НИЯУ МИФИ

Применение метода нечетких множеств в процессе проведения аудита информационной безопасности

Подготовил Антипенко Д.А.

Москва 2026

1. Постановка задачи и актуальность

- Аудит ИБ — процесс оценки соответствия требованиям защиты информации.

- Проблема: международные и отечественные стандарты опираются на качественные оценки.
- Следствие: высокая субъективность результатов и отсутствие числовых расчетов
- Задача: внедрение количественной оценки с помощью аппарата нечеткой логики.

2. Цели аудита информационной безопасности

3. Пять этапов формализации метода аудита

4. Классификация угроз по источникам и локализации

По типу источника: антропогенные, техногенные, стихийные .

По локализации:

1) Внутренние (субъекты с доступом к инфраструктуре).
2) Внешние (субъекты без санкционированного доступа).
3) Комбинированные.

5. Стандарты как фундамент критериев оценки

- BS 7799 и ISO/IEC 17799 (ГОСТ Р ИСО/МЭК 17799-2005).
- ISO/IEC 15408 (Общие критерии оценки ИТ) .
- Методика оценки угроз ФСТЭК России (05.02.2021 г.).

6. Принципы построения нечеткого классификатора

- Использование лингвистических переменных вместо сухих цифр.
- Определение взаимодействий через нечеткие высказывания.
- Описание операций специальными нечеткими алгоритмами.
- Применение весовых коэффициентов для каждого параметра

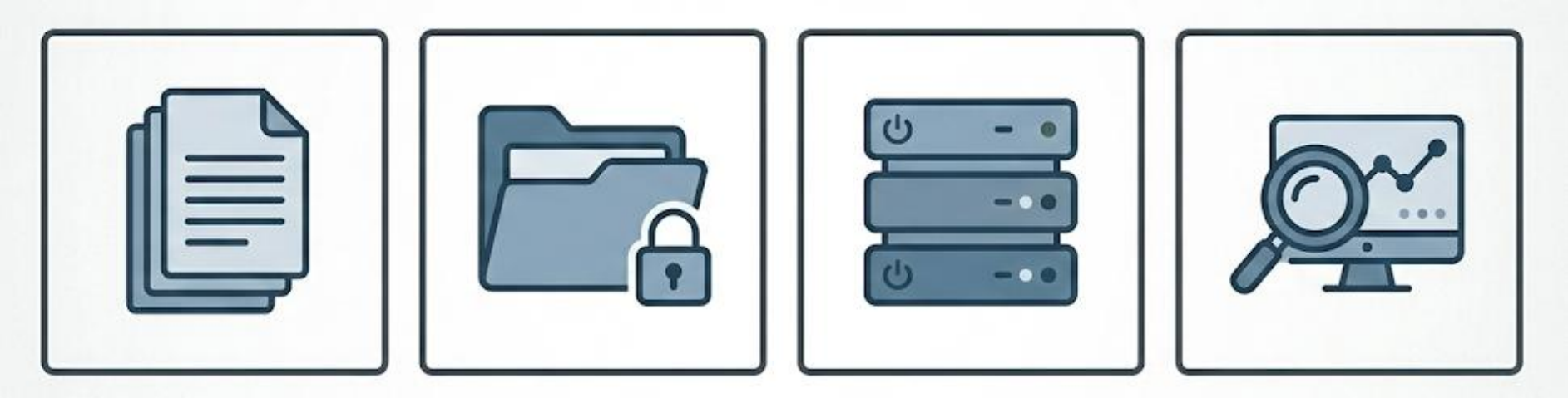
СХЕМА «ЧЕРНЫЙ ЯЩИК»: НЕЧЕТКАЯ ЛОГИКА

7. Многоуровневая структура аудита

- Вертикальная многоуровневая оценка защищенности.
- Итерационный подход вместо линейного анкетирования.
- Структура разделов:
  - Раздел 1 -> Уровень зрелости $1, 2, \ldots n$.
  - Раздел 2 -> Уровень зрелости $1, 2, \ldots n$.

8. Входные переменные модели (V1 – V4)

- $V1$: Организационная защита информации.
- $V2$: Защита конфиденциальных данных.
- $V3$: Защита АРМ, серверной и сетевой инфраструктуры.
- $V4$: Мониторинг событий информационной безопасности.



