

**Автономная некоммерческая организация
дополнительного профессионального образования
«ОРЛОВСКИЙ РЕГИОНАЛЬНЫЙ ЦЕНТР ИНТЕРНЕТ-ОБРАЗОВАНИЯ»**

ДИПЛОМНАЯ РАБОТА

«Автоматизация решения прикладной»

Слушатель: Б{ { { { {

Орел -2017

- 1) **Н**еопределенность подходов количественной оценки БИ КИВС
- 2) **О**тсутствие эффективных средств количественной оценки БИ в КИВС;
- 3) **С**ложность выбора рациональных систем ЗИ
- 4) **П**овышением требований к конфиденциальной информации субъектов информационных систем
- 5) **Ш**ирокое им внедрением ИКТ в сферы и виды деятельности личности, общества, государства
- 6) **И**ntenсивное развитие технических средств разведки, возникновением благоприятных условий их применения
- 7) **Д**ругие.

Цель работы: повышение качества процесса оценки безопасности информации, обрабатываемой в корпоративной информационно-вычислительной сети (КИВС)

Объект исследований: защищаемая КИВС
и ее компоненты

Предмет исследований: совокупность методов, моделей и средств оценки безопасности информации обрабатываемой в КИВС

Постановка частных задач работы:

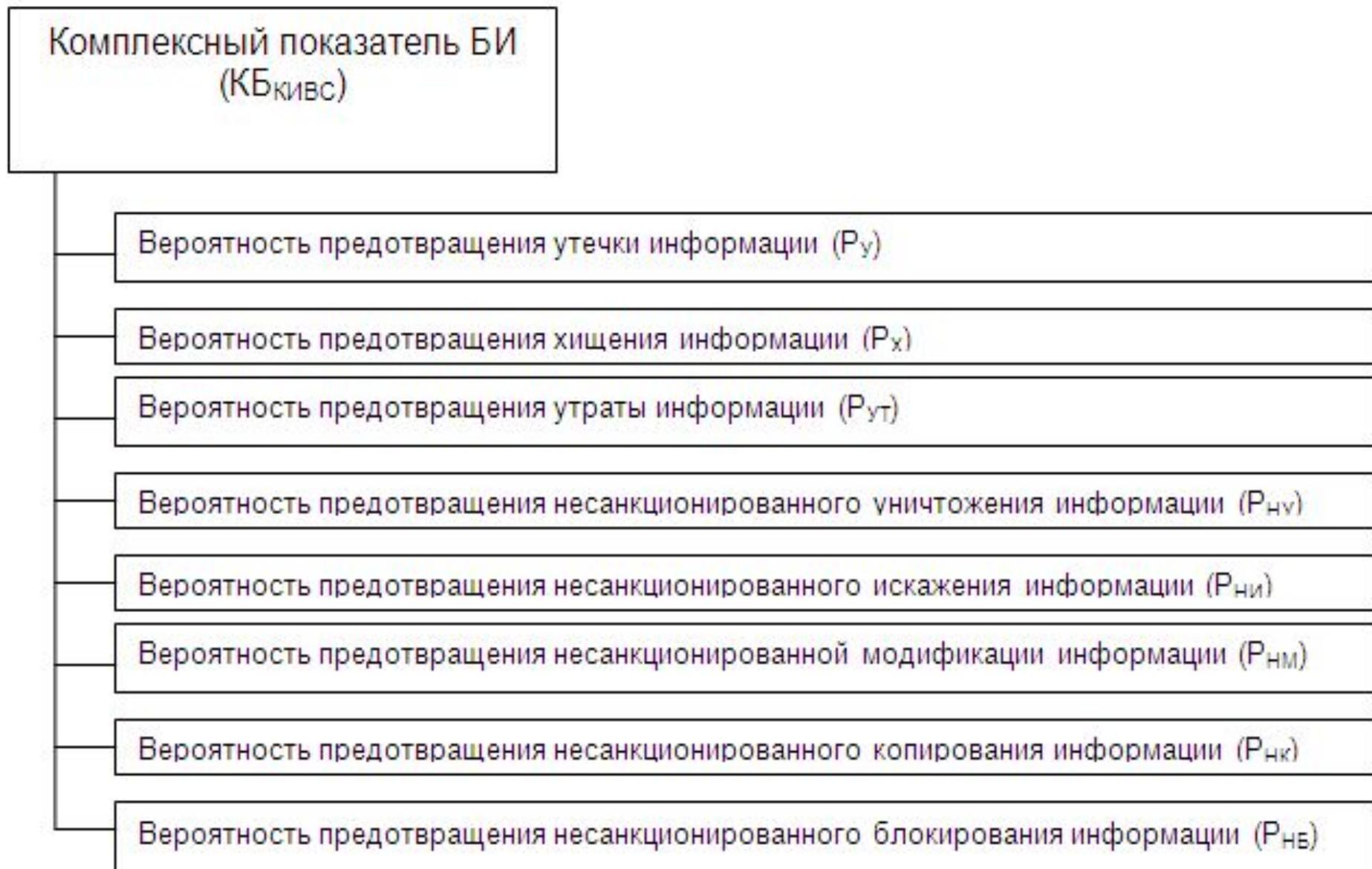
4

1. Анализ особенностей функционирования КИВС, угроз БИ, методов, способов и средств обеспечения БИ, обрабатываемой в КИВС
2. Разработка модели оценки безопасности информации, обрабатываемой в КИВС
3. Разработка алгоритма оценки безопасности информации, обрабатываемой в КИВС
4. Разработка прототипа программной реализации автоматизированной моделирующей системы оценки безопасности информации (АМСОБИ) обрабатываемой в КИВС

