



**УГАТУ**

Уфимский государственный  
авиационный технический  
университет

## Лекция 9

# АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ И НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ



# ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

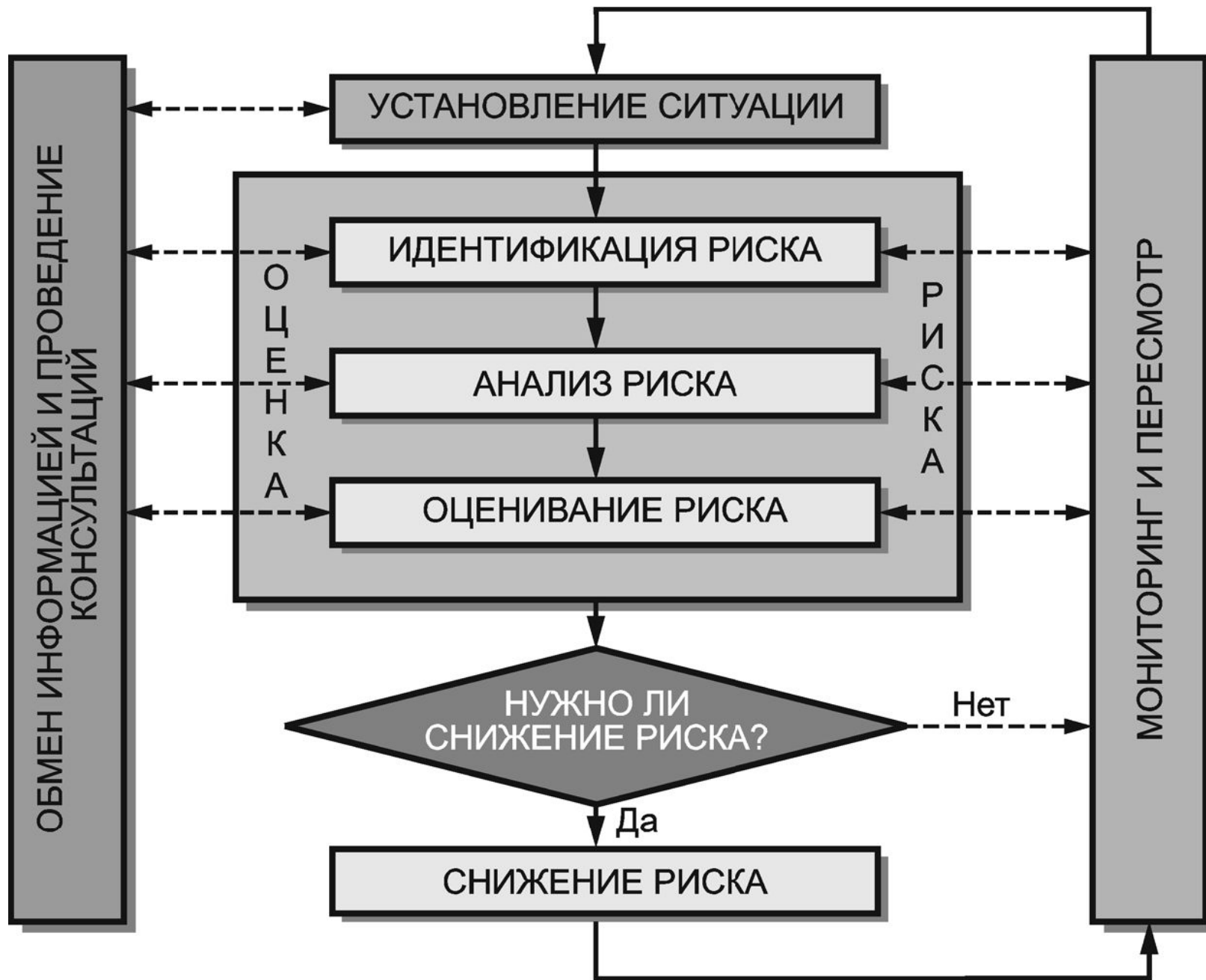
Информационная безопасность (ИБ) – это состояние защищенности информационной среды.

Кибербезопасность – это совокупность методов, технологий и продуктов, предназначенных для защиты целостности сетей, программ и данных от цифровых атак.

Объекты критической информационной инфраструктуры (КИИ) – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления (АСУ) субъектов КИИ.

