц. Список литературы включает 62 наименования.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность решаемой в диссертации научно-технической проблемы, сформулированы цель и задачи исследования, научная новизна и практическая ценность проведенных исследований.

В первой главе рассматривается вычислительный комплекс обработки и хранения персональных данных предприятия с численностью сотрудников до 1000 человек, формулируется понятие устойчивости функционирования ПС ПД ВККС, задачи и цели экспертизы устойчивости функционирования объекта исследования Data Server (ОС Windows 2003 server, СУБД MS SQL server), как основного элемента обработки и хранения персональных данных, имеющего заданную номенклатуру метрик и значения оценочных элементов критерия устойчивости функционирования [ГОСТ 28195-89]: вероятность безотказной работы - $P(t)$; среднее время восстановления после сбоев – $T_в$; функциональность ПО - $f_{ПО}$; показатель устойчивости – $K_у$, при работе с заданными характеристиками производительности и функциональными параметрами: Δ - время реакции; γ - пропускная способность; J_c – средний показатель использования; $K_{эф}$- коэффициент сохранения эффективности ПС ПД ВККС). Для оценки критерия устойчивости функционирования (H) ПС ПД ВККС в *широком смысле* определяемого: способностью восстановления при ошибках; способностью восстановления при сбоях оборудования; реализацией управления средствами восстановления, а также характеристиками информационной безопасности: конфиденциальности, целостности, доступности принимается единая шкала оценки критерия "устойчивость функционирования" ПС ПД ВККС - *от 0 до 1* (***0*** **-** максимально

необходимая, оптимальная, устойчивость функционирования – точка "горизонта"; ***1*** - полный крах системы) [ГОСТ 28195-89]. В главе рассматривается *взаимосвязь* фактора "устойчивость функционирования" ПС ПД ВККС, его метрик и оценочных элементов со стадиями жизненного цикла ПС для пяти основных стадий [ГОСТ Р ИСО/МЭК 12207-99]: 1) стадия заказа ПС ПД ВККС – (T_1); 2) стадия поставки ПС ПД ВККС – (T_2); 3) стадия разработки (установка в составе системы) ПС ПД ВККС – (T_3); 4) стадия эксплуатации ПС ПД ВККС – (T_4); 5) стадия сопровождения ПС ПД ВККС – (T_5).

Выполнено исследование существующих, наиболее часто используемых методов обеспечения достоверности экспертизы устойчивости функционирования ПС ПД ВККС, реализованных в следующих ПС: сканнеры безопасности Nessus Vulnerability Scanner (Tenable Network Security); Internet Security Systems' Internet Scanner (IBM); XSpider (Positive Technologies), а также средства анализа рисков CRAMM, COBRA, RA Software Tool. На основании экспериментальных исследований определены значения методической погрешности $\delta_{мп}$ - характеризующей способность ПС обеспечения достоверности экспертизы постепенно снижать эффективность экспертизы УФ при увеличении числа последовательно выполняемых операций. На основании определения методической погрешности $\delta_{мп}$ получены сравнительные характеристики достоверности анализа устойчивости функционирования ПС ПД ВККС на разных стадиях жизненного цикла (табл. 1).

		Средства анализа уязвимостей			Средства анализа рисков		
Достоверность экспертизы		Nessus	ISS	XSpider	CRAMM	COBRA	RA Software
Стадия ЖЦ.	T1	Сканирование не возможно			52 %	50 %	50 %
	T2	Сканирование не возможно			78 %	78 %	76 %
	T3	81 %	81 %	81 %	80 %	81 %	80 %
	T4	82 %	83 %	82%	80 %	87%	80 %
	T5	83 %	85 %	84 %	84 %	87 %	85 %

Таблица 1 – Таблица сравнительных характеристик обеспечения достоверности экспертизы при использовании ПС анализа устойчивости функционирования.

Из анализа статистических методов обеспечения достоверности экспертизы устойчивости функционирования ПС ПД ВККС, реализованных в наиболее часто применяемых сканерах безопасности, и вероятностных методов реализованных в наиболее часто применяемых программных средств анализа рисков, сделан вывод, что они имеют низкую эффективность на ранних стадиях жизненного цикла ввиду того, что необходимо большое количество достоверной ретроспективной информации отражающей особенности реализации информационной безопасности ПС ПД ВККС. Указанное обстоятельство требует разработки новых методов и рекомендаций по обеспечению достоверности экспертизы устойчивости функционирования ПС ПД ВККС на ранних стадиях жизненного цикла.

В первой главе, также выполнена математическая постановка задачи обеспечения достоверности экспертизы устойчивости функционирования ПС ПД ВККС. При рассмотрении задач обеспечения достоверности экспертизы устойчивости функционирования ПС ПД ВККС в условиях неполноты ретроспективной информации необходимо выделить проблемы, решение которых должно привести к требуемому уровню обеспечения достоверности экспертизы:

наличие неопределенности в результатах экспертизы УФ полученных статистическими или вероятностными методами; зависимость результатов экспертизы устойчивости функционирования ПС ПД ВККС от случайных и трудно прогнозируемых факторов, стратегий эксперта и его точки зрения; для каждой стадии ЖЦ требуется подготовка отдельного набора метрик оценки рисков информационной безопасности ПС ПД ВККС. Для решения вышеуказанных проблем в работе предлагается ввести следующие множества:

$ИД_{ij}$ $(i=\overline{1,n};\ j=\overline{1,m})$ - лингвистическое множество исходных данных для оценки устойчивости функционирования;

$КВ_{ij}$ $(i=\overline{1,n};\ j=\overline{1,m})$ – множество базовых экспертных оценок устойчивости функционирования ПС ПД ВККС;

$M = \{m_1 ... m_j\}$ – множество экспертов в составе группы;

$N = \{n_1 ... n_i\}$- множество метрик, описывающих основные показатели устойчивого функционирования ПС сервера обработки и хранения персональных данных Data Server ($P(t)$; Tcp_i; $T_в$; $f_{ПО}$; $K_у$);

$R_{ИБ} = \{R_{ИБ_1} \ldots R_{ИБ_n}\}$ - множество рисков (критичности угроз);

$T_{ЖЦ} = \{T_1; T_2; T_3; T_4; T_5\}$ – множество интервалов времени (стадий ЖЦ);

$U = \{u_1 ... u_n\}$ – множество стратегий оценки устойчивости функционирования;

$X_i = [x_1, \ldots, x_n]$ – множество угроз.