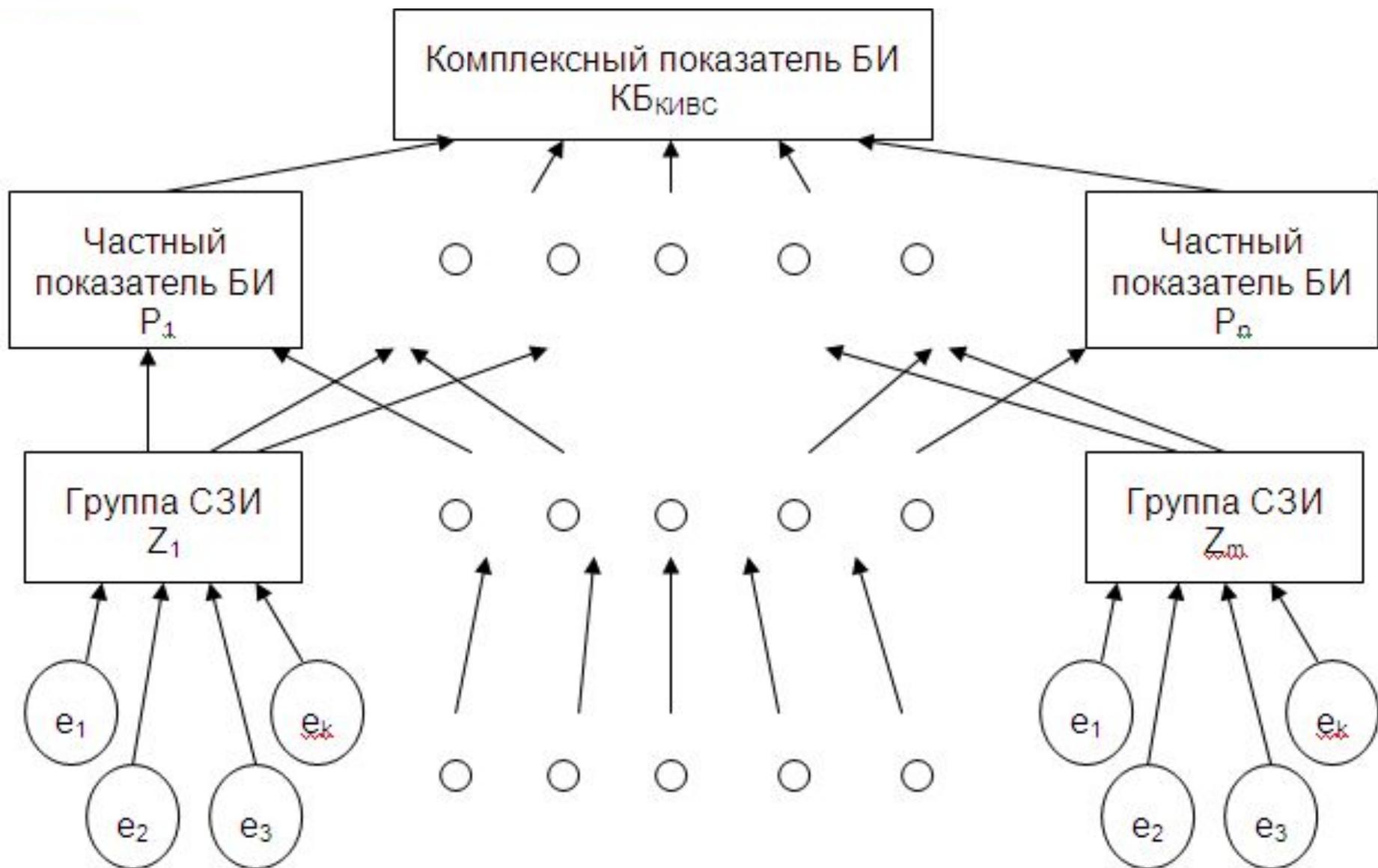
Основные результаты решения частных задач, выносимые на защиту

1. Структура показателей оценки БИ, обрабатываемой в КИВС, методика получения значений единичных показателей БИ, весовых коэффициентов значимости частных показателей БИ, обрабатываемой в КИВС
2. Модель оценки БИ в КИВС
3. Алгоритм оценки БИ в КИВС
4. Программный прототип автоматизированной моделирующей системы оценки БИ (АМСОБИ) обрабатываемой в КИВС

