



**УГАТУ**

Уфимский государственный  
авиационный технический  
университет

## Лекция 7

# СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК НА ОСНОВЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ



ИСКУССТВЕННАЯ ИММУННАЯ СИСТЕМА, ИИС (Artificial Immune System, AIS) – это защитная система, основанная на принципах иммунитета, т.е. обладающая заложенной в нее способностью противостоять внешним чужеродным воздействиям, а также возникшим внутренним аномалиям в поведении системы.

1974 – модель иммунной сети (Н. Ерне)

1990 – иммунная система обнаружения вторжений (С. Форрест, Д. Дасгупта)

1999 – книга “Artificial Immune Systems and Their Applications” (под ред. Д. Дасгупты)

2002 – 1-я Международная конференция по ИИС (ICARIS'2002), Великобритания

# СРАВНИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ ИИС И НС

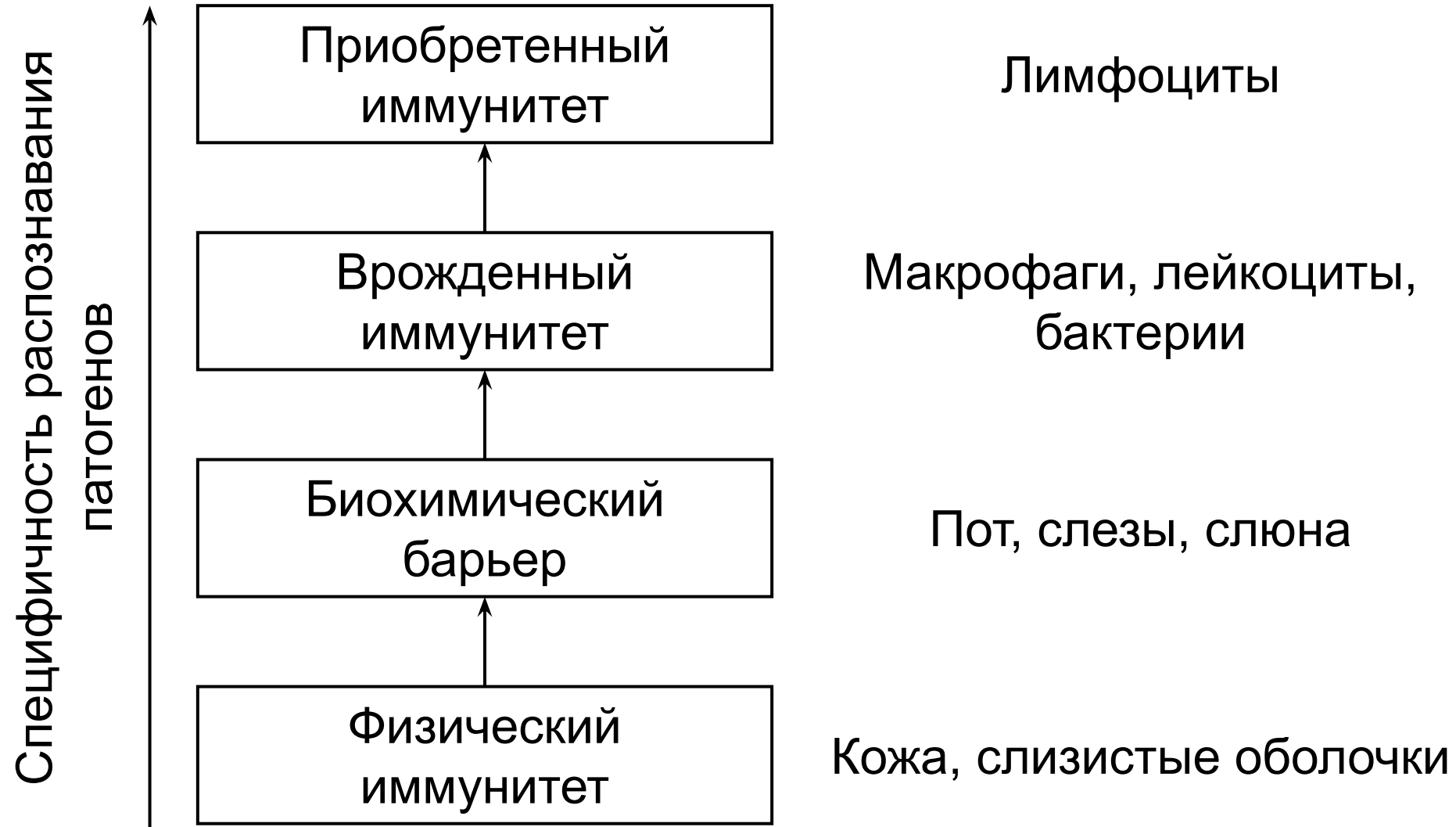
## Сходства ИИС и НС:

- обучение на шаблонах;
- наличие ассоциативной памяти;
- необходимость в предварительной настройке параметров;
- функционирование в условиях неполноты и неопределенности информации.

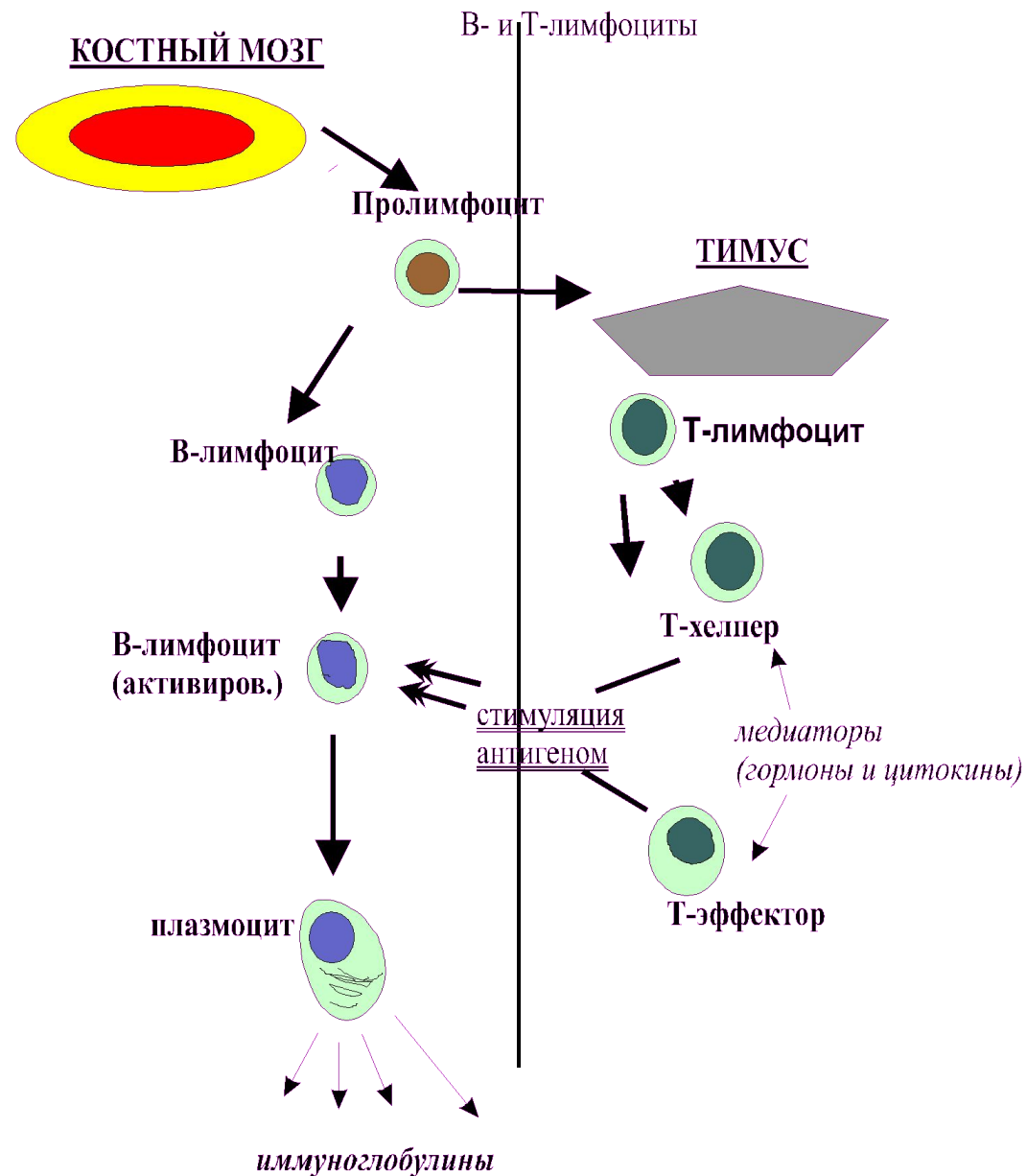
## Отличия ИИС:

- базовые элементы – лимфоциты и антитела;
- количество элементов, их положение и взаимодействие изменяется динамически;
- децентрализация управления;
- самоорганизация поведения.

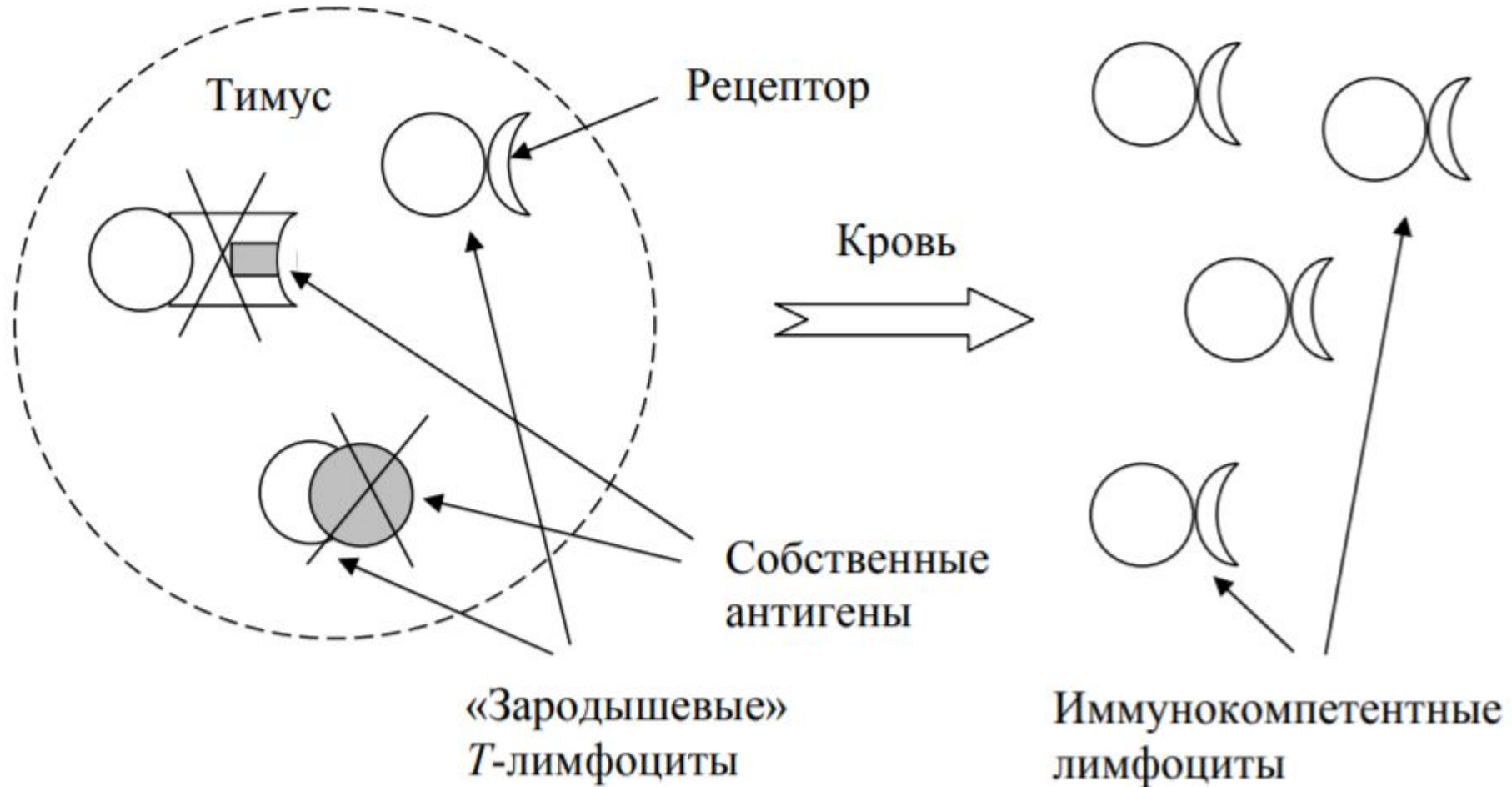
# МЕХАНИЗМЫ ФУНКЦИОНИРОВАНИЯ ИММУННОЙ СИСТЕМЫ ЧЕЛОВЕКА



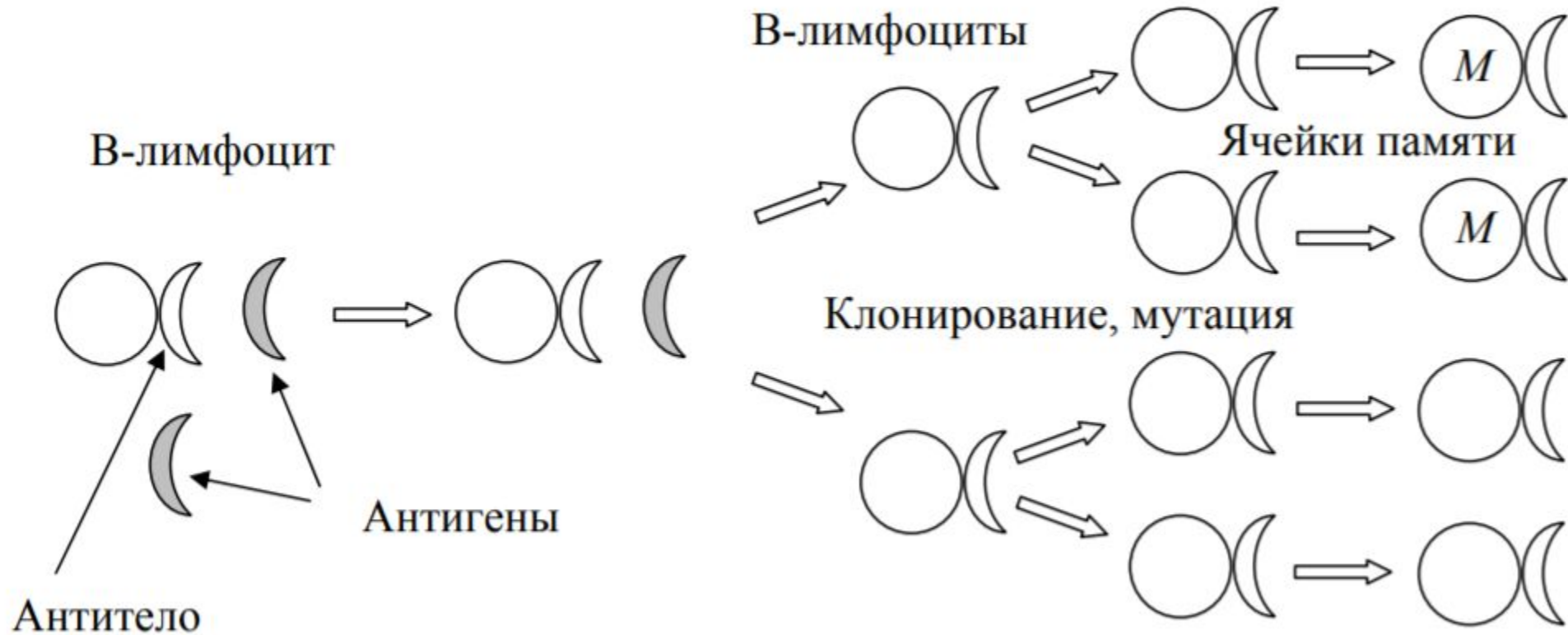
# ОБЩАЯ СХЕМА ФОРМИРОВАНИЯ ПРИОБРЕТЕННОГО (АДАПТИВНОГО) ИММУНИТЕТА