Тогда постановка задачи обеспечения достоверности экспертизы устойчивости функционирования ПС ПД ВККС в общем случае может быть представлена в следующем виде: необходимо найти достоверность экспертизы $J_\infty[U_0^\infty(*)]$, как множество поправок – $\Delta J_\infty[U_0^\infty(*)] = \{\Delta J_T[U_1^T(*)], \Delta J_T[U_2^T(*)], \ldots, \Delta J_T[U_n^T(*)]\}$ к оценкам основных параметров устойчивости функционирования ПС ПД ВККС; необходимо найти показатели эффективности, как функцию от времени накопления ретроспективной информации и стратегии управления экспертизой: $S(t)=f(\Delta J[U];\ T_N$.

<u>Во второй главе</u> разрабатывается метод согласования экспертных оценок устойчивости функционирования ПС ПД ВККС, реализующий возможность оценки взаимного влияния угроз информационной безопасности для объекта исследования (Data Server - ОС Windows 2003 server, СУБД MS SQL server) и учитывающий разброс экспертных оценок полученных статистическими или вероятностными методами в условиях неполноты ретроспективной информации, характерных для ранних стадий ЖЦ.

Разрабатываемый метод согласования экспертных оценок устойчивости функционирования ПС ПД ВККС предлагается основывать на принципах нечеткой логики, так как набор стандартных вероятностных понятий и методов оказывается неадекватным для описания ситуаций, связанных с отсутствием эргодичности процессов, их существенной нестационарностью, трудностью получения необходимой статистики, и т. д. В работе предлагается выбрать 6 угроз, наиболее характерных для сервера обработки и хранения персональных данных Data Server, согласно Бюллетеней по безопасности Microsoft MS07-017, MS08-040, MS09-004 (*актуальным на день проведения исследований*). Исходя из набора метрик критерия

устойчивости функционирования, которые описываются оценочными элементами: вероятность безотказной работы- *P(t)*; среднее время восстановления после сбоев– $T_в$; функциональность ПО- $f_{ПО}$; показатель устойчивости–$K_у$, формируется лингвистическое множество исходных данных - $ИД_{ij}$ ($i=\overline{1,n}$; $j=\overline{1,m}$), служащее компонентом вектора запроса. Шкалой для формирования экспертных оценок, в работе предлагается использовать таблицу (табл. 2) определения значимости угрозы, полученную на основе разработок National Institute for Standards and Technology (NIST) [NIST SP 800-26].

Таблица 2 – Таблица определения значимости угрозы.

Цена потери (степень серьезности угрозы)	Уровень угрозы								
	Низкий			Средний			Высокий		
	Н	С	В	Н	С	В	Н	С	В
Низкая	0	0.1	0.2	0.1	0.2	0.3	0.2	0.3	0.4
Ниже средней	0.1	0.2	0.3	0.2	0.3	0.4	0.3	0.4	0.5
Средняя	0.2	0.3	0.4	0.3	0.4	0.5	0.4	0.5	0.6
Выше средней	0.3	0.4	0.5	0.4	0.5	0.6	0.5	0.6	0.7
Высокая	0.4	0.5	0.6	0.5	0.6	0.7	0.6	0.7	0.8

Экспертами выполняется ранжирование угроз по степени их влияния на значения основных оценочных элементов (*P(t); $T_в$; $f_{ПО}$; $K_у$*) определяющих критерий "устойчивость функционирования" ПС ПД ВККС, через определение коэффициентов важности $KB_j=[KB_1,\ldots,KB_m]$ (где *n* — количество угроз; *m* – количество экспертов). На основании результатов ранжирования коэффициентов важности метрик KB_j на множестве исходных данных X_i определяется *функция принадлежности (ФП)* $\mu_{\underset{\sim}{KB}}(x_i)$ (табл. 3). Для определения базовой (эталонной) функции принадлежности (ФП) нечеткого множества коэффициентов важности в диссертационной работе выполняется анализ различных методов её построения (метод опроса (МО); числовой метод (ЧМ); метод лингвистических термов (МЛТ); и др.) [Заде Л.А.,1976].

В работе предлагается использовать метод построения *экспоненциальной* ФП (Гаусса – gaussmf, в интерпретации MATLAB), как наиболее удобной для решения задач представления *нормально* распределенных случайных величин, таких как угрозы информационной безопасности.

$$\mu_{\underset{\sim}{KB}}(x_i)=e^{-\alpha(KB_j-x_i)^2} \quad (1),$$

где

$$\alpha=-4\ln(0,5)/\beta^2 \quad (2),$$

Значения *"α"* и *"β"– границ толерантности* НЧ предлагается определить из экспериментальных исследований применяемого метода экспертизы (статистического или вероятностного), на основе результатов решения задач отыскания экспоненциальной функции принадлежности НЧ, приблизительно

Таблица 3 - Коэффициенты важности угроз.

		Коэффициент Важности (KB_j)													
		Статистические методы							Вероятностные методы						
		KB_1	KB_2	KB_3	KB_4	KB_5	KB_6	$\mu(x)$	KB_1	KB_2	KB_3	KB_4	KB_5	KB_6	$\mu(x)$
Угрозы X_i	x_1 Уязвимость GDI, приводящая к несанкционированному получению локальных прав, (CVE-2006-5758)	0.6	0.5	0.6	0.5	0.5	0.6	**0.50**	0.7	0.6	0.6	0.5	0.5	0.6	**0.58**
	x_2 Уязвимость WMF, приводящая к отказу в обслуживании, (CVE-2007-1211)	0.5	0.4	0.4	0.5	0.4	0.5	**0.41**	0.5	0.4	0.4	0.6	0.5	0.5	**0.48**
	x_3 Уязвимость EMF, приводящая к несанкционированному получению прав, (CVE-2007-1212)	0.1	0.4	0.5	0.2	0.3	0.3	**0.26**	0	0.4	0.6	0.2	0.3	0.3	**0.3**
	x_4 Уязвимость, связанная с обработкой GDI недопустимых размеров окна и приводящая к несанкционированному получению прав, (CVE-2006-5586)	0.3	0.1	0.2	0.1	0.4	0.3	**0.22**	0.3	0.2	0.2	0.1	0.5	0.3	**0.26**
	x_5 Уязвимость анимированного курсора Windows, приводящая к удаленному выполнению кода, (CVE-2007-0038)	0.2	0.2	0.1	0.2	0.2	0.1	**0.17**	0.3	0.2	0	0.2	0.3	0.2	**0.2**
	x_6 Уязвимость, связанная с обработкой GDI недопустимых параметров (CVE-2007-1215)	0.1	0.2	0.2	0.1	0	0.2	**0.14**	0.2	0.2	0.3	0.1	0	0.2	**0.16**

равной некоторому четкому числу $КВ_j$.