Структура частных показателей оценки БИ

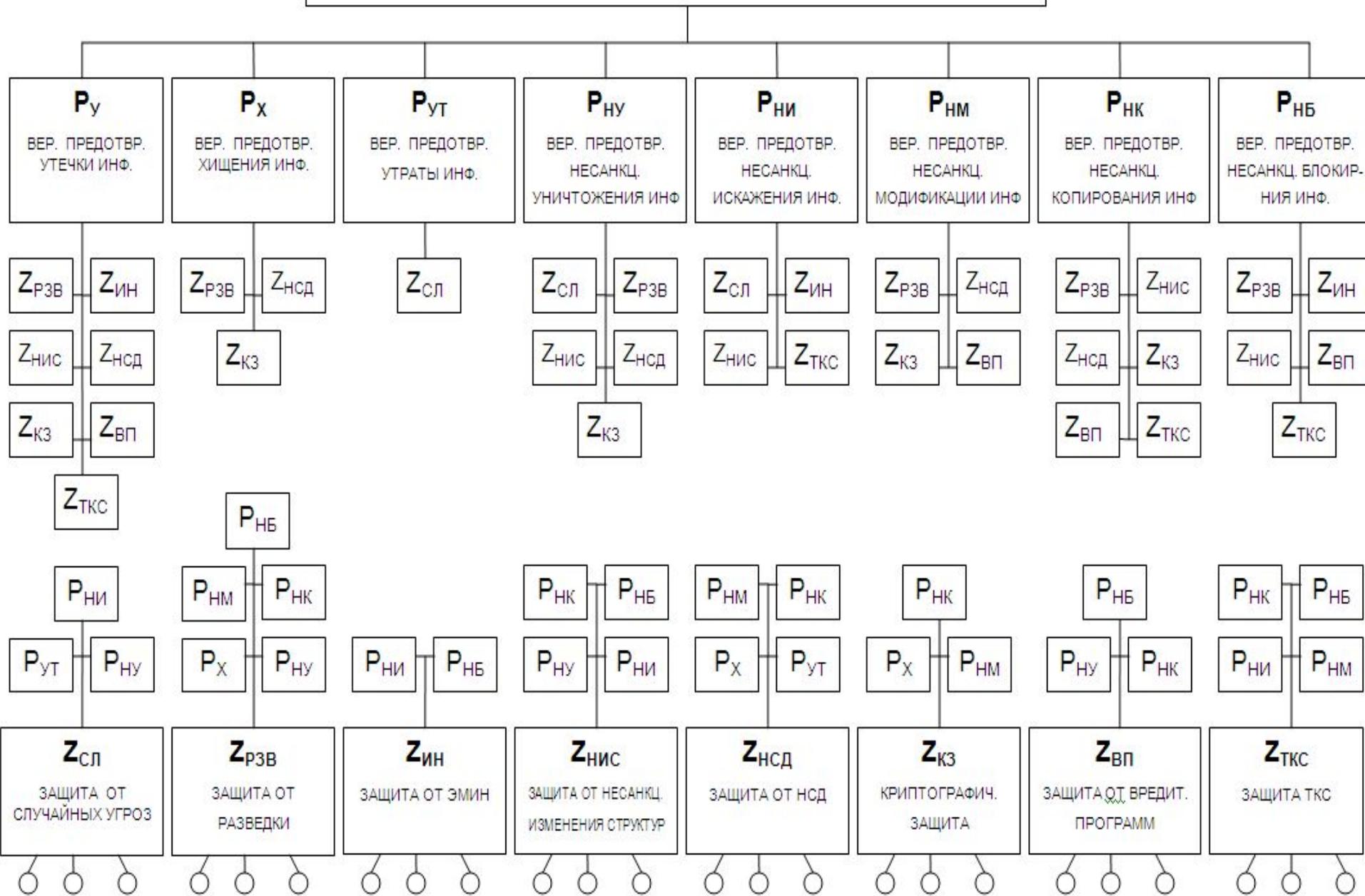


Структура показателей оценки БИ



Комплексный показатель БИ защищённой КИВС