# МЕХАНИЗМ ОТРИЦАТЕЛЬНОГО ОТБОРА (Т-лимфоциты)



# МЕХАНИЗМ КЛОНАЛЬНОЙ СЕЛЕКЦИИ (В-лимфоциты)



# ОБНАРУЖЕНИЕ АНОМАЛИЙ ПРОЦЕССА НА ОСНОВЕ МЕХАНИЗМОВ ИММУННОЙ СИСТЕМЫ

## Этап 1. Сбор исходных данных о работе ИС

Пусть  $S = \{s_1, s_2, s_3, \dots, s_N\}$  временной ряд, составленный из условных номеров (кодов)  $s_1, s_2, s_3, \dots, s_N$  системных вызовов, последовательно выполняемых различными приложениями информационной системы (ИС) на конечном интервале времени при ее нормальной работе.

Способ кодирования:

Системный вызов	Номер $s_i$
Cancel Remove Device	1
Cancel Stop Device	2
Close File	3
...	...
Write File	133



## Этап 2. Формирование шаблонов нормальной активности ИС

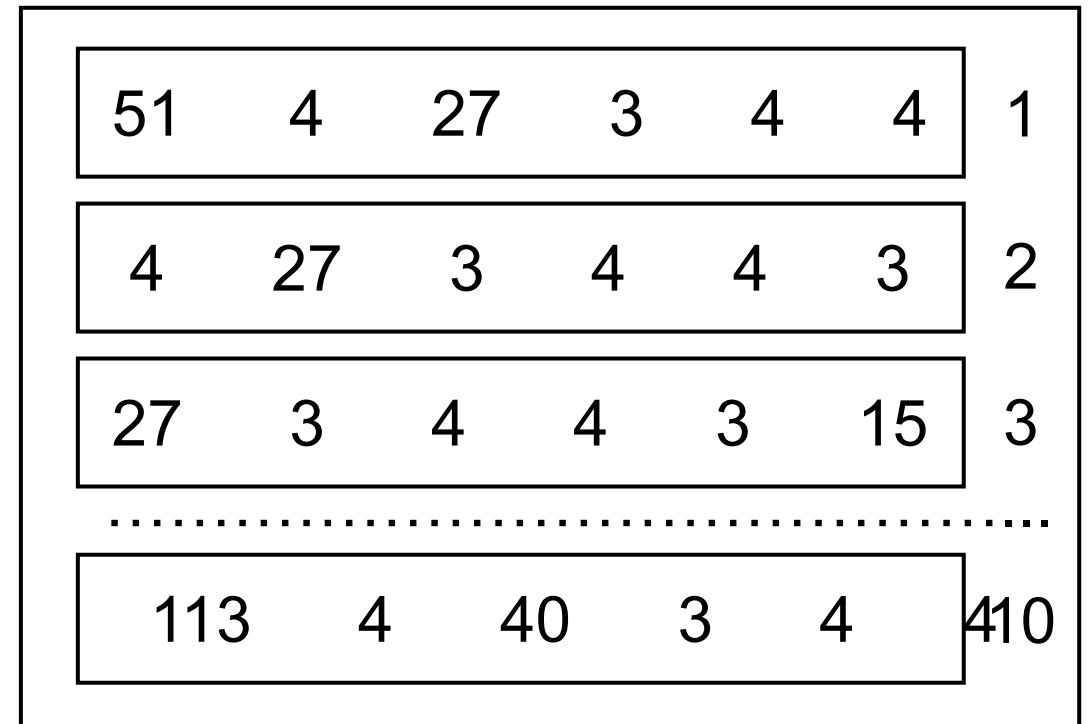
Последовательность системных вызовов:



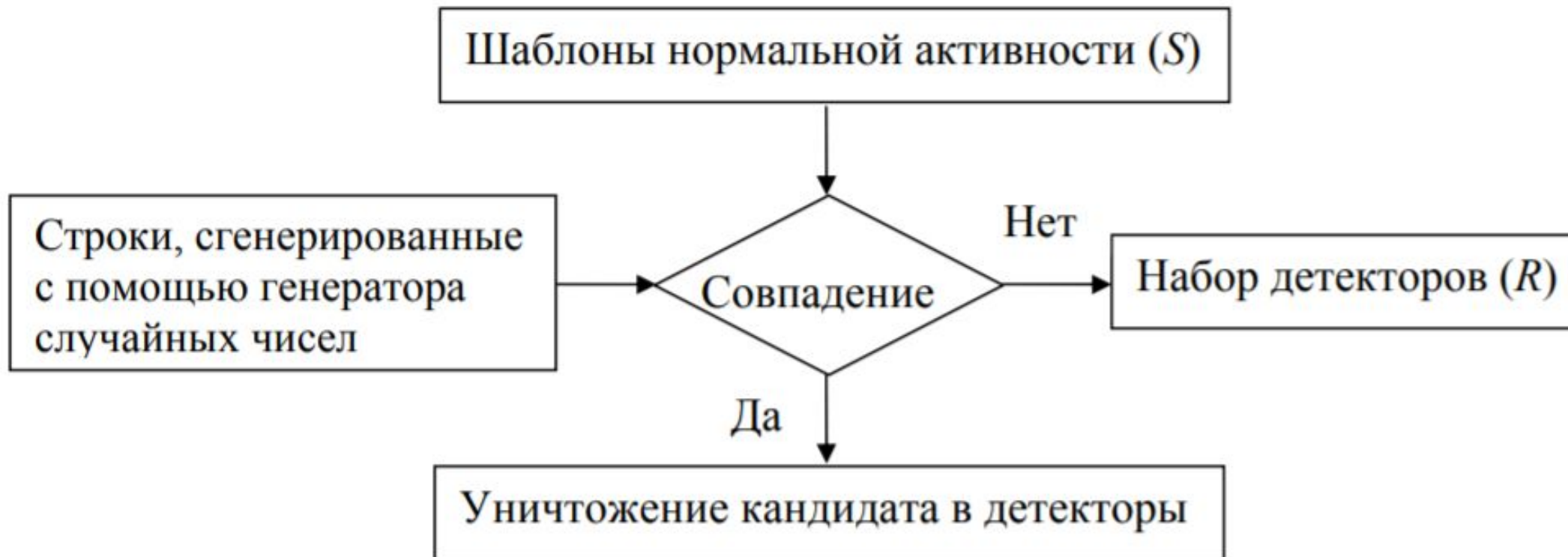
Размер скользящего временного окна:  $n = 6$ ;

Сдвиг временного окна (шаг):  $h = 1$

Набор шаблонов (профилей) нормальной активности:



### Этап 3. Формирование набора детекторов (алгоритм отрицательного отбора)



АФФИННОСТЬ (от лат. *affinitas* – близость, родство) – определяется как число совпадающих смежных элементов 2-х строк: кандидата в детекторы ( $g^{(i)}$ ) и шаблона нормальной активности ( $s^{(j)}$ ):

$$Aff(g^{(i)}, s^{(j)}) = n - d(g^{(i)}, s^{(j)}), \quad (1)$$

где  $d(g^{(i)}, s^{(j)})$  – расстояние Хемминга (число несовпадающих элементов строк  $g^{(i)}$  и  $s^{(j)}$  в идентичных позициях),  $i$  и  $j$  – соответственно номера случайно сгенерированной строки и шаблона ( $n$  – длина строк  $g^{(i)}$  и  $s^{(j)}$ ).