В работе предлагается, множество, образуемое одной или несколькими зависимыми *метриками* устойчивости функционирования ПС ПД ВККС воспринимать, как нечеткое полихроматическое множество (*ПS*), где понятие *цвет* рассматривать как согласование понятий: *свойство, атрибут, характеристика*:

$ПS_X = (X, F(x), F(X), [X \times F(x)], [X \times F(X)], [X \times X(F)])$ (4), где $[X \times F(x)]$ - булева матрица персональных цветов каждой угрозы $x_i \in X$, *или множество "чистых" свойств каждой угрозы*; $[X \times F(X)]$ - булева матрица персональных цветов элемента, одноименных унитарным цветам в *F(X), или множество совпадающих свойств каждой угрозы;*

$[X \times X(F)]$ - булева матрица *тел*, или множество элементарных свойств *каждой угрозы*, порождаемое свойствами других, более простых, составляющих.

В работе предлагается, во избежание некорректности нечетких моделей учитывать влияние *множества самостоятельных свойств* элементов (персональных цветов) на множество свойств элементов в составе группы (*унитарных* цветов самого ПS), которые в сою очередь могут быть *доминирующими (при позитивном воздействии* - расширяющими множество совместных свойств ПS-множества*), доминируемыми (при негативном воздействии* - сужающими множество совместных свойств ПS-множества*) или нейтральными.*

Составы элементов $X_i(F_j) \subseteq X$, представляются булевой матрицей $\left\| c_{i(j)} \right\| = [F(x) \times X(F)]$ (5), где *X(F)* есть объединение всех вариантов тел унитарных цветов *F(X)*. Мнемонически полученная конструкция будет выглядеть в виде (табл. 4):

Таблица 4 - Мнемоническое представление булевой матрицы (5).

		Тела унитарных цветов					
		$X_1(F)$	$X_2(F)$	$X_3(F)$	$X_4(F)$	$X_5(F)$	$X_6(F)$
Персональные цвета	$F(x_1)$	+-	-	-	+	+	-
	$F(x_2)$	+	+-	-	+	+	+-
	$F(x_3)$	+	+	+-	+	+	+
	$F(x_4)$	-	-	-	+-	+	-
	$F(x_5)$	-	-	-	-	+-	-
	$F(x_6)$	+	+-	-	+	+	+-

где + - позитивное воздействие элемента; - - негативное воздействие элемента; +- - нейтральное воздействие элемента.

В работе предлагается считать степенью взаимного влияния между соседними элементами в ПS – множестве, *расстояние Хемминга* (6), а также выразить его относительное значение (7) [Павлов В. В.,2006].

$$d_h(F(x_{i-1}),\ F(x_i)) = \sum_{i=1}^{m^*} \left| \mu_{x_{i-1}}(F_j) - \mu_{x_i}(F_j) \right| \quad (6)$$

$$d_{h(0)}(F(x_{i-1}),\ F(x_i)) = d_h(F(x_{i-1}),\ F(x_i)) \cdot m^{-1} \quad (7), \text{ где } 0 \le d_{h(0)} \le 1.$$

где m^* – число цветов (реакций экспертов на каждую из *n* угроз)

Очевидно: чем больше *относительное* расстояние Хемминга, тем меньше

рассматриваемое свойство метрики влияет на свойство родственной по смыслу метрики, в рассматриваемом универсуме ПU (множестве оценочных элементов $P(t)$; $T_в$; $f_{ПО}$; $K_у$). На основании (5) и её мнемонического представления (табл. 4) получаем числовые значения относительных расстояний Хемминга (табл. 5):

Основу нечеткого логического вывода множества оценок устойчивости функционирования ПС ПД ВККС составляет композиционное *правило Заде* [Заде Л.А., 1966], формулируемое для решаемой задачи следующим образом: если известно нечеткое отношение $\tilde{F}$ между нечетким множеством экспертных оценок ($w0$) УФ (входной переменной) и множеством значений нечеткого вывода $\overline{w0}$ (выходной переменной), то при нечетком значении входной переменной $x = \tilde{A}$, нечеткое значения выходной переменной определяется так: $\overline{w0} = \tilde{A} \circ \tilde{F}$, где $\circ$ - максминная композиция, или *функция максимизации минимума возможных решений*.

Таблица 5 - Значения относительных расстояний Хемминга.

$d_{h(o)}$	Персональные цвета $F(x_i)$					
Персональные цвета $F(x_j)$	$F(x_1)$	$F(x_2)$	$F(x_3)$	$F(x_4)$	$F(x_5)$	$F(x_6)$
$F(x_1)$	0	0.67	0.5	0.5	0.5	0.67
$F(x_2)$	0.67	0	0.83	0.5	0.5	0.33
$F(x_3)$	0.5	0.83	0	0.67	0.67	0.5
$F(x_4)$	0.5	0.5	0.67	0	0.33	0.83
$F(x_5)$	0.5	0.5	0.67	0.33	0	0.5
$F(x_6)$	0.67	0.33	0.5	0.83	0.5	0

На основании анализа результатов экспериментальных исследований проведенных в среде MATLAB, различных методов нечеткого вывода - *Мамдани* (Mamdani), Цукамото, Ларсена, Сугено показавших, что разница получаемых четких значений не превышает 15%, а также, в виду того, что алгоритм *Мамдани* по сравнению с другими методами нечеткого вывода обладает экономичностью алгоритмической реализации почти на 20%, а также наилучшим образом применим для нечетких множеств соответствующих термам заключений, относящихся к одним и тем же выходным лингвистическим переменным [Леоненков А. В., 2003], **в работе предлагается** использовать **для получения результатов *экспликации*** экспертных оценок метрик устойчивости функционирования объекта исследования (Data Server) именно алгоритм *Мамдани*.

