Уфимский Государственный Авиационный Технический Университет
Кафедра Вычислительной Техники и Защиты Информации

Подход к обнаружению вторжений на основе модели иммунной системы и иммунокомпьютинга

Вадим Д. Котов

Содержание

1. Ссылки
2. Структура иммунной системы
3. Приобретенный иммунитет
4. Иммунный ответ по клеточному типу
5. Отрицательный отбор
6. Иммунный ответ по гуморальному типу
7. Иммунная сеть
8. Искусственные иммунные системы и иммунокомпьютинг
9. Алгоритм отрицательного отбора.
10. Аффинность
11. Модель костного мозга
12. Алгоритм клональной селекции
13. Классификация систем обнаружения вторжений
14. Модель иммунной системы для обнаружения вторжений
15. Formal Immune Network
16. Классификация с помощью иммунной сети
17. Иммунокомпьютинг в обнаружении вторжений
18. Предлагаемый подход
19. Представление данных
20. Расположение датчиков в сети
21. Эксперименты
22. Результаты
23. Сравнение с классической иммунной моделью
24. Выводы

Ссылки

- **D. Dasgupta, L. F. Nino**, *Immunological Computation. Theory and Applications*. CRC Press, 2009.
- **A. O. Tarakanov,** "Immunocomputing for Intelligent Intrusion Detection" in IEEE Computational Intelligence Magazine, May 2008, pp. 23-30.
- **A. O. Tarakanov** , "Mathematical Models for Intrusion Detection by Intelligent Immunochip" in CCIS (LNCS), vol. 3630, pp. 510-519, 2005
- **A. O. Tarakanov, V. A. Skormin, S. P. Sokolova**, *Immunocomputiong: Principles And Applications.* New-York: Springer, 2003
- **J. Kim, P. Bentley**, "An Artificial Immune Model for Network Intrusion Detection" in 7th European Congress on Intelligent Techniques and Soft Computing (EUFIT'99), 1999
- **J. Kim, P. Bentley**, "The Human Immune System and Network Intrusion Detection". in 7th European Congress on Intelligent Techniques and Soft Computing (EUFIT'99), 1999
- **E. Carter, J. Hogue**, *Intrusion Prevention Fundamentals*. Cisco Press, 2008.
- DARPA Intrusion Detection Evaluation, Available: http://www.ll.mit.edu
- **V. D. Kotov, V. I. Vasilyev** "Artificial Immune Systems Based Intrusion Detection System" Proc. of the 2nd International Conference on Security of Information and Networks, 2009, pp. 207-212.
- **D. Dasgupta** (ed) Artificial Immune Systems And Their Applications, Springer-Verlag, 1999.
- **De Castro L. N., Timmis J**. Artificial Immune Systems: A New Computational Intelligence Approach, Springer-Verlag, 2002.
- **Warrender C., Forrest S., Pearlmutter B.** Detecting Intrusions Using System Calls: Alternative Data Models. Proc. of 1999 IEEE Symposium on Security and Privacy, pp. 133-145, May 1999.
- **Forrest S., Perelson A. S., Allen L., Cherukuri R.** Self-nonself discrimination in a computer, Proc. of 1994 IEEE Symposium on Research in Security and Privacy, pp. 202-212, May 1994.