Риск ИБ – это мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

# АНАЛИЗ И ОЦЕНКА РИСКОВ ИБ



# АРХИТЕКТУРА ПРОМЫШЛЕННОЙ АСУ ТП (ГОСТ Р МЭК 62443-3-3-2015)

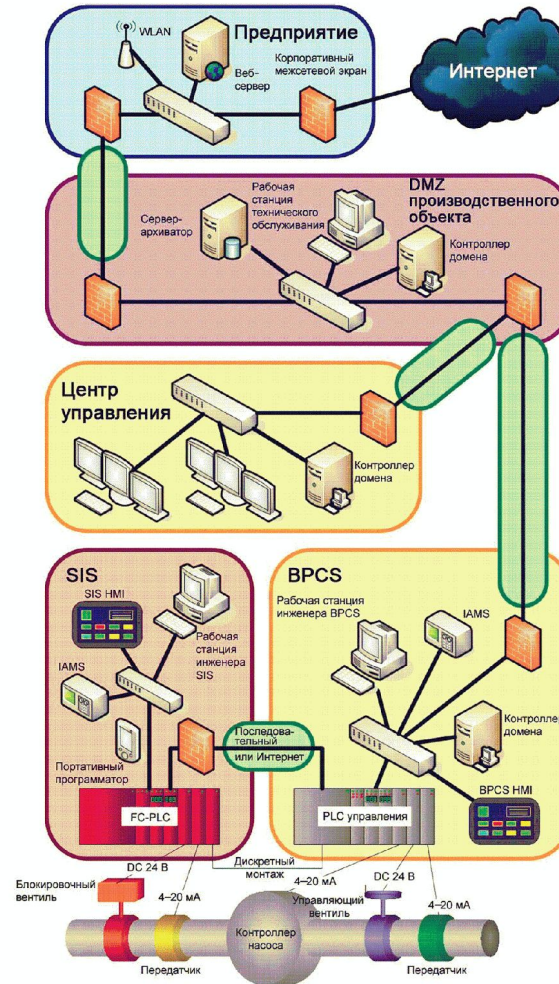


Рисунок А.1 — Общий пример из обрабатывающей промышленности, иллюстрирующий зоны и тракты

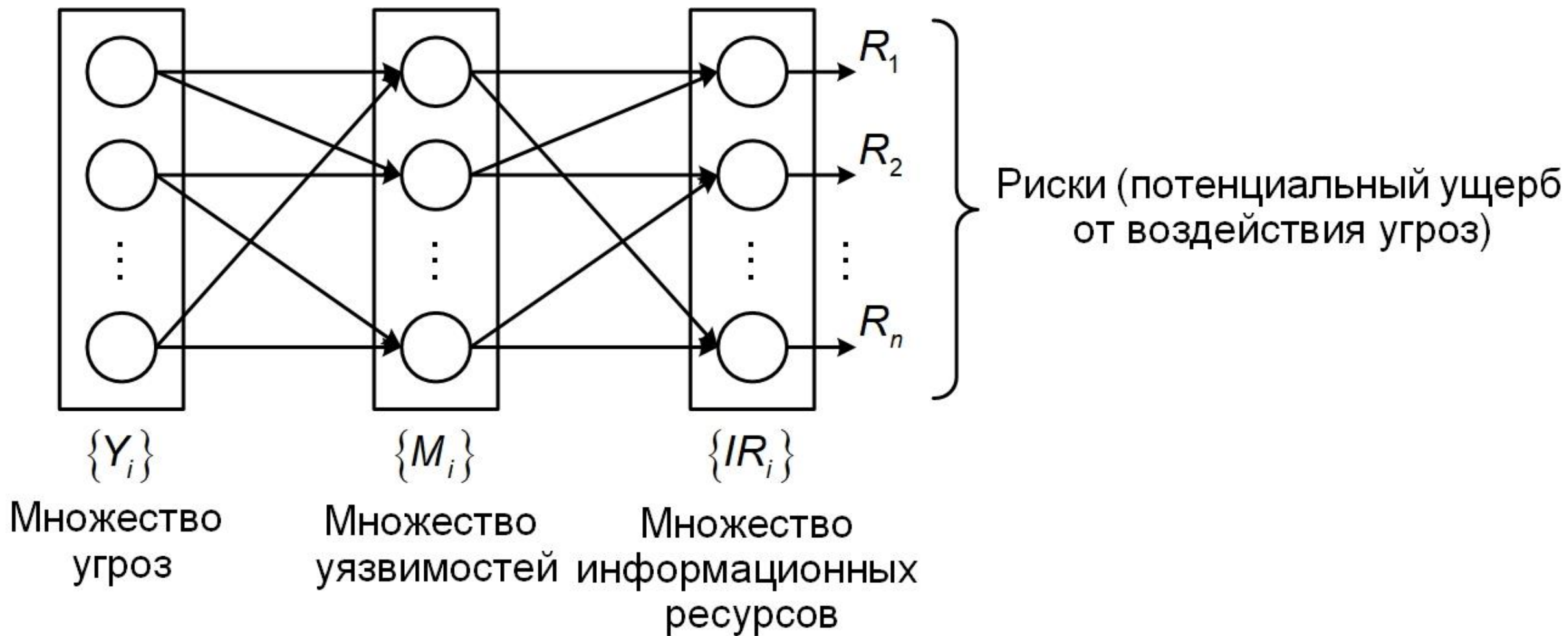
На рисунке А.2 представлено графическое изображение производственного объекта. Он содержит четыре обозначенные зоны: корпоративную сеть, промышленно-корпоративную DMZ и две промышленные сети. Корпоративная инфраструктура включает в себя WLAN и соединение с Интернетом. Многие организации используют DMZ между важными частями их систем, предназначенную для изоляции сетевого трафика. В данном конкретном примере каждая промышленная сеть функционирует относительно независимо от другой промышленной сети и при этом содержит свой PLC, периферийные устройства и HMI.