На основании приведения к четкости, *четкое* значение w_0 (*четкая* функция нечетких оценок метрик устойчивости функционирования объекта исследования (Data Server):

$w_0 = \mu_\Sigma F(P(t);\ T_в;\ f_{ПО};K_у)$ переменной x_i определяется по формуле (8):

$$w_{0_i} = \frac{\int_\Omega w_i \cdot \mu_\Sigma(w)dw}{\int_\Omega \mu_\Sigma(w)dw}$$ (8), где Ω – область определения функции $\mu_\Sigma(w)$ - [0;1]

В работе предлагается, с целью учета влияния свойств каждого оценочного элемента на свойства нечеткого множества оценок, отобразить относительное расстояние Хемминга на множестве выходных переменных:

$d^{+1}_{h(0)}$ - относительное расстояние Хемминга (6) при *позитивном* воздействии свойств; $d^{-1}_{h(0)}$ - при *негативном* воздействии свойств; $d^{0}_{h(0)}$ - при *нейтральном*

воздействии свойств;

Тогда *четкое* значение $\overline{w0}_i$ оценок метрик устойчивости функционирования ($P(t)$; $T_в$; $f_{ПО}$; $K_у$) объекта исследования (Data Server) с учетом *влияния цветности* будет представлено формулой вида:

$$\overline{w0}_i = \sum_{i=1}^{m} (d_{h(0)_i}^{\pm 1} \cdot w_{0_i}) \Big/ m \quad (9),$$ где m – количество экспертов.

Для наглядного сравнения результатов экспертной оценки до и после согласования предлагается составить сводную таблицу (табл. 6). Так, например, из анализа полученной таблицы можно сделать вывод о том, что меньше всего экспертами изучена уязвимость, связанная с обработкой GDI недопустимых параметров (CVE-2007-1215). Это обстоятельство обусловлено тем, что реализация этой угрозы имеет наименьший риск и поэтому её изучению эксперты уделяли минимум внимания.

Таблица 6 - Таблица сравнения результатов экспертизы.

Угроза	*Экспертная оценка (KB_i)*		$\overline{w0}_i$
	Статистич.	Вероятностн.	
Уязвимость GDI, приводящая к несанкционированному получению локальных прав, (CVE-2006-5758)	0.50	0.58	$0.55 \pm 10\%$
Уязвимость WMF, приводящая к отказу в обслуживании, (CVE-2007-1211)	0.41	0.48	$0.31 \pm 10\%$
Уязвимость EMF, приводящая к несанкционированному получению прав, (CVE-2007-1212)	0.26	0.3	$0.14 \pm 10\%$
Уязвимость, связанная с обработкой GDI недопустимых размеров окна и приводящая к несанкционированному получению прав, (CVE-2006-5586)	0.22	0.26	$0.41 \pm 10\%$
Уязвимость анимированного курсора Windows, приводящая к удаленному выполнению кода, (CVE-2007-0038)	0.17	0.2	$0.33 \pm 15\%$
Уязвимость, связанная с обработкой GDI недопустимых параметров, (CVE-2007-1215)	0.14	0.16	$0.17 \pm 25\%$
Средняя оценка нечеткости экспертизы всех угроз			0.35
Средняя оценка устойчивости функционирования ПС ПД ТСКС			0.68

В работе предлагается, для представления уровня неопределенности экспертных оценок устойчивости функционирования объекта исследования (Data Server) на каждой стадии жизненного цикла, ввести понятие "*степени неполноты ретроспективной информации*" на основе определения значения *нечеткой мощности нечеткого множества* [Заде Л.А., 1966]:

$$|P|_f = \frac{\sum \alpha_{(1)}^{*(m)} \Big/ \left|P_{\alpha^*}\right|}{m} \quad (10),$$ где $\alpha_{(1)}^{*(m)} = \sup\{\alpha^* \left|P_{\alpha^*}\right| \Big/ m\}$ – значения индекса сравнения $\left|P_{\alpha^*}\right|$, подсчитанного на α^* - срезах множества коэффициентов важности KB_iв периоды времени $T = \{T_1; T_2; T_3; T_4; T_5\}$. Так, например, на стадии T_5 нечеткая мощность нечеткого множества для угрозы CVE-2007-1215 составила $|P|_{T_1} = 25\%$, а для наиболее критичной угрозы CVE-2006-5758 - $|P|_{T_5} = 10\ \%$.

Полученные значения уровня неопределенности дают возможность оценить темпы роста достоверности экспертизы от стадии к стадии.

<u>В третьей главе</u>: **Разрабатывается** метод оптимизации стратегии экспертной оценки УФ за счет уменьшения издержек в исходном описании объекта и угроз на ранних стадиях жизненного цикла ПС ПД ВККС в условиях неполноты ретроспективной информации.

Для оценки оптимальности стратегии экспертной оценки устойчивости функционирования существуют *вероятностные, статистические*, а также простые *интуитивные* модели оценки достоверности УФ [*Майерс Г.*2003.].

Разработку вероятностных моделей обеспечения достоверности УФ начинают с уточнения поведения функции риска *R(t)=f(N(t))*, которая характеризуется условной вероятностью того, что ошибка экспертизы проявится в интервале от t

до $t+\Delta t$. Недостатками вероятностных моделей являются необходимость допущений: все ошибки экспертизы одинаково серьезны; ошибки экспертизы исправляются немедленно после обнаружения; каждая обнаруженная ошибка уменьшает значение скорости обнаружения и устранения ошибок.

Особенностью *статистических* моделей роста достоверности УФ является необходимость принудительного "засорения" результатов экспертизы устойчивости функционирования ПС ПД ВККС некоторым количеством известных ошибок, что для рассматриваемой ПС ПД ВККС не реализуемо. Для реализации простых *интуитивных* моделей обеспечения достоверности УФ необходимо создание тестовой ПС ПД ВККС, полностью аналогичной рассматриваемой, с заранее известными характеристиками УФ, что также нереализуемо.

В работе предлагается, для решения указанных проблем, когда стратегия обеспечения экспертизы достоверности УФ только путем создания *избыточности ретроспективной информации* неэффективна, а во многих случаях *нереализуема*, реализовать модель обеспечения достоверности экспертизы устойчивости функционирования ПС ПД ВККС в соответствии с принципом нормализации стратегии.