Структура иммунной системы

Кожа

Биохимический барьер

- Пот
- Слюна
- Слезы

Врожденный иммунитет

- Сдерживание инфекции
- Воспаление

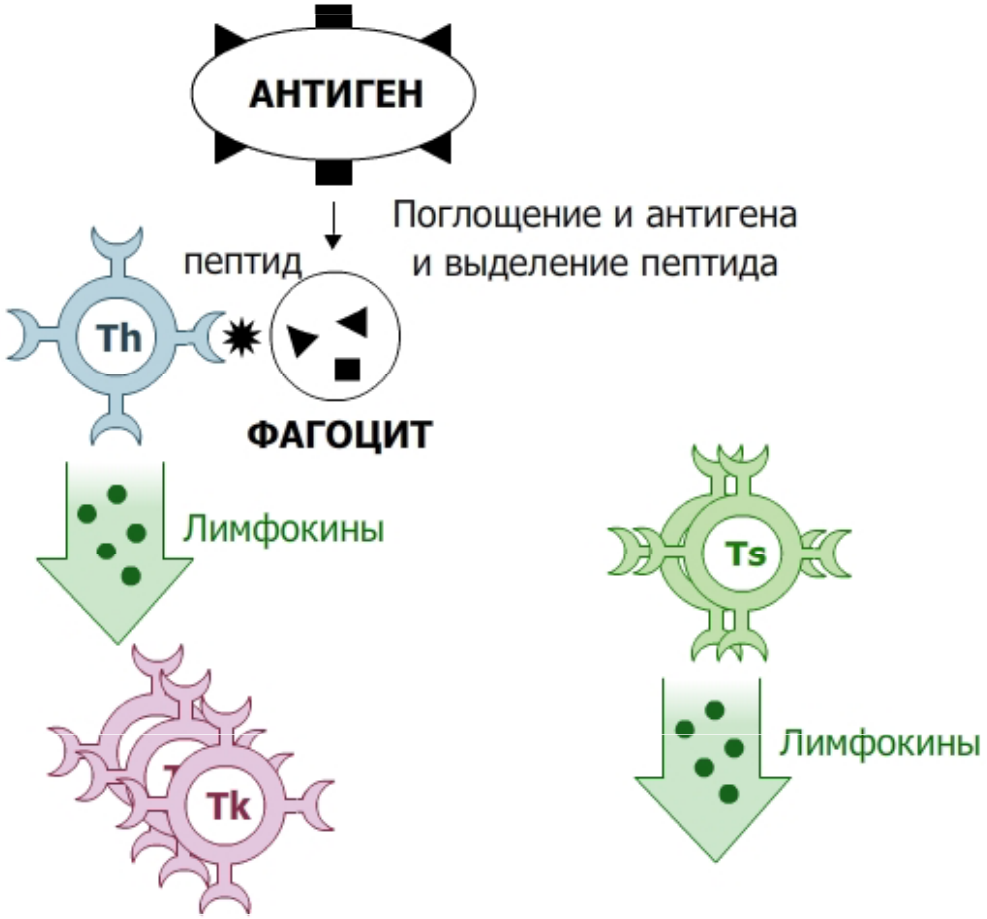
Приобретенный иммунитет

- Уничтожение вредоносных организмов
- Иммунная память для быстрого ответа на подобные инфекции