# ОПРЕДЕЛЕНИЯ

(ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009)

- Зона безопасности – совокупность логических или физических объектов, к которым предъявляются общие требования безопасности.
- Тракт – логическое объединение каналов связи, связывающие между собой две или более зоны безопасности.
- Уровень безопасности – степень необходимой эффективности контрмер и внутренне присущих свойств безопасности устройств и систем для зоны или тракта, основанная на оценке риска для данной зоны или тракта.

# ОБЩАЯ СХЕМА ФОРМИРОВАНИЯ РИСКОВ ИБ (модель Клементса-Хоффмана)



# ФОРМУЛА РИСКА

РИСК = УГРОЗА \* УЯЗВИМОСТЬ \* ИНФОРМАЦИОННЫЙ РЕСУРС

Локальный риск (для  $i$ -го информационного ресурса):

$$R_{i\text{гр}} = f(P_{\text{уязв } i}, P_{\text{ИР } i}, C_{i\text{гр}}), \quad (1)$$

где  $R_{i\text{гр}} = C_{\text{ИР } i} \cdot C_{\text{уязв } i}$ ;  $P_{\text{уязв } i}$  – вероятности появления  $i$ -й угрозы и реализации  $i$ -й уязвимости;  $C_{\text{ИР } i}$  – стоимость (ценность)  $i$ -го ИР;  $C_{i\text{гр}}$  – величина ущерба от реализации  $i$ -й угрозы.

Для совокупности информационных ресурсов:

а) максимальный локальный риск:

$$R_{i\text{max}} = \max_{1 \leq i \leq n} \{R_i\} \quad (2)$$

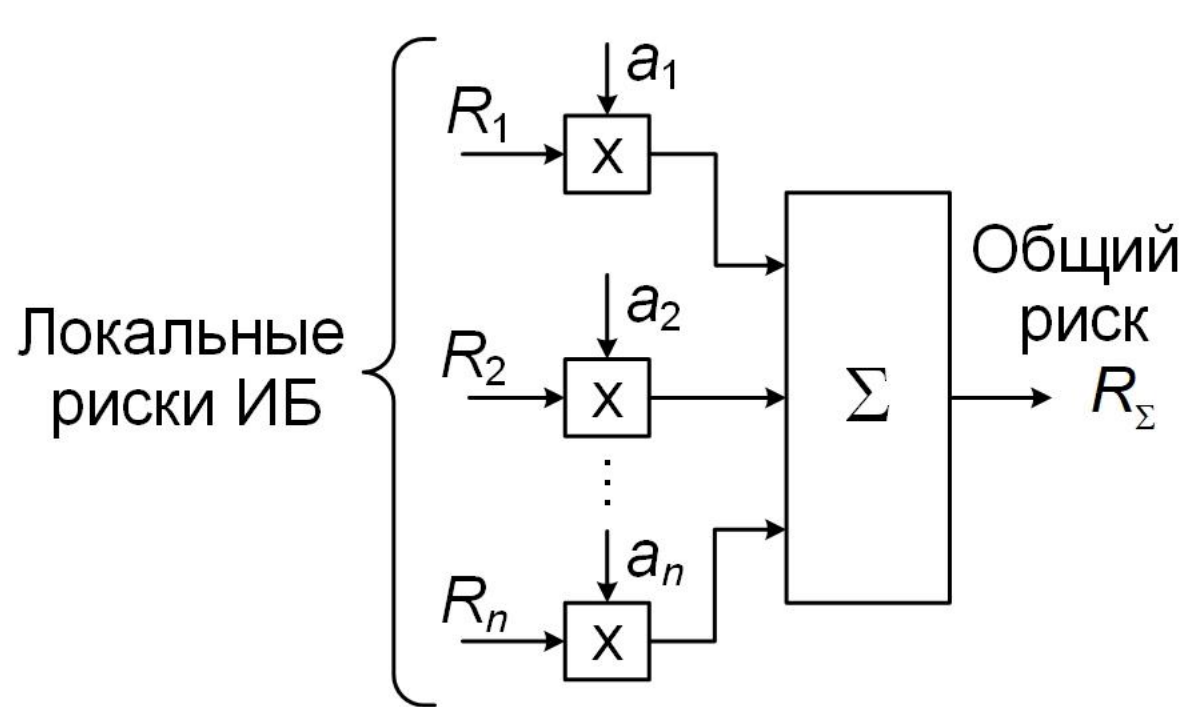
б) общий (суммарный) риск:

$$R_{\Sigma} = \sum_{i=1}^n a_i R_i, \quad (3)$$

где  $a_{\text{ИР } i} = C_{\text{ИР } i} / C_{\Sigma}$  – удельный вес (значимость)  $i$ -го ИР;

$C_{\text{ИР } i} = \sum_{i=1}^n C_{\text{ИР } i}$  – общая стоимость (ценность) всех ИР.

# ВЫЧИСЛЕНИЕ ОБЩЕГО РИСКА ИБ



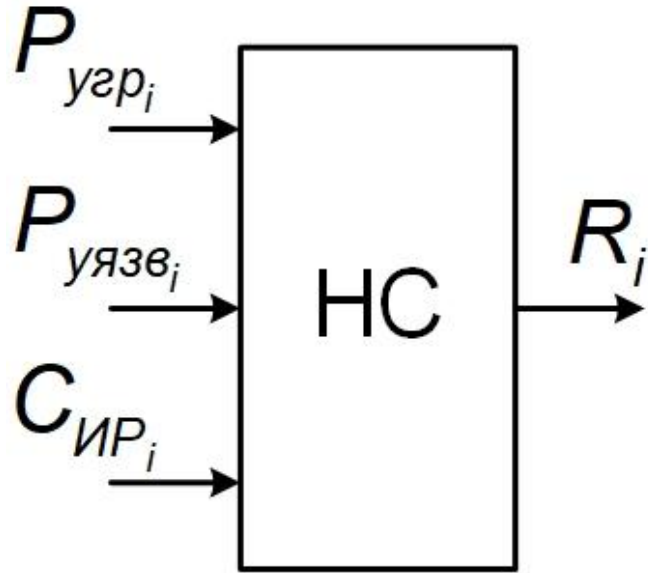
$$\begin{aligned}
 R_\Sigma &= \frac{\sum_{i=1}^n C_{ущ_i}}{C_{ИР_\Sigma}} = \frac{C_{ущ_1}}{C_{ИР_\Sigma}} + \dots + \frac{C_{ущ_n}}{C_{ИР_\Sigma}} = \\
 &= \frac{C_{ущ_1}}{C_{ИР_1}} \cdot \frac{C_{ИР_1}}{C_{ИР_\Sigma}} + \dots + \frac{C_{ущ_n}}{C_{ИР_n}} \cdot \frac{C_{ИР_n}}{C_{ИР_\Sigma}} = \\
 &= a_1 R_1 + \dots + a_n R_n.
 \end{aligned}$$

где  $a_{ИР} = \frac{C_{ИР_i}}{C_{ИР_\Sigma}}$ ;  $C_{ИР_\Sigma} = \sum_{i=1}^n C_i$

Здесь:  $0 \leq R_i \leq 1$ , ( $i = 1, 2, \dots, n$ );  $0 \leq R_\Sigma \leq 1$ ;  $\sum_{i=1}^n a_i = 1$ .