Для этого предлагается рассмотреть структурную схему (рис.2) модели обеспечения достоверности экспертизы устойчивости функционирования ПС ПД ВККС на ранних стадиях жизненного цикла, в условиях неполноты априорной информации [Бунич А. Л., Бахтадзе Н. Н., 2003].

Краткое описание модели: *Y(t)* – показания "датчика" состояния объекта являются реакцией этого "датчика" на метрику *X(t)*; *U(t)* – стратегия управления; w0(t) – предварительная оценка метрики УФ. Эксперты получают ретроспективную информацию, соответствующую оценкам выбранных метрик, об устойчивости функционирования ПС ПД ВККС ("*Объект*" (рис. 2) - Data Server (ОС Windows 2003 server, СУБД MS SQL server)) Ретроспективная информация обрабатывается статистическими и нестатистическими (вероятностными) методами (п. 1.3.), как функция конечного состояния системы:

Степень серьезности угрозы (цена потерь)	Уровень угрозы								
	Низкий			Средний			Высокий		
	Н	С	В	Н	С	В	Н	С	В
Низкая	0	0.1	0.2	0.1	0.2	0.3	0.2	0.3	0.4
Ниже средней	0.1	0.2	0.3	0.2	0.3	0.4	0.3	0.4	0.5
Средняя	0.2	0.3	0.4	0.3	0.4	0.5	0.4	0.5	0.6
Выше средней	0.3	0.4	0.5	0.4	0.5	0.6	0.5	0.6	0.7
Высокая	0.4	0.5	0.6	0.5	0.6	0.7	0.6	0.7	0.8

Рисунок 2 - Структурная схема модели обеспечения достоверности экспертизы устойчивости функционирования ПС ПД ВККС

$$W(p) = W(j\omega)e^{-\tau p} \quad (11);$$

где $p(t)$ – функция комплексной переменной, определяемая преобразованием Лапласа $x(p) = \int_0^\infty x(t)\,e^{-pt}dt$ из функции времени *x(t)*; τ - постоянная времени запаздывания, характеристика равная времени принятия решения экспертами; считаем, что $\tau \le 0.001T_{CT}$ (12);

К - имеет смысл коэффициента *восприимчивости* (*инициативности*) экспертной группы, и зависит от интеллектуальных способностей экспертной группы.

В качестве идентификатора ("*Идентификатор*" (рис.2)) выступает таблица 2 – Таблица определения значимости угрозы в зависимости от трех уровней угрозы.

Предельно достижимая скорость сходимости экспертных оценок метрик и их оценочных элементов [ГОСТ 28195-89] устойчивости функционирования ограничена условиями неполноты ретроспективной информации.

В диссертационной работе предлагается, выразить уравнением (13) стратегию реализации рандомизированных обратных связей модели управления достоверностью экспертизы устойчивости функционирования ПС ПД ВККС, с учетом ограничений на глубину памяти *m*:

$$y_t = U_t(y_{t-m}^{t-1}, r^t, w0_{t-m}^t, \theta_{t-1}) + r_t, \quad \theta_t = F_t(\theta_{t-1}, y_{t-m}^{t-1}, w0_{t-m}^t) \quad (13),$$

где θ_t - оптимизированное значение изменения одного из наблюдаемых параметров устойчивости функционирования объекта исследования Data Server (любого значений *P(t); Тв*; $f_{ПО}$; K_y); $\overline{w0_0^t} = (\overline{w0_0}, \ldots, \overline{w0_t})$ - множество известных значений оценки (2.18), приведенных к четким значениям при поступлении рандомизирующих тестовых воздействий (например, результатов активных системных опросов сканнера безопасности Nessus) $r^t = \{r_0, \ldots, r_t\}$ в моменты времени [*0;t*] – (такты управления).

Достоверность экспертизы устойчивости функционирования ПС ПД ВККС будет определятся предельным функционалом средних издержек:

$$J_\infty^{-1}[U_0^\infty(*)] = \sigma\left|P\right|_f \cdot \liminf_{T\to\infty} \Gamma^{-1}(\sum_{t=1}^{T} EQ_t(X_t, y_{t-1}\theta^*) \quad (14),$$

где $U_0^\infty(*)$ - стратегия экспертизы (например, тестирование с увеличением количества SQL запросов и д.р.);

E – математическое ожидание применения стратегии $U_0^\infty(*) = \overline{w0_i}(p) \cdot W_i(p)$, формируемой на такте времени *t,* порожденной обратными связями $y_t = U_t(u^{t-1}, Z^t, r_0^t, \tau(\theta^*))$; $Q_t(X_t, y_{t-1}\theta^*) \geq 0$ - заданная функция потерь (принятые риски); *Г*- горизонт управления: $0 \leq \Gamma(\overline{w0_i}) \leq 1$; $\sigma\left|P\right|_f$ - среднеквадратичное отклонение нечеткой мощности нечеткого множества.

Численно, издержки экспертизы удобно представить в виде *поправки* функционала средних издержек:

$$\Delta J_\infty[U_0^\infty(*)] = \{\Delta J_T[U_1^T(*)], \Delta J_T[U_2^T(*)], \ldots, \Delta J_T[U_n^T(*)]\} = \frac{J_T[U_0^T(*)]}{J_\infty[U_0^\infty(*)]} \cdot 100\% \quad (15),$$ где

поправки (допуски) к оценкам параметров устойчивости функционирования *P(t); Тв*; $f_{ПО}$; K_y при сохранении исходных значений Δ; γ; J_c, находится как отношение текущего значения достоверности экспертизы, $J_T[U_0^T(*)]$ к её среднему значению на всём жизненном цикле и выражаются в процентах для каждой стадии жизненного цикла - *ТЖЦ*.

Значения поправки функционала средних издержек к оценкам текущего уровня

устойчивости функционирования ПС ПД ВККС, полученные по формуле (15), приведены в таблице 7. Сравнительная характеристика изменения поправки функционала средних издержек в зависимости от применяемой модели устойчивости функционирования показана на рисунке 5 [Липаев В. В., 2005]. Из этого рисунка можно проследить темпы снижения издержек экспертизы устойчивости функционирования ПС ПД ВККС (Data Server на базе ОС Windows 2003 server, СУБД MS SQL server) от стадии к стадии жизненного цикла (см. сравнительные характеристические касательные a, b, c - рисунок 4).

Таблица 7 - Значения поправки функционала средних издержек.