КБ_{КИВС}

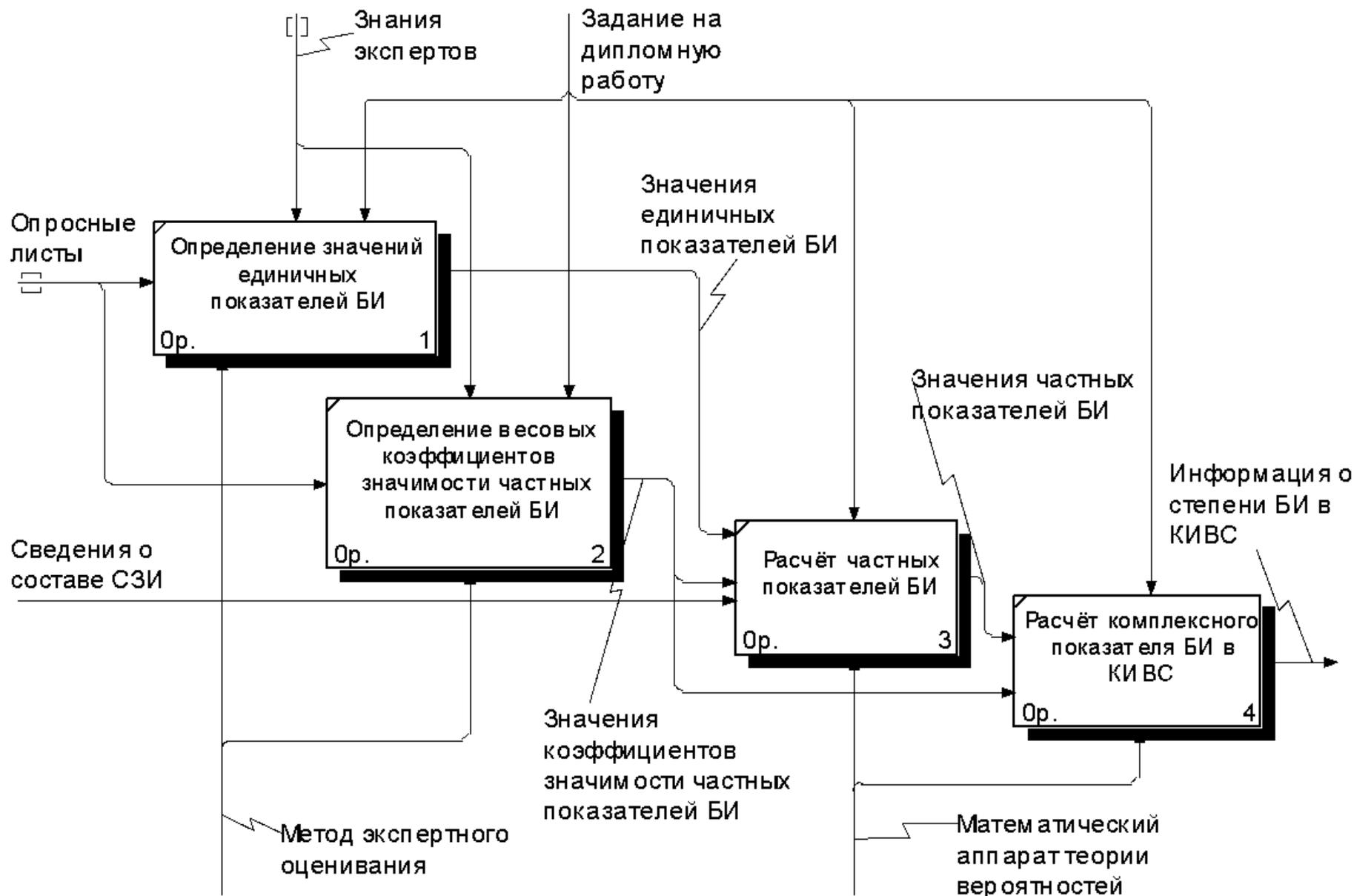


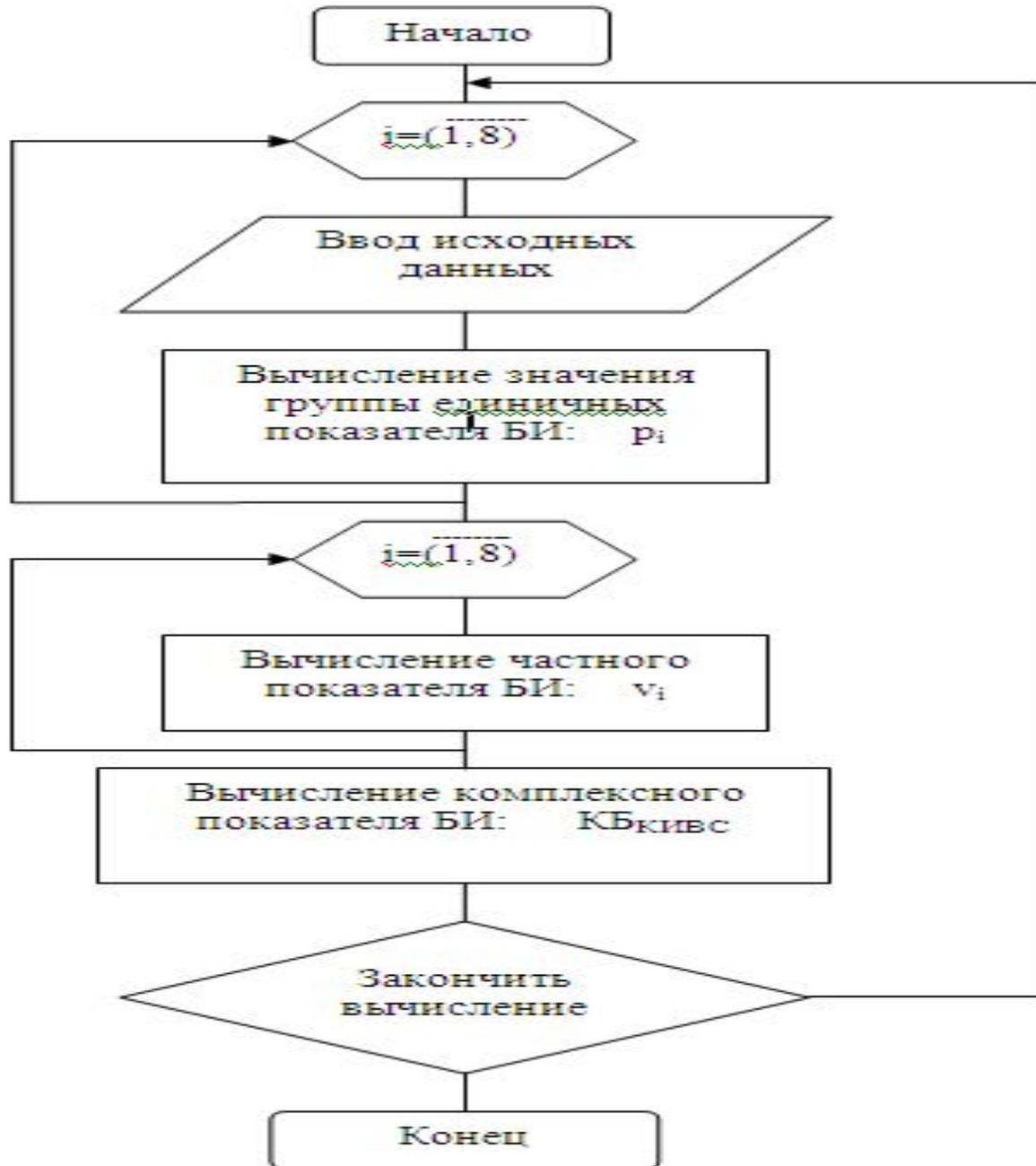
Общая модель оценки БИ, обрабатываемой в КИВС 9