# ОЦЕНКА РИСКОВ ИБ С ПОМОЩЬЮ НС



Варианты построения НС:

- а) многослойный персептрон;
- б) РБФ-сеть;
- в) нейро-нечеткая сеть ANFIS.

Процедура обучения НС:

Подготовка исходных данных

↓  
Построение обучающей выборки

↓  
Выбор архитектуры / структуры НС

↓  
Обучение / тестирование НС

## ДОСТОИНСТВА применения НС для оценки рисков ИБ:

- возможность обучения на реальных данных;
- универсальность (НС – «универсальный аппроксиматор»).

## НЕДОСТАТКИ:

- отсутствие или недостаток реальных данных;
- сложности обучения больших НС («проклятие размерности»);
- непрозрачность, недостаточная интерпретируемость НС.

**ВЫХОД:** применение методов и технологий нечеткого когнитивного моделирования.

# НЕЧЕТКАЯ КОГНИТИВНАЯ КАРТА (Fuzzy Cognitive Map)

– это модель системы (проблемы, ситуации) в форме ориентированного графа, состоящая из 3-х множеств:

$$\text{НКК} = \langle C, F, W \rangle, \quad (1)$$

где  $C = \{C_i\}$  – множество концептов (вершин графа);

$F = \{F_{ij}\}$  – множество связей между концептами (дуг графа);

$W = \{W_{ij}\}$  – множество весов связей;  $i, j = 1, 2, \dots, n$ ,  $n$  – число вершин графа.

Уравнения состояния концептов ( $k = 0, 1, 2, \dots$ ):

$$X_i(k+1) = f \left( X_i(k) + \sum_{j=1}^n W_{ji} X_j(k) \right), \quad (2)$$

где  $X_i(k)$  – переменная состояния концепта  $C_i$ ;  $f(\cdot)$  – функция активации концепта:

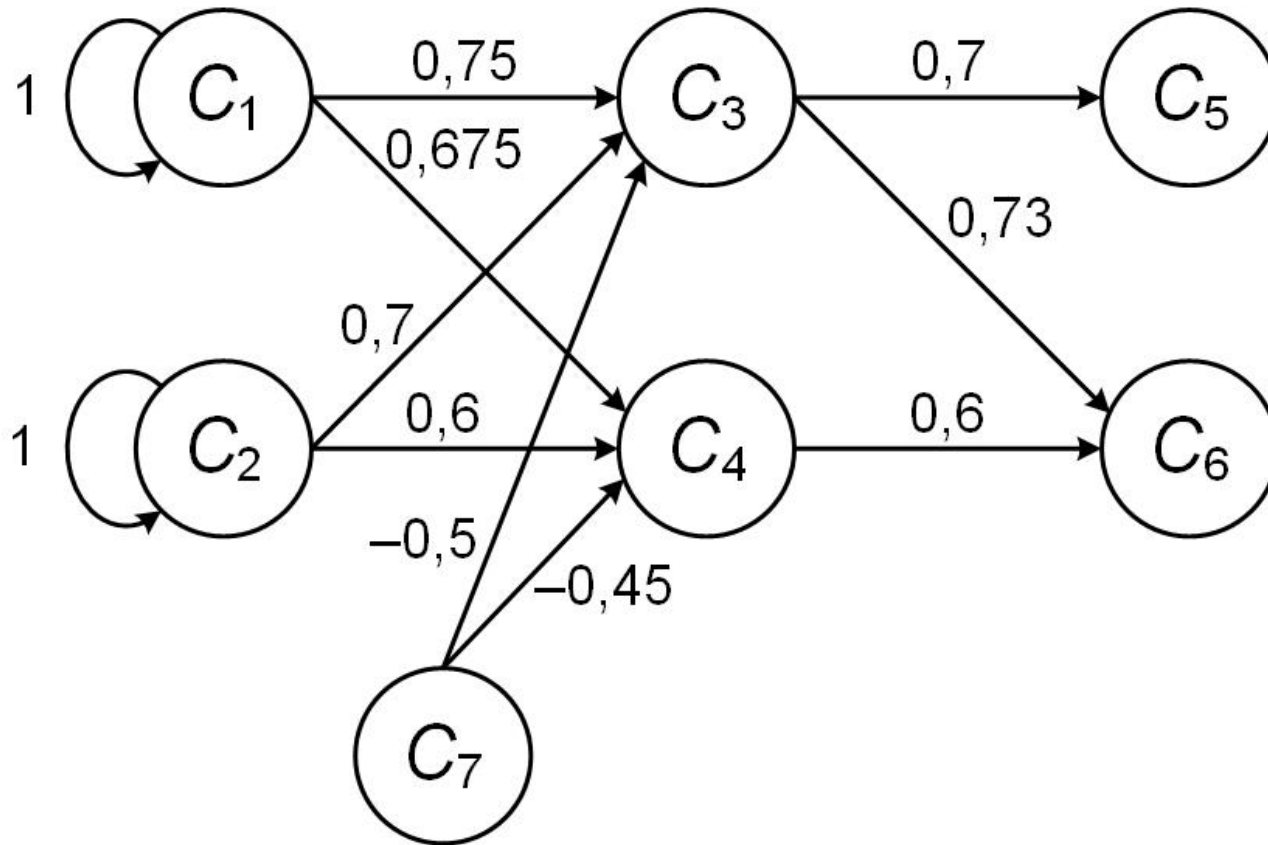
$$f(x) = \frac{1}{1 + e^{-x}}; \quad f(x) = \frac{1 - e^{-x}}{1 + e^{-x}}. \quad (3)$$