	Изменение функционала средних издержек ΔJ_{0_i} на каждой стадии (при $T=T_{этапа}$) ЖЦ.					
		ΔJ_1^T	ΔJ_2^T	ΔJ_3^T	ΔJ_4^T	ΔJ_5^T
Угроза	Уязвимость GDI, приводящая к несанкционированному получению локальных прав, (CVE-2006-5758)	34.9 %	15.5 %	12.5 %	11.1 %	9.8 %
	Уязвимость WMF, приводящая к отказу в обслуживании, (CVE-2007-1211)	35.1 %	15.5 %	12.8 %	11.3 %	9.9 %
	Уязвимость EMF, приводящая к несанкционированному получению прав, (CVE-2007-1212)	34.8 %	15.0 %	12.9 %	11.4 %	9.8 %
	Уязвимость, связанная с обработкой GDI недопустимых размеров окна и приводящая к несанкционированному получению прав, (CVE-2006-5586)	35.1 %	15.0 %	12.5 %	11.4 %	9.9 %
	Уязвимость анимированного курсора Windows, приводящая к удаленному выполнению кода, (CVE-2007-0038)	35.5 %	15.8 %	12.8 %	12.3 %	10.1 %
	Уязвимость, связанная с обработкой GDI недопустимых параметров, (CVE-2007-1215)	36.0 %	15.6 %	12.3 %	12.2 %	10.5 %

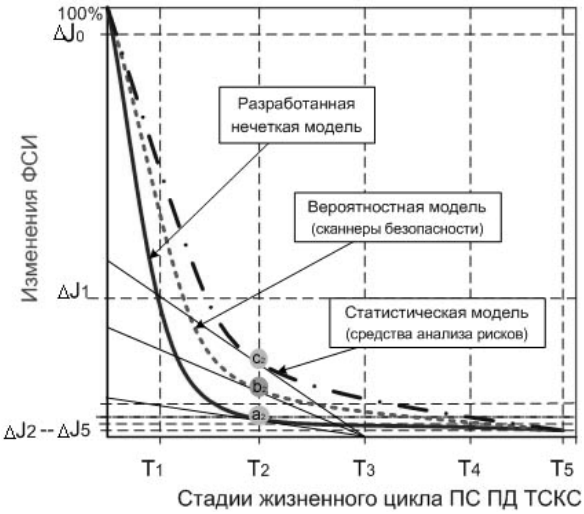

Рисунок 4 – Изменение функционала средних издержек и сравнение эффективности экспертизы (a_2, b_2, c_2)

Из анализа значений поправки функционала средних издержек (табл. 7) можно получить значения *достоверности* экспертных оценок, которая возрастает от стадии к стадии. Темпы роста достоверности (табл. 8) относительно каждой из угроз не одинаковы, так как различным угрозам эксперты с самого начала экспертизы уделяли не равнозначное внимание, а выделяли, на свое усмотрение, более или менее значимые.

	Достоверность экспертных оценок устойчивости функционирования ПС ТСКС для каждой стадии (при $T=T_{стадии}$) ЖЦ - J_{Ti}.					
		J_{T1}	J_{T2}	J_{T3}	J_{T4}	J_{T5}
Риск реализации угрозы	Уязвимость GDI, приводящая к несанкционированному получению локальных прав, (CVE-2006-5758)	65.1 %	84.5 %	87.5 %	88.9 %	90.2 %
	Уязвимость WMF, приводящая к отказу в обслуживании, (CVE-2007-1211)	64.9 %	84.5 %	87.2 %	88.7 %	90.1 %
	Уязвимость EMF, приводящая к несанкционированному получению прав, (CVE-2007-1212)	65.2 %	85.0 %	87.1 %	88.6 %	90.2 %
	Уязвимость, связанная с обработкой GDI недопустимых размеров окна и приводящая к несанкционированному получению прав, (CVE-2006-5586)	64.9 %	85.0 %	87.5 %	88.6 %	90.1 %
	Уязвимость анимированного курсора Windows, приводящая к удаленному выполнению кода, (CVE-2007-0038)	64.5 %	84.2 %	87.2 %	87.7 %	89.9 %
	Уязвимость, связанная с обработкой GDI недопустимых параметров, (CVE-2007-1215)	64.0 %	84.4 %	87.7 %	87.8 %	89.5 %

Таблица 8 - Результаты обеспечения достоверности экспертизы в зависимости от стадии жизненного цикла.

Например, риску появления уязвимости GDI, приводящей к несанкционированному получению локальных прав, (CVE-2006-5758) эксперты изначально уделили наиболее пристальное внимание, как наиболее опасному с их точки зрения. Наименьшее внимание эксперты уделяли возникновению уязвимости GDI, связанной с обработкой недопустимых параметров, (CVE-2007-1215), по причине высокой степени *резервирования* компонентов, участвующих в

процессах обработки SQL запросов ПС ПД ВККС.

В работе предлагается провести оценку эффективности предложенных решений, сводящуюся к определению *эластичности* (*stretchability*) функционала средних издержек в зависимости от стадии ЖЦ в точках $a=\{a_1, a_2, a_3, a_4, a_5,\}$; $b=\{b_1, b_2, b_3, b_4, b_5\}$; $c=\{c_1,c_2,c_3,c_4,c_5\}$ (см. рисунок 5), для уязвимости GDI, приводящей к несанкционированному получению локальных прав, (CVE-2006-5758). Задача оценки эффективности найденная по формулам (16, 17, 18):

$$S_a(t)=\frac{T_N}{\Delta J_a}\Delta J'(t),\ (16);\quad S_b(t)=\frac{T_N}{\Delta J_b}\Delta J'(t),\ (17);\quad S_c(t)=\frac{T_N}{\Delta J_c}\Delta J'(t),\ (18);$$

где ΔJ_a - значение функционала средних издержек в точке *a* полученном с помощью предложенной нечеткой модели; ΔJ_b - значение функционала средних издержек в точке *b* полученном с помощью вероятностной модели устойчивости функционирования; ΔJ_c - значение функционала средних издержек в точке *c* полученном с помощью статистической модели устойчивости функционирования; T_N – времени конца стадии (для примера на рисунке 5 - стадии поставки) жизненного цикла. Можно получить сравнительную характеристику эффективности различных методов (моделей) оценки устойчивости функционирования по формулам (16, 17, 18) в графическом виде представленную на рисунке 5. Эластичность $S_0(t)$ (16, 17, 18) функционала средних издержек $\Delta J(t)$ показывает относительное изменение (*убывание*) издержек вызванных условиями неполноты ретроспективной информации о значениях основных параметров устойчивости функционирования ПС ПД ВККС ($P(t)$; $T_в$; $f_{ПО}$; $K_у$ при сохранении исходных Δ; γ; J_c) при приращении времени стадии жизненного цикла ($T=\{T_1, T_2, T_3, T_4, T_5\}$) на один процент.