Функциональная модель оценки БИ, обрабатываемой в КИВС

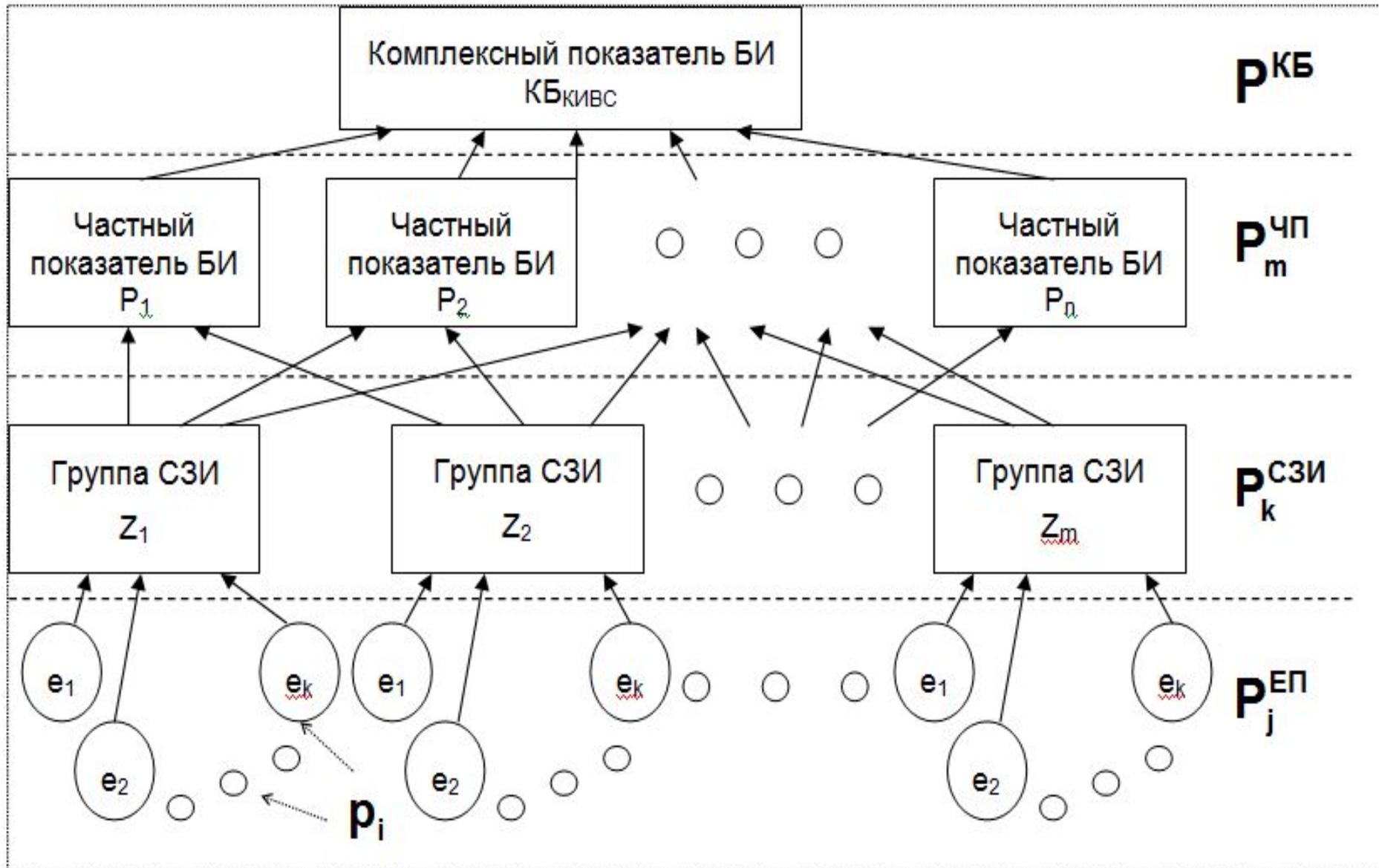
10





Вычисление показателей БИ, обрабатываемой в КИВС

12



Вычисление показателей БИ, обрабатываемой в КИВС

13

$$P_j^{\text{ЕП}} = 1 - \prod_i (1 - p_i) \quad (1)$$

$$P_k^{\text{СЗИ}} = 1 - \prod_l (1 - \alpha_l^{\text{ЕП}} \cdot P_l^{\text{ЕП}}) \quad (2)$$

$$P_m^{\text{ЧП}} = 1 - \prod_n (1 - \alpha_n^{\text{СЗИ}} \cdot P_n^{\text{СЗИ}}) \quad (3)$$

$$P^{\text{КБ}} = 1 - \prod_q (1 - \alpha_q^{\text{ЧП}} \cdot P_q^{\text{ЧП}}) \quad (4)$$

p_i – вероятность обеспечения БИ i -ым единичным показателем БИ

$P_j^{\text{ЕП}}$ – вероятность предотвращения угрозы j -ой группой единичных показателей

$P_k^{\text{СЗИ}}$ – вероятность предотвращения угрозы k -ой группой СЗИ

$\alpha_l^{\text{ЕП}}$ – весовой коэффициент значимости l -той группы единичных показателей БИ

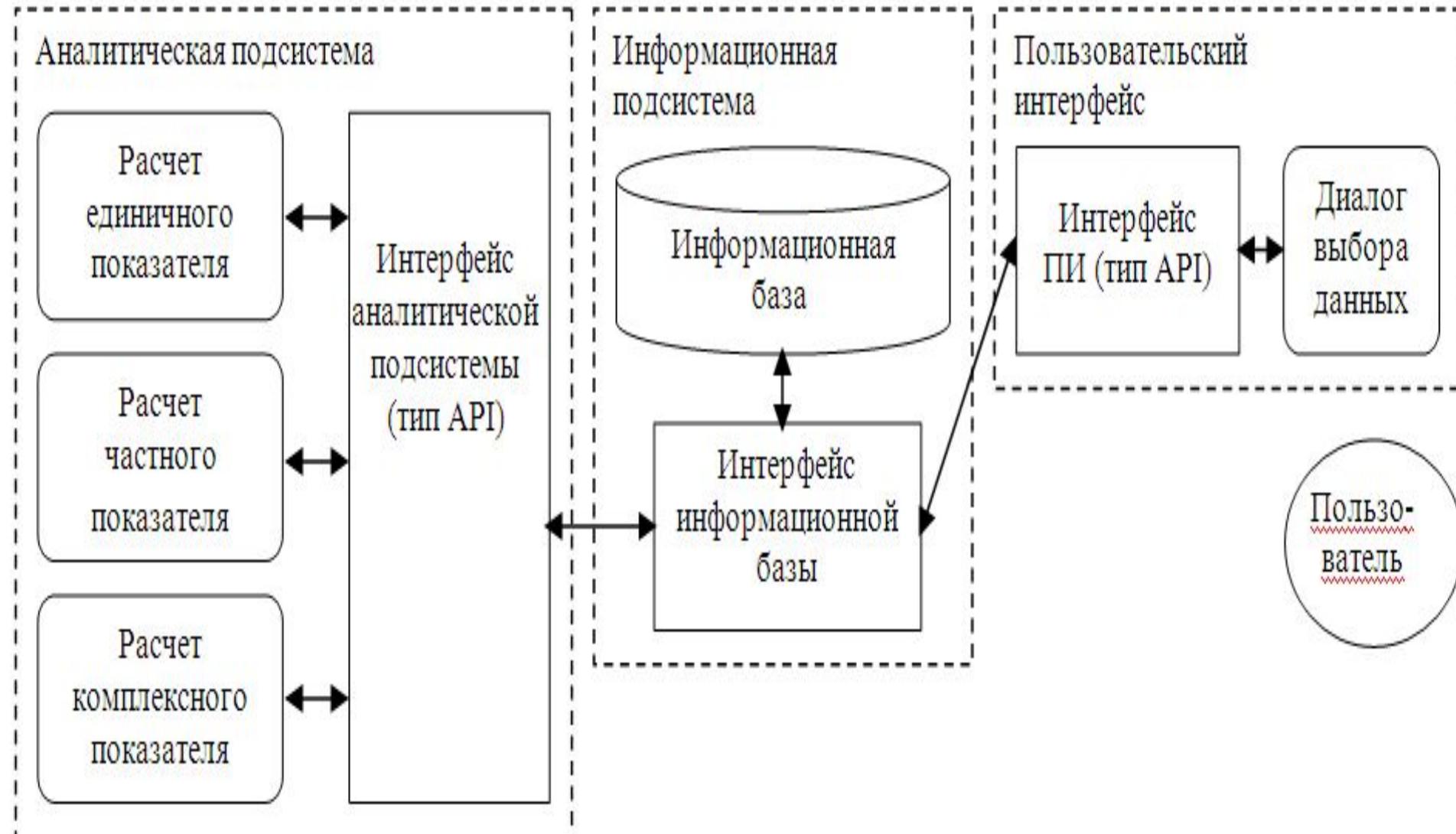
$P_m^{\text{ЧП}}$ – вероятность предотвращения m -ой угрозы, т.е. частный показатель БИ