Приобретенный иммунитет

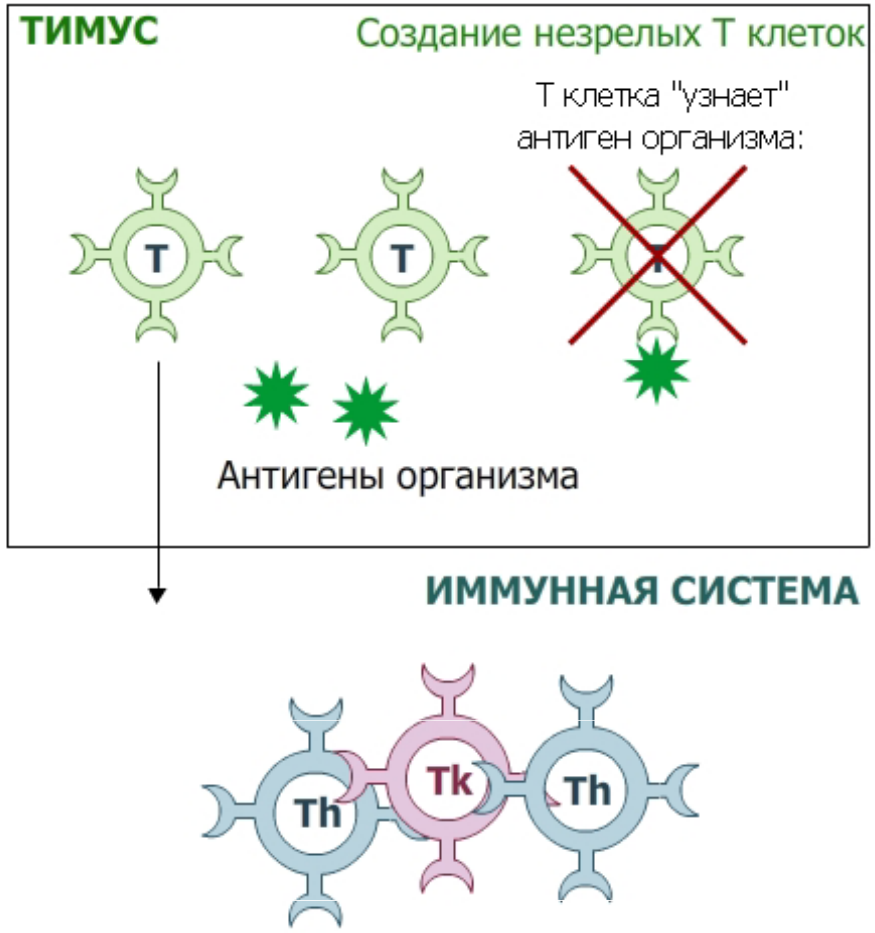
Свойства приобретенного иммунитета	Основные участники	Типы иммунного ответа
Специфичность иммунного ответа – способность лимфоцитов распознавать определенные антигены	*Т-лимфоциты* (киллеры, хелперы, супрессоры)	*По клеточному* (основные участники – Т-лимфоциты)
Иммунная память – способность осуществлять быстрый иммунный ответ при повторной встрече с известным антигеном	*В-лимфоциты* (В-лимфоциты, плазмациты, клетки памяти)	*По гуморальному типу* (основные участники – В-лимфоциты)
Саморегуляция –способность к активации и подавлению иммунного ответа	*Свободные антитела* (рецепоторы В-лимфицита, покинувшие его поверхность)	
	Лимфокины - вещества активирующие или подавляющие иммунный ответ	

Иммунный ответ по клеточному типу

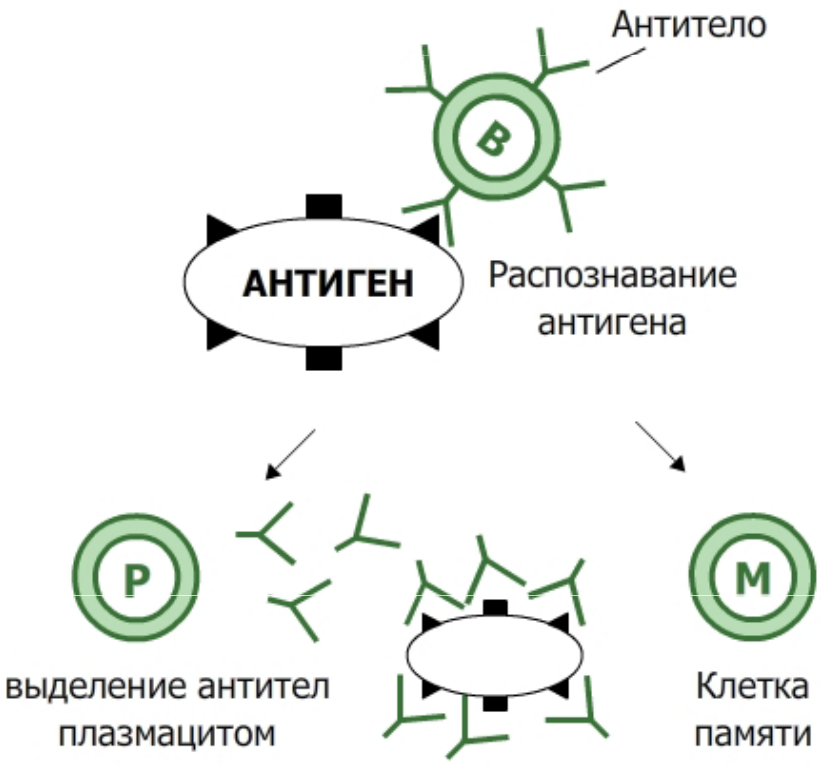


1. Фагоцит поглощает антиген;
2. Фагоцит переваривает поглощенный антиген и выделяет из него пептид;
3. Пептид презентуется на поверхности фагоцита;
4. Т-хелпер распознает пептид
5. Т-хелпер выделяет лимфокины, активирующие Т-киллеров;
6. Т-киллеры уничтожают зараженные клетки;
7. Т-супрессоры выделяют лимфокины, подавляющие иммунный ответ.