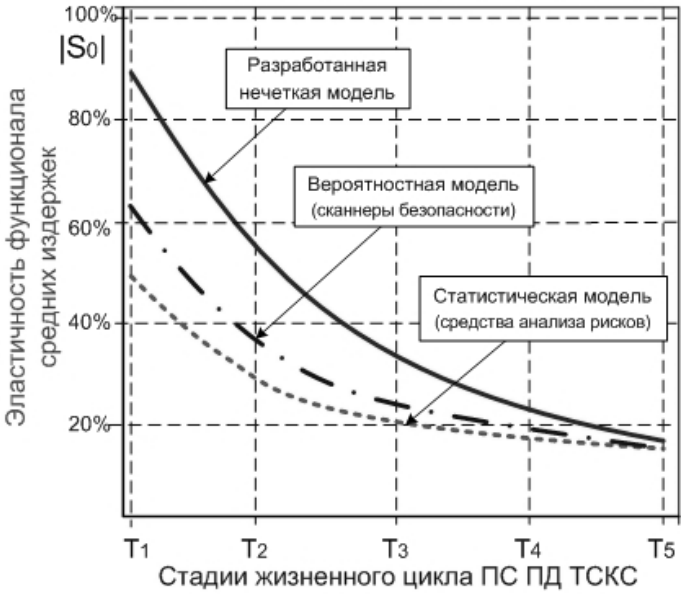

Рисунок 5 – графическая интерпретация эластичности функционала средних издержек полученного с помощью различных моделей устойчивости функционирования.

Из сравнения результатов (таблица 16, рисунок 10) видно, что *издержки,* при применении **предлагаемой нечеткой модели,** на ранних стадиях жизненного цикла убывают почти на 30 % быстрее, чем при применении вероятностной модели и почти на 40% быстрее, чем при применении статистической модели устойчивости функционирования.

<u>В четвертой главе</u> выполняется разработка рекомендаций по автоматизации метода согласования экспертных оценок устойчивости функционирования ПС ПД ВККС в условиях неполноты ретроспективной информации. Разрабатываемые рекомендации позволяют повысить производительность работ по проведению экспертизы устойчивости функционирования ПС ПД ВККС за счет

автоматизации процессов сбора и графического представления аналитической информации на основе внедрения программного средства, созданного в среде нечеткого моделирования MATLAB. Структурная схема модели автоматизации метода согласования экспертных оценок устойчивости функционирования ПС ПД ВККС представлена на рисунке 6. Посредством установки сенсоров, на базе контроллеров Infineon C166, модель автоматизации позволяет интерпретировать в графической форме события, приводящие к изменениям параметров устойчивости функционирования ПС ПД ВККС - $P(t)$; $T_в$; $f_{ПО}$; $K_у$. Результаты экспертизы представляются экспертам в виде эталонной функций принадлежности для чего вызывается графический интерпретатор нечеткого вывода командой (Ctrl+6).

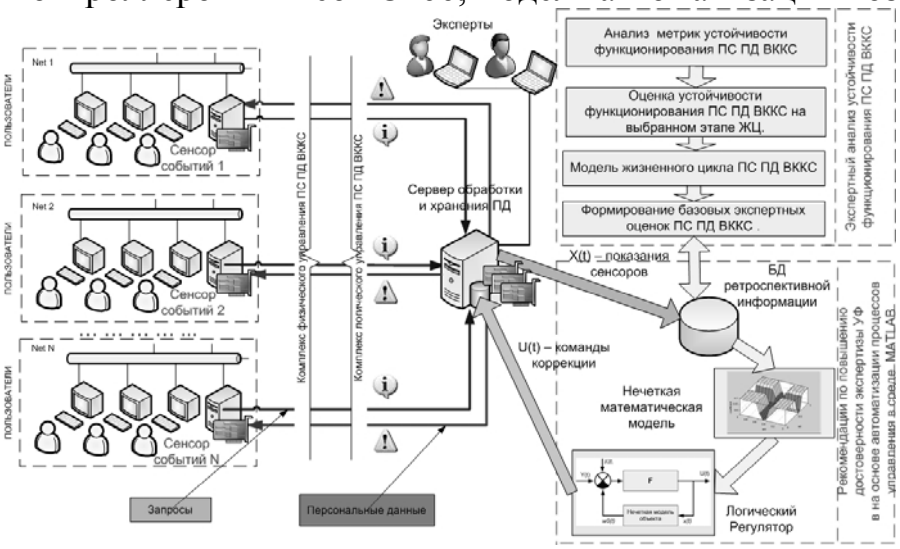

Рисунок 6 – Структурная схема модели автоматизации задачи обеспечения достоверности экспертизы устойчивости функционирования ПС ПД ВККС.

Результаты работ по моделированию взаимодействия угроз в аналитической форме были представлены в таблице 8. Значения поправок к измерениям основных параметров устойчивости функционирования ПС ПД ВККС - $P(t)$; $T_в$; $f_{ПО}$; $K_у$ при сохранении исходных значений Δ; γ; J_c, заложенным в требованиях ФСТЭК и ФСБ России и представлены в таблице 9 в виде *допусков*.