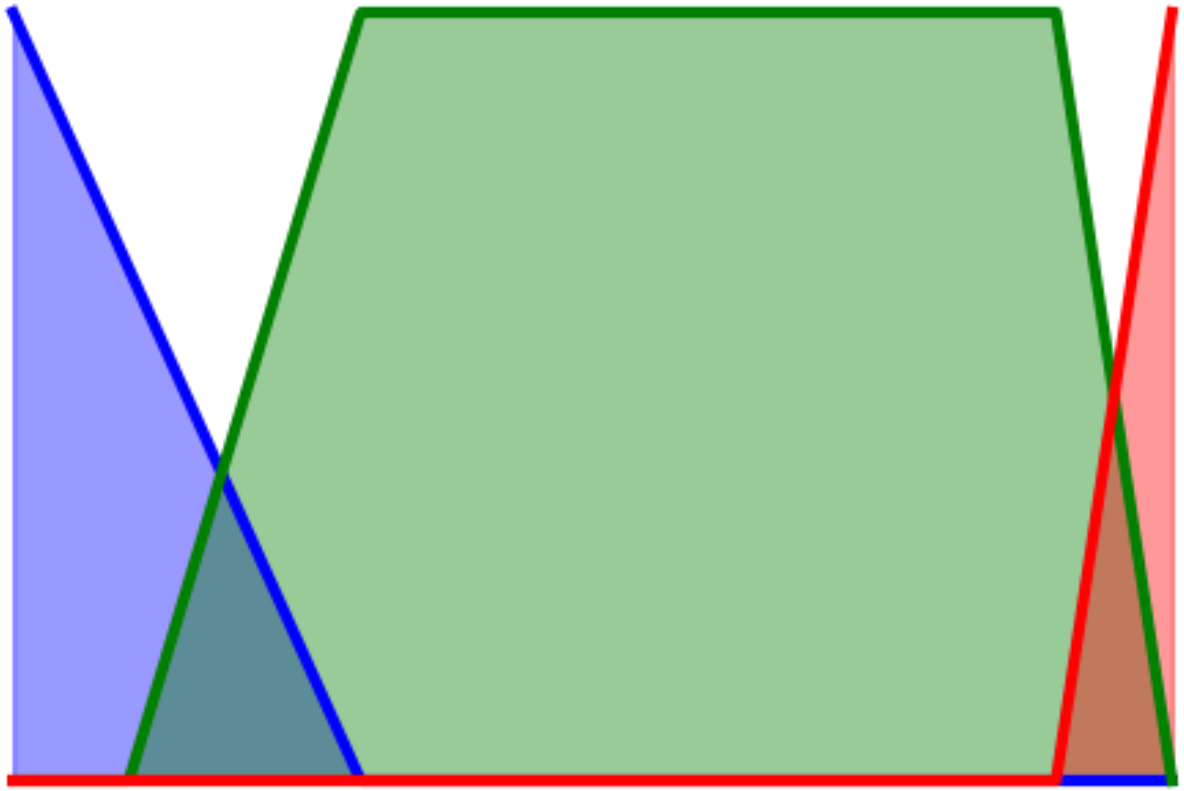
9. Входные переменные модели (V5 – V8)

- $V5$: Осведомленность сотрудников.
- $V6$: Управление информационными активами.
- $V7$: Анализ защищенности инфраструктуры.
- $V8$: Управление рисками и уязвимостями.

10. Фаззификация: термы входных показателей

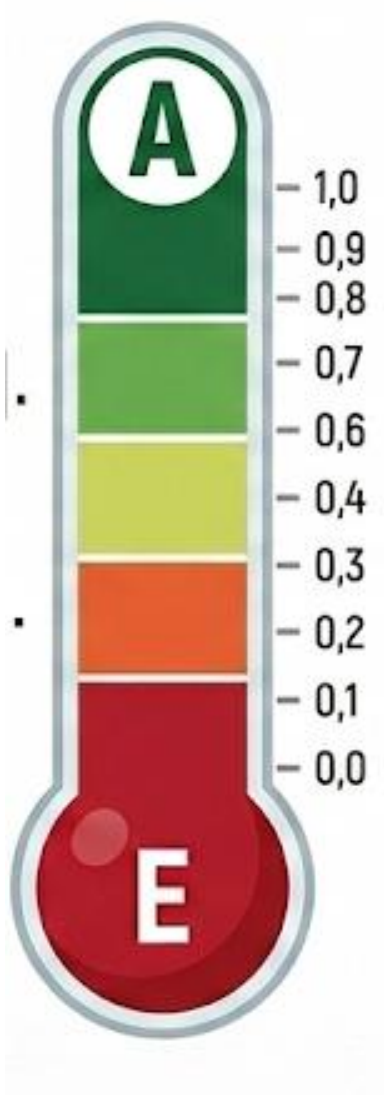
- Однозначные (Да/Нет):
- U (Up) — выполняется ($X_j = 1$).
- D (Down) — не выполняется ($X_j = 0$).

- Неоднозначные (интервалы):
- L (Low) — низкий $[0; 0{,}3]$.
- M (Medium) — средний $[0{,}3;\ 0{,}9]$.
- H (High) — высокий $[0{,}9;\ 1]$.