# ВЕСА СВЯЗЕЙ НКК

Лингвистическое значение силы связи	Терм	Числовой диапазон
Не влияет	Z	0
Очень слабая	VS	(0; 0,15]
Слабая	S	(0,15; 0,35]
Средняя	M	(0,35; 0,6]
Сильная	H	(0,6; 0,85]
Очень сильная	VH	(0,85; 1]

Z – Zero; VS – Very Small; S – Small; M – Middle; H – High; VH – Very High

# ПРИМЕР ПОСТРОЕНИЯ НКК



Требуется оценить риски нарушения конфиденциальности ( $C_5$ ) и целостности информации, вызванные попыткой НСД ( $C_1$ ) и воздействием вредоносного ПО ( $C_2$ ).

№ концептов	Наименование концептов	Переменные состояния, $X_i$
$C_1$	Попытка НСД к информации	Вероятность возникновения
$C_2$	Вредоносное программное воздействие (ПВ)	Вероятность возникновения
$C_3$	БД, размещенная на сервере	Доля утраченных или искаженных записей, к общему количеству
$C_4$	Электронный документооборот организации	Доля времени на простои или восстановление нормальной работы ЭДО, к общему времени
$C_5$	Ущерб вследствие нарушения конфиденциальности информации	Величина ущерба, в отн. ед.
$C_6$	Ущерб вследствие нарушения целостности информации	Величина ущерба, в отн. ед.
$C_7$	Контрмеры по ЗИ	Стоимость контрмер, в отн. ед.

# СЦЕНАРИИ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

Сценарий А (НСД при отсутствии контрмер по ЗИ):

$$X(0) = (0,9; 0; 0; 0; 0; 0; 0).$$

Сценарий В (Вредоносное ПВ при отсутствии контрмер по ЗИ):