Отрицательный отбор

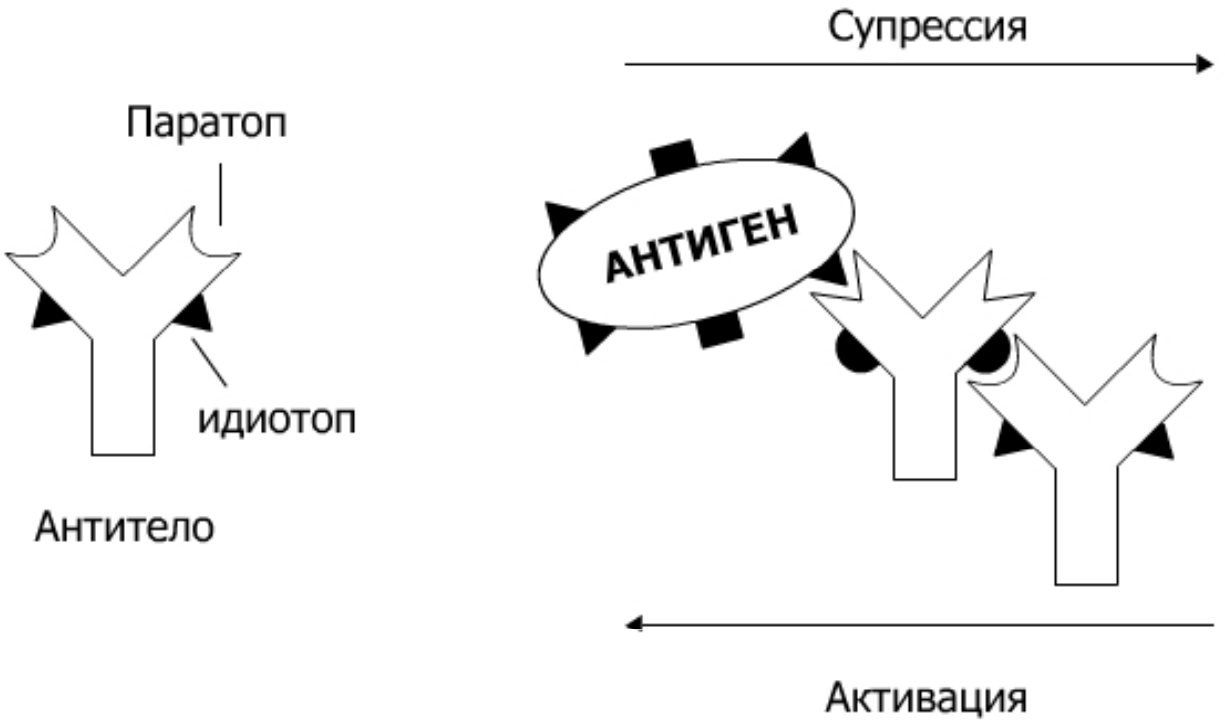


Иммунный ответ по гуморальному типу



1. В-лимфоцит «узнает» антиген;
2. В-лимфоцит размножается, антитела на поверхности клонов претерпевают мутации;
3. Часть клеток выделяет антитела со свей поверхности (они становятся плазмацитами);
4. После иммунного ответа часть лимфоцитов умирает;
5. В-лимфоциты лучше «узнающие» антигены становятся клетками памяти и сохраняются примерно год (клональная селекция).