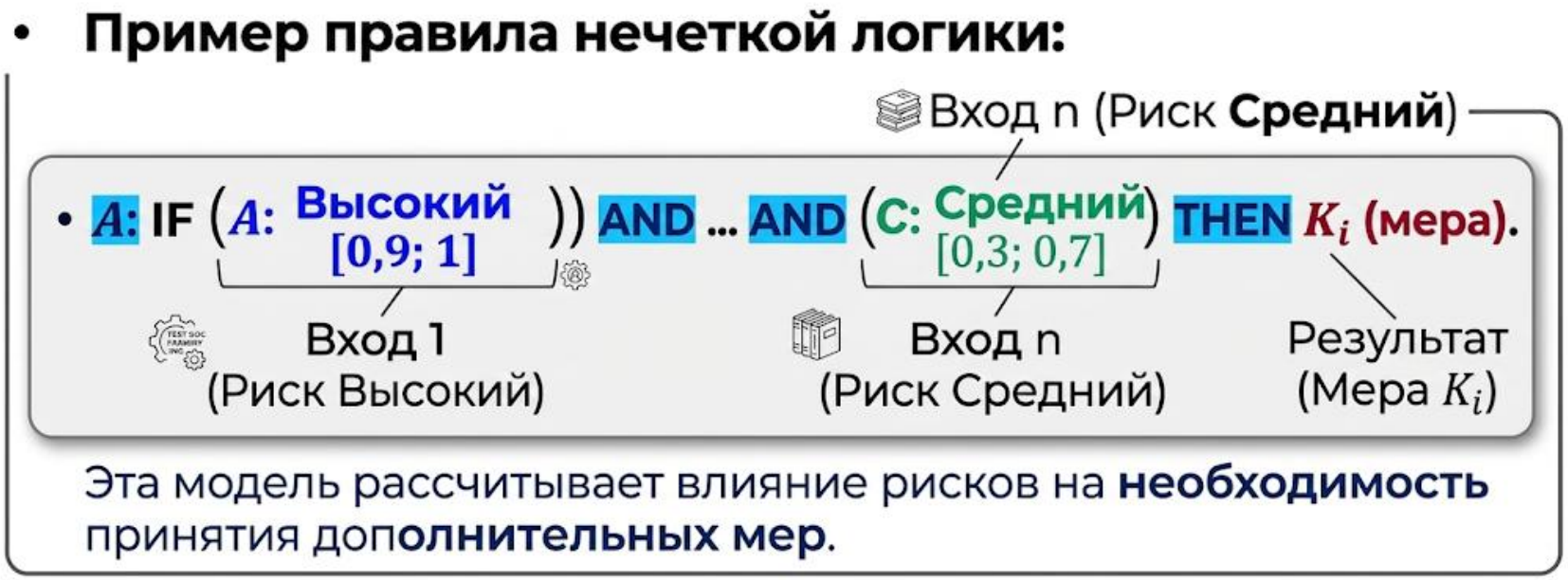
11. Выходные параметры: уровни зрелости ИБ

- A: Высокий $[0{,}9;\ 1]$.
- B: Выше среднего $[0{,}7;\ 0{,}9]$.
- C: Средний $[0{,}3;\ 0{,}7]$.
- D: Ниже среднего $[0{,}1;\ 0{,}3]$.
- E: Низкий $[0;\ 0{,}1]$.



12. Алгоритм нечеткого вывода

- Логика правил:
  ЕСЛИ «Условие» И «Условие» ТОГДА «Следствие»
- Формула:
  K_i: $IF\left(V_1\ IS\ L_1^j\right)AND\ \ldots AND\left(V_n\ IS\ L_i^j\right)THEN\ Y_i = Z_i^j$.
- Модель рассчитывает влияние рисков
  на необходимость принятия дополнительных мер.



13. Пример применения и результат (Case Study)

Входные данные примера:

- Орг. защита $(V1) = U\ (1)$;
- Защита данных $(V2) = D\ (0{,}4)$.
- Инфраструктура $(V3) = B\ (0{,}7)$;
- Мониторинг $(V4) = D\ (0{,}4)$.
- Осведомленность $(V5) = A\ (1)$.

Итоговый результат: $C = 0{,}6\ (60\%)$.

Численные критерии оценки безопасности

Входные параметры					Y
V_1	V_2	V_3	V_4	V_5	
1	0,4	0,7	0,4	1	0,6

14. Анализ результатов примера

- Общая оценка соответствует уровню «Выше среднего».

- Критические точки:
  сфера защиты конфиденциальных данных и процесс мониторинга ИБ.

- Преимущество метода:
  наглядная демонстрация зон,
  требующих немедленных инвестиций и внимания.

15. Заключение и выводы

- Традиционные стандарты перегружены качественными описаниями без цифр.
- Нечеткая логика обеспечивает объективность и высокую детализацию аудита.
- Метод позволяет точно рассчитывать величины рисков и уровни соответствия.