$\alpha_n^{\text{СЗИ}}$ – весовой коэффициент значимости n -ой группы СЗИ

$\alpha_q^{\text{ЧП}}$ – весовой коэффициент значимости q -ого частного показателя БИ

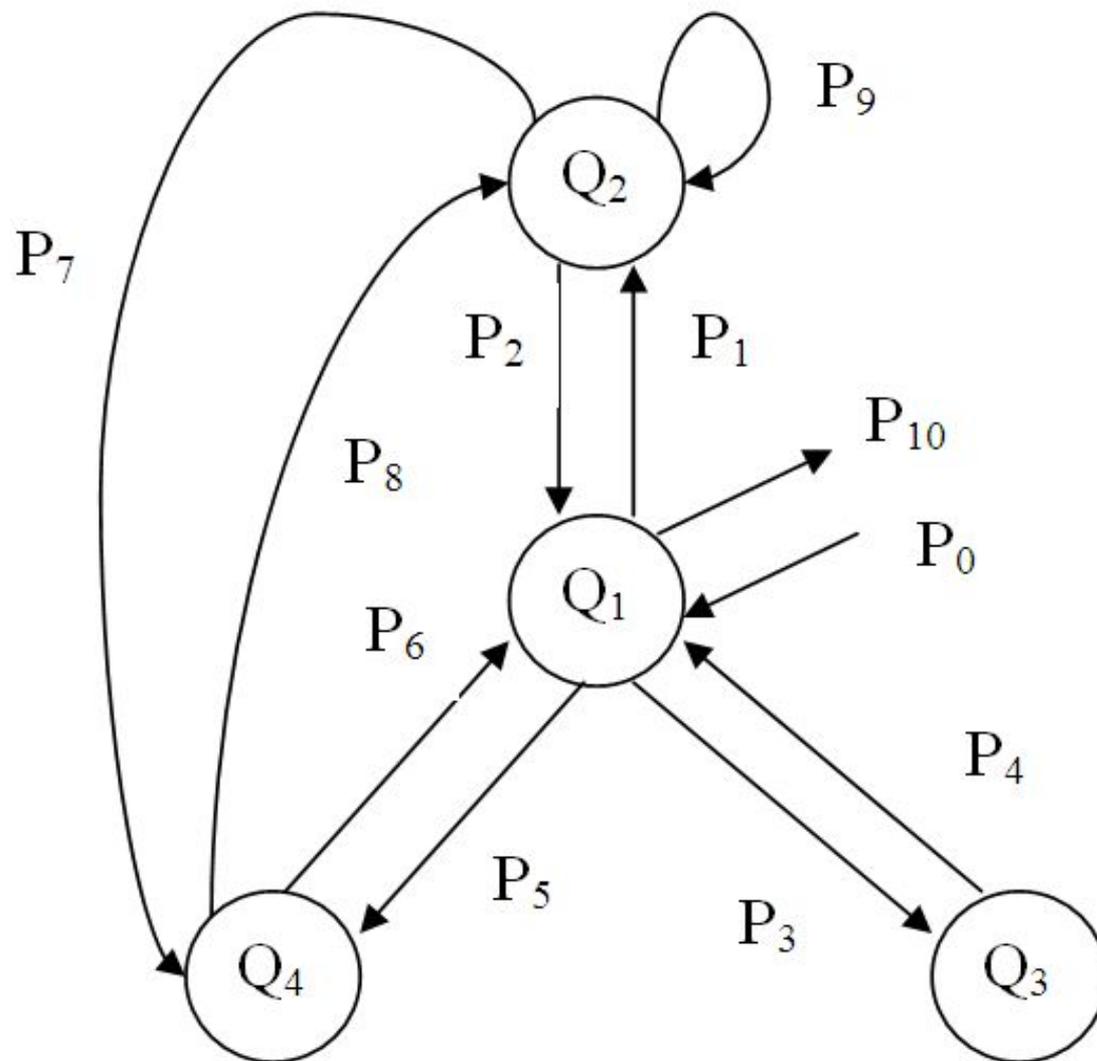
$P^{\text{КБ}}$ – значение комплексного показателя безопасности БИ в защищённой КИВС

Структурная схема АМСОБИ, обрабатываемой КИВС



Транзитивная сеть пользовательского интерфейса

15



Состояния пользовательского интерфейса АМСОБИ 16

Состояние	Функция	Задача	Событие	Сообщение	Постусловие
Q ₁	Приём команд по выбору действия	Ожидание; отображение результатов расчёта	Запуск приложения	–	True
Q ₂	Ввод исходных данных	Приём и отображение <u>исходных</u> данных	Нажатие кнопки «Комплексный показатель БИ»	–	True
Q ₃	Сохранение результатов расчёта	Ожидание ввода имени файла	Нажатие кнопки «Сохранить»	–	True
Q ₄	Просмотр справки	Отображение содержания файла справки	Нажатие кнопки «Справка»	–	<u>True</u>