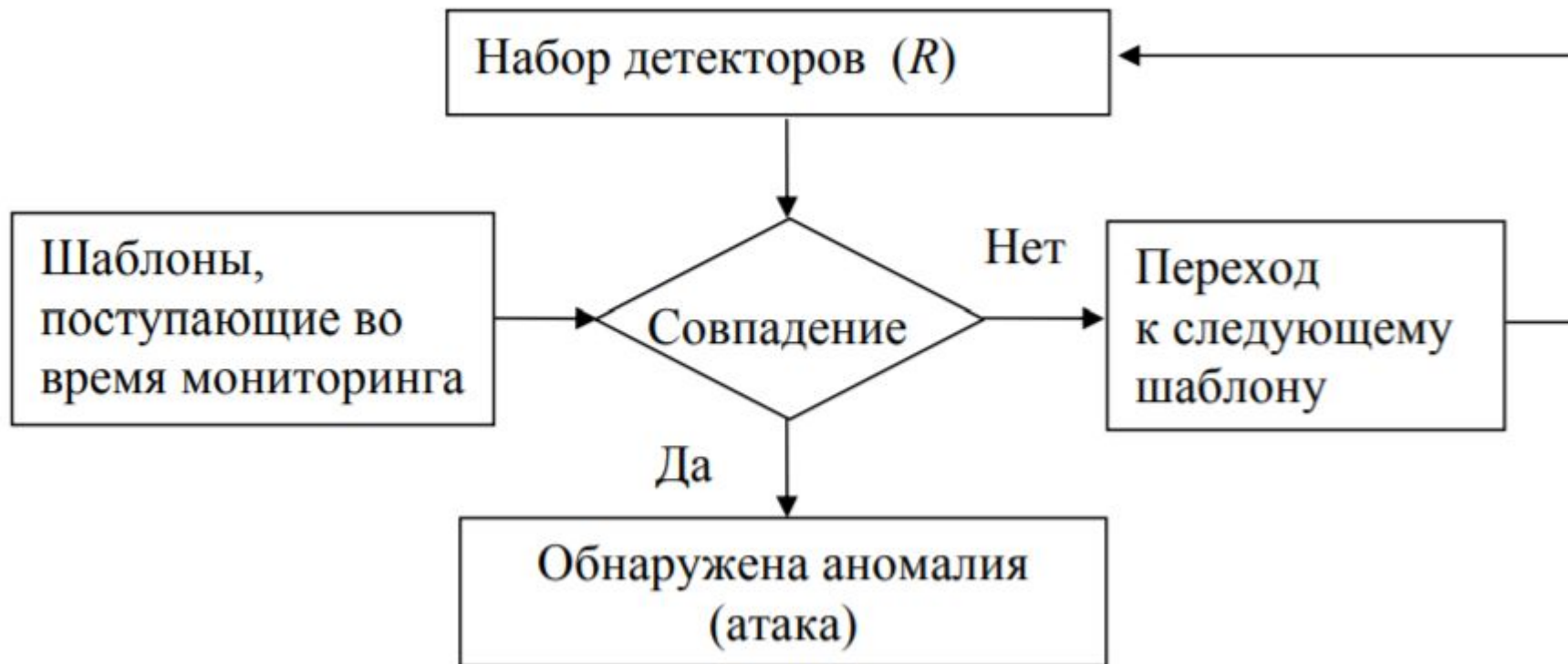
Правило частичного совпадения 2-х строк: строки  $g^{(i)}$  и  $s^{(j)}$  совпадают, если они совпадают по крайней мере в  $r$  идентичных смежных позициях:  $Aff(g^{(i)}, s^{(j)}) \geq r$ , где  $r$  – заданный порог аффинности.

Пример. Дано:  $n = 8$ ;  $r = 5$ ;

$$\begin{aligned} g^{(1)} &= 51 \quad 4 \quad 27 \quad 3 \quad 4 \quad 4 \quad 3 \quad 15 \\ s^{(1)} &= 41 \quad 15 \quad 27 \quad 3 \quad 4 \quad 4 \quad 3 \quad 113 \end{aligned}$$

→ Данные строки совпадают, т.к.  $d(g^{(1)}, s^{(1)}) = 3$ ;  $Aff(g^{(1)}, s^{(1)}) = 8 - 3 = 5 = r$ . 11

## Этап 4. Обнаружение аномалий в поведении процесса



# СХЕМА РАБОТЫ СИСТЕМЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ



# ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1. Брюхомицкий Ю.А. Искусственные иммунные системы в информационной безопасности: учебное пособие, Таганрог: Изд-во Южного федерального ун-та, 2019. 147 с.
2. Васильев В.И., Шамсутдинов Р.Р. Интеллектуальная система обнаружения сетевых атак на основе механизмов искусственной иммунной системы // Моделирование, оптимизация и информационные технологии / Электронный научный журнал, г. Воронеж, том 7, № 1, 2019. [http:// moit.vivt.ru/doi:10.26102/2310-6018/2019.24.1.0101](http://moit.vivt.ru/doi:10.26102/2310-6018/2019.24.1.0101)
3. Сулавко А.Е. Абстрактная модель искусственной иммунной сети на основе комитета классификаторов и ее использование для распознавания образов клавиатурного почерка // Компьютерная оптика, том 44, № 5, 2020. С. 830-844.