$$X(0) = (0; 0,9; 0; 0; 0; 0; 0).$$

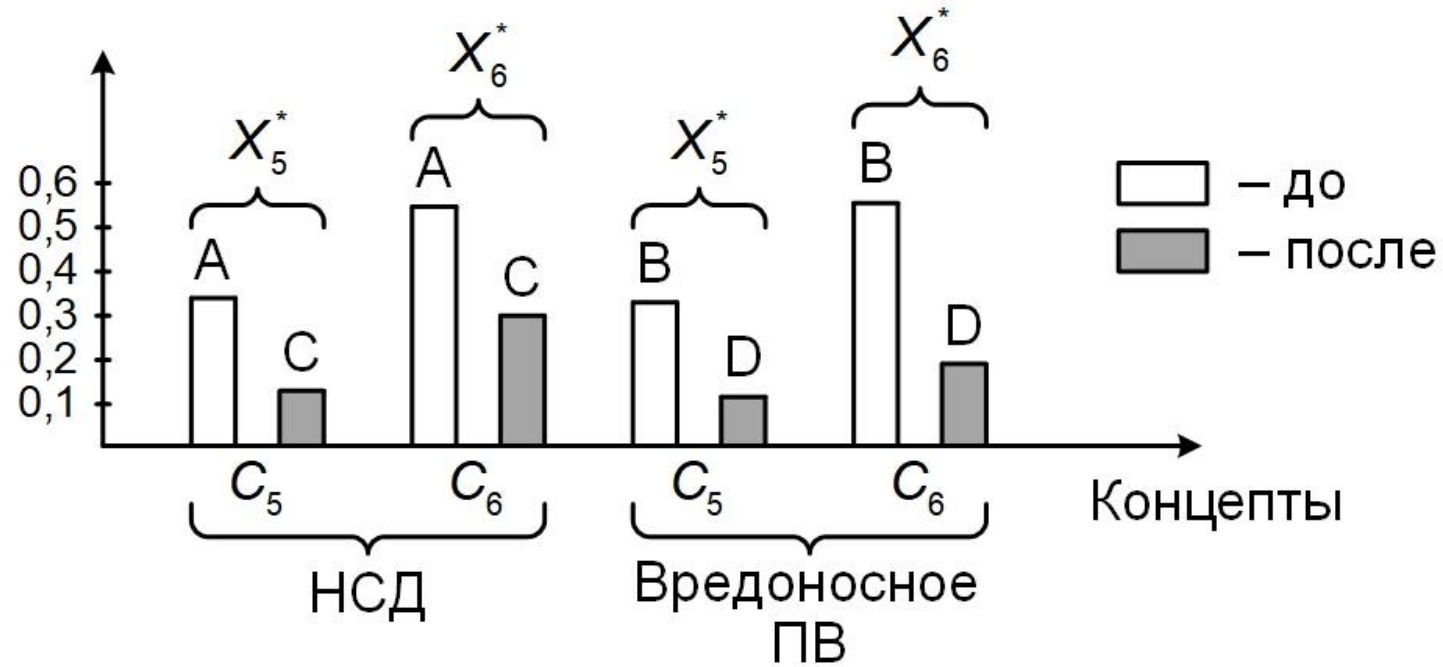
Сценарий С (НСД при использовании контрмер по ЗИ):

$$X(0) = (0,9; 0; 0; 0; 0; 0; 0,9).$$

Сценарий D (Вредоносное ПВ при использовании контрмер по ЗИ):

$$X(0) = (0; 0,9; 0; 0; 0; 0; 0,9).$$

# РИСКИ ИБ (до и после принятия контрмер по ЗИ)



Риски ИБ	НСД		Вредоносное ПО	
	До принятия контрмер	После принятия контрмер	До принятия контрмер	После принятия контрмер
Нарушение конфиденциальности ( $X_5^*$ )	0,34	0,135	0,325	0,12
Нарушение целостности ( $X_6^*$ )	0,555	0,25	0,53	0,195

$X_5^*$ ,  $X_6^*$  – установившиеся значения переменных  $X_5$ ,  $X_6$  (через 8-10 итераций).



# ДРУГИЕ КЛАССЫ НКК



Преимущества НКК по сравнению с НС:

- наглядность;
- прозрачность (интерпретируемость).

Но: субъективность в выборе весов связей НКК.

# ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1. Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт // Информационные технологии, т. 24, № 10, 2018. С. 657-664.
2. Васильев В.И., Вульфин А.М., Гузаиров М.Б., Картак В.М., Черняховская Л.Р. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт // Информационные технологии, т. 26, № 4, 2020. С. 213-221.
3. Васильев В.И., Вульфин А.М., Герасимова И.Б., Картак В.М. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт // Вопросы кибербезопасности, № 2 (36), 2020. С. 11-21.
4. Васильев В.И., Вульфин А.М., Черняховская Л.Р. Анализ рисков инновационных проектов с использованием технологии многослойных нечетких когнитивных карт // Программная инженерия, т. 11, № 3, 2020. С. 142-151.