Переходы пользовательского интерфейса АМСОБИ

17

Переход	Событие	Предусловие	Форма	Объект	Субъект	Методы
P_0	Запуск приложения	—	Form1	Файл приложения	Пользователь	Form1.Create
P_1	Нажатие кнопки «Комплексный показатель БИ» или «Вероятность предотвращения ...»	$Q_1=true$	Form1	Форма пользовательского интерфейса	Пользователь	Form2.Show Modal, Form3.Show Modal
P_2	Нажатие кнопки «Далее >>>»	$Q_2=true$	Form2, Form7, Form9	Форма пользовательского интерфейса	Пользователь	Form1. <u>Show</u>

Переходы пользовательского интерфейса 18

АМСОБИ

Переход	Событие	Предусловие	<u>Форма</u>	Объект	Субъект	<u>Методы</u>
P ₃	Нажатие кнопки «Сохранить»	Q ₁ =true	Form1	Форма пользовательского интерфейса	Пользователь	Form1. <u>SaveDialog</u>
P ₄	Нажатие кнопки «Сохранить» или «Отмена»	Q ₃ =true	<u>SaveDialog</u>	Стандартная форма сохранения файла	Пользователь	SaveDialog. <u>Close</u>
P ₅	Нажатие кнопки «Справка»	Q ₁ =true	Form1	Форма пользовательского интерфейса	Пользователь	Form14. <u>ShowModal</u>
P ₆	Нажатие кнопки «Вернуться»	Q ₄ =true	Form14	Окно справки	Пользователь	Form14. <u>Close</u>
P ₇	Нажатие кнопки «Справка»	Q ₂ =true	Form2-Form13	Форма пользовательского интерфейса	Пользователь	Form2-13. <u>Close</u>

Переходы пользовательского интерфейса АМСОБИ

Переход	Событие	Предусловие	Форма	Объект	Субъект	Методы
P ₈	Нажатие кнопки «Вернуться»	<u>Q₄=true</u>	Form14	Окно справки	Пользователь	Form14.Close
P ₉	Нажатие кнопки «Далее»	Q ₂ =true	Form2-Form13	Форма пользовательского интерфейса	Пользователь	<u>FormX.Close</u>
P ₁₀	Нажатие кнопки «Выход»	Q ₁ =true	Form1	Форма пользовательского интерфейса	Пользователь	Form1.Close

Объект	Спецификация	Переменные входного сообщения
O ₁	Окно	PosX1 – координата X левого верхнего угла PosY1 – координата Y левого верхнего угла PosX2 – координата X правого нижнего угла PosY2 – координата Y правого нижнего угла <u>Menu</u> – вид системного меню Icon – иконка <u>Name</u> – имя окна
O ₂	Строка редактирования	PosX1 – координата X левого верхнего угла PosY1 – координата Y левого верхнего угла PosX2 – координата X правого нижнего угла PosY2 – координата Y правого нижнего угла
O ₃	Кнопка	PosX1 – координата X левого верхнего угла PosY1 – координата Y левого верхнего угла PosX2 – координата X правого нижнего угла PosY2 – координата Y правого нижнего угла <u>Name</u> – название кнопки
O ₄	Флаговая кнопка	PosX1 – координата X левого верхнего угла PosY1 – координата Y левого верхнего угла PosX2 – координата X правого нижнего угла PosY2 – координата Y правого нижнего угла <u>Name</u> – название кнопки Check – состояние кнопки
O ₅	Селективная кнопка	PosX1 – координата X левого верхнего угла PosY1 – координата Y левого верхнего угла PosX2 – координата X правого нижнего угла PosY2 – координата Y правого нижнего угла <u>Name</u> – название кнопки Check – состояние кнопки

Форма	Спецификация	Объект
Form1	Главное окно	O _{1_1} – окно O _{3_1} – кнопки
Form2	Окно ввода данных «Защита от случайных угроз»	O _{1_2} – окно O _{3_2} – кнопки O _{4_2} – <u>флаговые кнопки</u> O _{5_2} – селективные кнопки
Form3	Окно ввода данных «Защита от разведки»	O _{1_3} – окно O _{3_3} – кнопки O _{4_3} – <u>флаговые кнопки</u> O _{5_3} – селективные кнопки
Form4	Окно ввода данных «Защита от ЭМИН»	O _{1_4} – окно O _{3_4} – кнопки O _{4_4} – <u>флаговые кнопки</u> O _{5_4} – селективные кнопки
Form5	Окно ввода данных «Защита от несанкционированного изменения структур»	O _{1_5} – окно O _{3_5} – кнопки O _{4_5} – <u>флаговые кнопки</u> O _{5_5} – селективные кнопки

Форма	Спецификация	Объект
Form6	Окно ввода данных «Защита от НСД»	O _{1_6} – окно O _{3_6} – кнопки O _{4_6} – флаговые кнопки O _{5_6} – селективные кнопки
Form7	Окно ввода данных «Криптографическая защита»	O _{1_7} – окно O _{2_7} – окно редактирования O _{3_7} – кнопки O _{4_7} – флаговые кнопки O _{5_7} – селективные кнопки
Form 8	Окно ввода данных «Защита от вредительских программ»	O _{1_8} – окно O _{2_8} – окна редактирования O _{3_8} – кнопки O _{4_8} – флаговые кнопки O _{5_8} – селективные кнопки
Form 9	Окно ввода данных «Защита телекоммуникационной составляющей»	O _{1_9} – окно O _{3_9} – кнопки O _{4_9} – флаговые кнопки O _{5_9} – селективные кнопки
Form 10	Окно ввода данных «Контролируемая территория»	O _{1_10} – окно O _{3_10} – кнопки O _{4_10} – флаговые кнопки
Form 11	Окно ввода данных «Здание»	O _{1_11} – окно O _{3_11} – кнопки O _{4_11} – флаговые кнопки
Form 12	Окно ввода данных «Помещение»	O _{1_12} – окно O _{3_12} – кнопки O _{4_12} – флаговые кнопки
Form 13	Окно ввода данных «Устройства, носители информации»	O _{1_13} – окно O _{3_13} – кнопки O _{4_13} – флаговые кнопки