	Оценка показателя устойчивости функционирования ПС ПД ТСКС.				
Параметр	**T1**	**T2**	**T3**	**T4**	**T5**
Δ - время реакции	< 5 сек. ±34.3%	< 5 сек. ±14.3%	< 5 сек. ±12.3%	< 5 сек. ±11.1%	< 5 сек. ±10%
γ - пропускная способность	12,2 Мбайт/с. ±34.3 %	12,2 Мбайт/с. ±14.3%	12,2 Мбайт/с. ±12.3%	12,2 Мбайт/с. ±11.1%	12,2 Мбайт/с. ±10%
J_c-показатель использования	50% ±35.1%	57% ±15.3%	59% ±12.8%	70% ±11.3%	70% ±10%
$K_{эф}$ - коэффициент сохранения эффективности ПС ПД ТСКС	0,999 ±35.9 %	0,999 ±15.5 %	0,999 ±12.7 %	0,999 ±12.4 %	0,9997 ±10.2%
$P(t)$ - вероятность безотказной работы	0.6068 ±35.4 %	0.6530 ±15.3%	0.7650 ±12.3%	0.8019 ±11.3%	0.8187 ±9.3 %
$Tср_i$ - средняя наработка до отказа	1200 ч. ±35.4 %	1600 ч. ±15.4 %	1800 ч. ±12.4 %	2000 ч. ±11.4 %	2000 ч. ±10.1 %
$Tв$ - время восстановления после сбоев	10 ч ±34.1 %	9 ч ±15.1 %	8 ч ±12.6 %	8 ч ±12.1 %	8 ч ±11.3%
$f_{по}$ функциональность ПО	0,99 ±34.3 %	0,99 ±15.3 %	0,999 ±12.3 %	0,999 ±12.3 %	0,9997 ±11.3%
$K_у$ – Показатель устойчивости	0,995 ±35.5 %	0,997 ±15.5 %	0,9970 ±12.5 %	0,9974 ±12.3 %	0,9974 ±10 %
Средняя оценка достоверности	**65.1 %**	**84.5 %**	**87.5 %**	**88.9 %**	**90.2 %**

Также, при анализе действия угроз, по оценкам экспертов наибольшую опасность для устойчивости функционирования ПС ПД ВККС может представлять сочетание угроз, образуемое в *эпицентре* полученной оценочной графической поверхности. Наименее критичными являются угрозы вызванные уязвимостью CVE-2007-1215.

Таблица 9 - Достоверность экспертных оценок устойчивости функционирования.

Как показало практическое применение разработанных рекомендаций по обеспечению достоверности экспертизы устойчивости функционирования ПС ПД

ВККС на базе программного комплекса MATLAB, время анализа полученных результатов не превышает 0,5 значения времени отведенного для принятия решения (12), что доказывает его высокую эффективность.

ЗАКЛЮЧЕНИЕ

В ходе проведения диссертационных исследований были получены следующие научные и практические выводы и результаты.

1. Современные ПС ПД ВККС широко используются в существующей информационной инфраструктуре Российской Федерации и в значительной степени влияют на дальнейшее развитие Государства. Многообразие сложных систем ПС ПД ВККС, наряду с территориальной распределенностью сегментов, значительным объемом хранимой, обрабатываемой и передаваемой информации, определяют их высокую уязвимость при воздействии различного вида угроз.

2. С целью обеспечения требуемой устойчивости функционирования сложных систем входящих в комплекс ПС ПД ВККС в условиях воздействия неблагоприятных факторов необходимо решение научной задачи обеспечения достоверности экспертизы устойчивости функционирования ПС ПД ВККС на ранних стадиях ЖЦ в условиях неполноты ретроспективной информации, вне зависимости от применяемых методов экспертизы. Математическая постановка рассматриваемой научной задачи в работе представлена, как задача согласования экспертных оценок устойчивости функционирования ПС ПД ВККС на основе принципов нечеткой логики. При этом структура экспертных оценок устойчивости функционирования ПС ПД ВККС задается совокупностью нечетких полихроматических множеств, определяющих взаимосвязь угроз информационной безопасности, в условиях неполноты ретроспективной информации и дается определение степени такой неполноты.

3. Разработан метод оптимизации стратегии экспертной оценки устойчивости функционирования ПС ПД ВККС на ранних стадиях жизненного цикла в условиях неполноты ретроспективной информации на основе нахождения предельного функционала средних издержек. На основании полученной модели издержек в исходном описании объекта и угроз определяется набор стратегий по оптимальной организации экспертизы устойчивости функционирования ПС ПД ВККС. Такая постановка задачи, способна сократить значение издержек организации процессов и работ по принятию решения экспертами на ранних стадиях ЖЦ почти на 30%, в сравнении с применением вероятностной модели и почти на 40%, в сравнении с применением статистической модели устойчивости функционирования.

4. Разработаны рекомендации по автоматизации метода согласования экспертных оценок устойчивости функционирования в условиях неполноты ретроспективной информации на ранних стадиях жизненного цикла, на основе среды программирования MATLAB, способные сократить время принятия решения экспертами об устойчивости функционирования ПС ПД ВККС в условиях неполноты ретроспективной информации, на ранних стадиях жизненного цикла до 50 %, за счет автоматизации процессов согласования экспертных оценок и графического представления аналитической информации в

виде удобном для обработки.

Основные положения диссертации изложены в следующих публикациях.

Реферируемые издания, рекомендованные ВАК

1. Тюрин М. В. Экспертная оценка живучести телекоммуникационных систем и компьютерных сетей в условиях неполноты информации // Автоматизация в промышленности. – 2008. - №7. - С.15 - 18. – реферируемое издание рекомендованное ВАК.
2. Тюрин М. В. Некоторые пути повышения живучести телекоммуникационных систем и компьютерных сетей // Автоматизация в промышленности. – 2007. - №7. - С.11 - 16. – реферируемое издание рекомендованное ВАК.
3. Тюрин М. В. Стандартизация информационной безопасности в банковской деятельности // Банковское дело. – 2006. - №7. - С.50 - 53. – реферируемое издание, рекомендованное ВАК.

Другие издания

4. Тюрин М. В. Некоторые аспекты управления живучестью телекоммуникационных систем и компьютерных сетей // Технологии безопасности. – 2007. - №2. - С.15 - 19.
5. Тюрин М. В. Национальные особенности управления информационными рисками // Byte. – 2006. - №3(91). - С. 62 – 67.
6. Тюрин М. В. Особенности российских стандартов защиты информации // Byte. – 2005. - №12(88). - С. 65 – 68.
7. Тюрин М. В. Особенности национальной стандартизации информационной безопасности // PCWeek/RE. - 2005. - № 36(498). - С. 33 - 35.

Подписано в печать 18.10.2010
Бум. офсетная, Формат 60x84 1/16. Печать офсетная.
Усл. печ. л. 1. Тираж 100
Заказ 835
ЗАО «Копи Центр»
Павелецкая пл., д.2, стр.1.