Экранная форма Главного окна пользовательского интерфейса

23

Комплекс оценки безопасности информации в КИВС

Комплексный показатель БИ 0,0%

Вероятность предотвращения утечки информации	0,0%
Вероятность предотвращения хищения информации	0,0%
Вероятность предотвращения утраты информации	0,0%
Вероятность предотвращения несанкционированного уничтожения информации	0,0%
Вероятность предотвращения несанкционированного искажения информации	0,0%
Вероятность предотвращения несанкционированной модификации информации	0,0%
Вероятность предотвращения несанкционированного копирования информации	0,0%
Вероятность предотвращения несанкционированного блокирования информации	0,0%

Сохранить Справка Выход

Экранной форма вложенного окна «Защита от случайных угроз»

24

Защита от случайных угроз

<p>Дублирование информации</p> <p><input checked="" type="radio"/> не применяется <input type="radio"/> применяется частично <input type="radio"/> применяется</p>	<p>Повышение надёжности КИВС</p> <p><input checked="" type="radio"/> не применяется <input type="radio"/> применяется частично <input type="radio"/> применяется</p>	<p>Блокировка ошибок</p> <p><input checked="" type="radio"/> не применяется <input type="radio"/> применяется частично <input type="radio"/> применяется</p>
<p>Восстановление информации:</p> <p><input type="checkbox"/> неоперативное <input type="checkbox"/> оперативное</p> <p>Средства восстановления:</p> <p><input type="checkbox"/> дополнительные ВЗУ <input type="checkbox"/> спец. области памяти <input type="checkbox"/> съёмные носители</p> <p>Дублирование:</p> <p><input type="checkbox"/> одноуровневое <input type="checkbox"/> многоуровневое <input type="checkbox"/> сосредоточенное <input type="checkbox"/> рассредоточенное <input type="checkbox"/> полное копирование <input type="checkbox"/> частичное копирование <input type="checkbox"/> зеркальное копирование <input type="checkbox"/> со сжатием данных <input type="checkbox"/> без сжатия данных</p>	<p>Программное обеспечение:</p> <p><input type="checkbox"/> прогрессивные технологии <input type="checkbox"/> контроль правильности <input type="checkbox"/> лицензионное ПО</p> <p>Аппаратное обеспечение:</p> <p><input type="checkbox"/> профилактика <input type="checkbox"/> контроль функционир-ния</p>	<p><input type="checkbox"/> защитные экраны <input type="checkbox"/> ограждения <input type="checkbox"/> предохранители <input type="checkbox"/> блокировка записи <input type="checkbox"/> аппар.-программные средства</p>
	<p>Повышение отказоустойч-ти КИВС</p> <p><input checked="" type="radio"/> не применяется <input type="radio"/> применяется частично <input type="radio"/> применяется</p>	<p>Оптимизация работы с системой</p> <p><input checked="" type="radio"/> не применяется <input type="radio"/> применяется частично <input type="radio"/> применяется</p>
	<p><input type="checkbox"/> резервирование <input type="checkbox"/> помехоустойчивое кодирование <input type="checkbox"/> создание адаптивных систем</p>	<p><input type="checkbox"/> оборудование рабочих мест <input type="checkbox"/> оптимальн. режим труда/отдыха <input type="checkbox"/> дружелюбный интерфейс <input type="checkbox"/> воспитание персонала <input type="checkbox"/> обучение персонала</p>

Далее >> **Отмена**

Экранной форма вложенного окна «Защита от разведки»

25

Защита от разведки

Система охраны объекта

отсутствует
 имеется

контролируемая территория
 здание
 помещение
 устройства

Защита от подслушивания

отсутствует
 имеется

В каналах связи:

скремблирование
 шифрование

В помещениях:

звукоизоляция
 зашумление
 обнаружение диктофонов
 обнаружение "жучков"

Защита в оптическом диапазоне

отсутствует
 имеется

"односторонние" стёкла
 окрашивание стёкол
 шторы
 правильное размещение

Защита от злоумышленных действий персонала

отсутствует
 имеется

сбор информации о сотрудниках
 охрана сотрудников
 разграничение доступа к ИР
 контроль злоумышленных действий
 создание здорового климата

Организация работ с конфиденциальными ИР

отсутствует
 имеется

разграничение полномочий
 оборудованы места работы с конфиденц. ИР
 установлен порядок учёта, выдачи, работы
 организовано уничтожение мусора
 организован контроль работы

Далее >> **Отмена**

Экранная форма окна «Защита от разведки» – «Помещение»

26

The screenshot shows a software window titled "Помещение" (Room) with a close button (X) in the top right corner. The window contains several sections of security-related options, each with a list of items and a checkbox:

- Инженерные конструкции**
 - деревянные двери
 - металлические двери
 - механические замки
 - кодовые замки
 - решётки на окнах
 - специальные стёкла
- Средства наблюдения**
 - видеокамеры
 - коммутаторы
 - мультиплексоры
 - детекторы движения
- Система доступа**
 - пропуска
 - пароли
 - коды
 - ключи от дверей
 - пластиковые карты
 - биометрическая идентификация
- Дежурная смена охраны**
 - круглосуточная
 - вооружённая
- Охранная сигнализация**
 - контактные датчики
 - оптико-электронные датчики
 - микроволновые датчики
 - вибрационные датчики
 - акустические датчики

At the bottom of the window, there are two buttons: "Отмена" (Cancel) on the left and "Далее >>" (Next >>) on the right.

Разработанный прототип программной реализации автоматизированной моделирующей системы оценки БИ, обрабатываемой в КИВС, позволяет:

- 1) получить объективную количественную оценку БИ;
- 2) Обеспечивает оперативность решения задачи оценки БИ в условиях изменения количества угроз и комплекса мер, средств и мероприятий ЗИ;
- 3) получить прогнозную оценку вновь разрабатываемых и модернизируемых КИВС

Результаты работы, выносимые на защиту обладают элементами **новизны** и **практической значимости** для деятельности практических органов и организаций при разработке защищенных КИВС, организации системы ЗИ КИВС и контроля за степенью обеспечения БИ, обрабатываемой КИВС