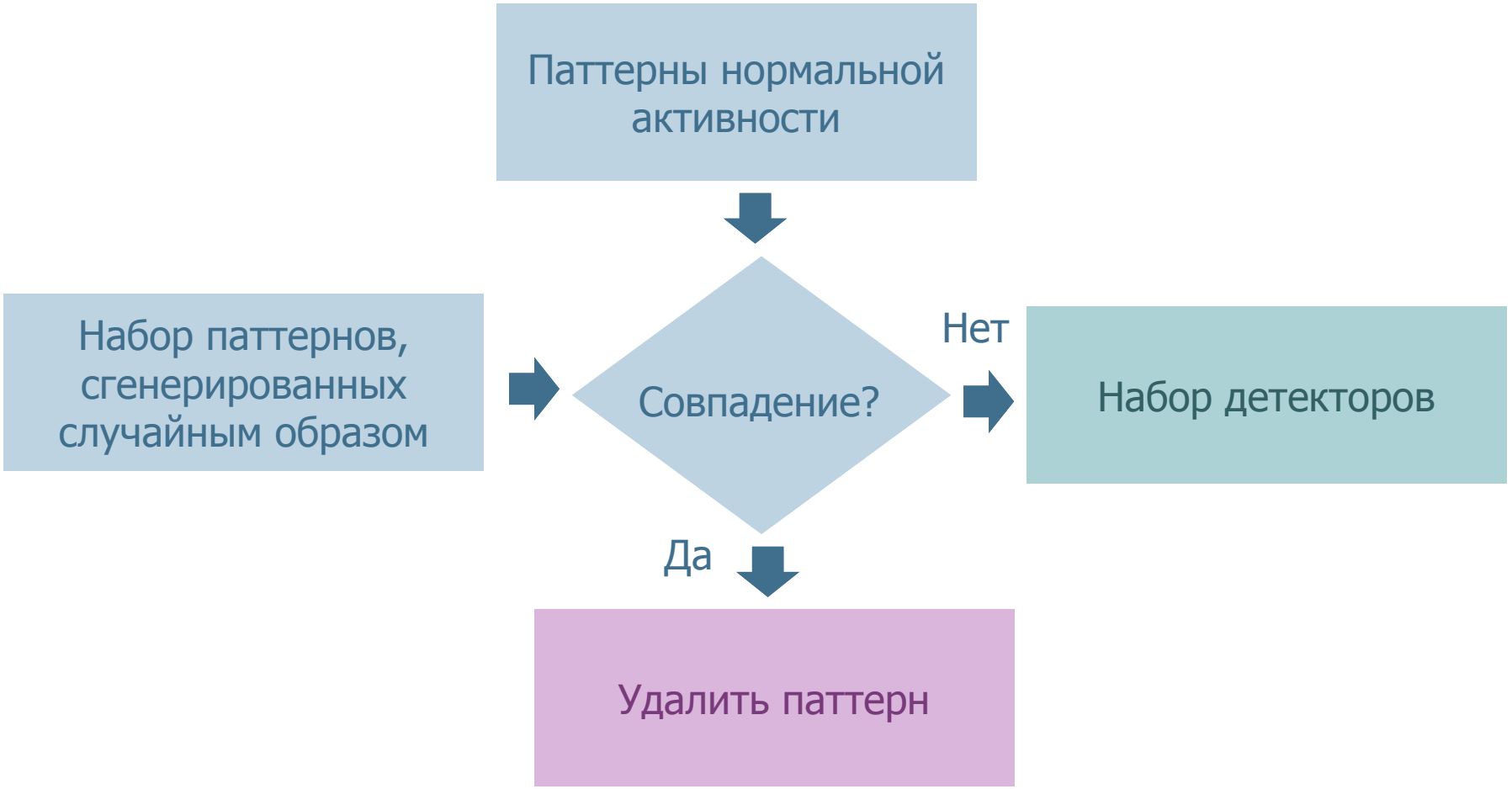
Иммунная сеть



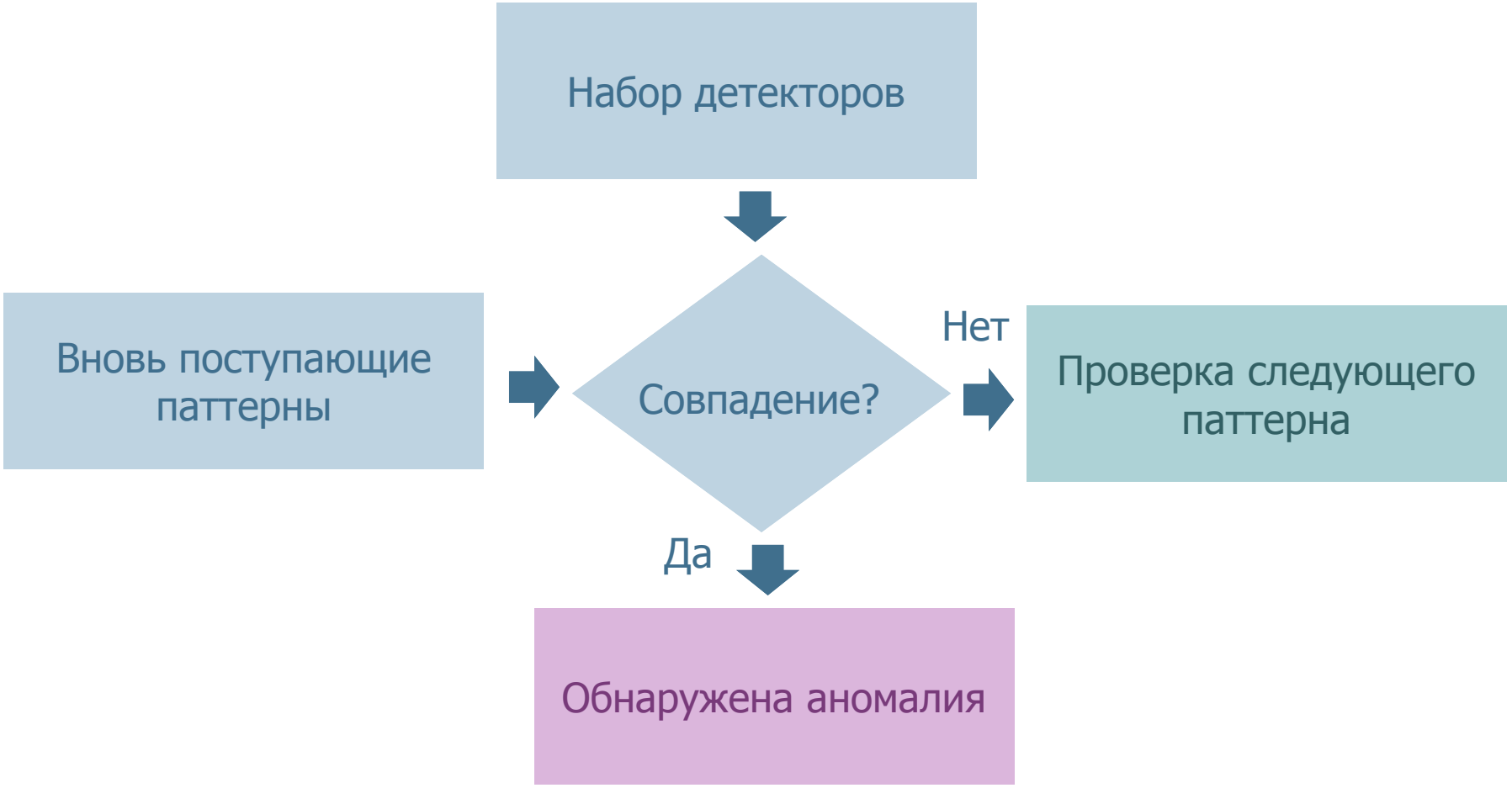
Искусственные иммунные системы и иммунокомпьютинг

Иммунная система	Компьютерная имплементация
Отрицательный отбор Т-лимфоцитов →	Алгоритм отрицательного отбора
Клональная селекция В-лимфоцитов →	Алгоритм клональной селекции
Иммунная сеть →	Формальная иммунная сеть (FIN, Formal Immune Network)

Алгоритм отрицательного отбора. Генерирование детекторов



Алгоритм отрицательного отбора.Обнаружение аномалий



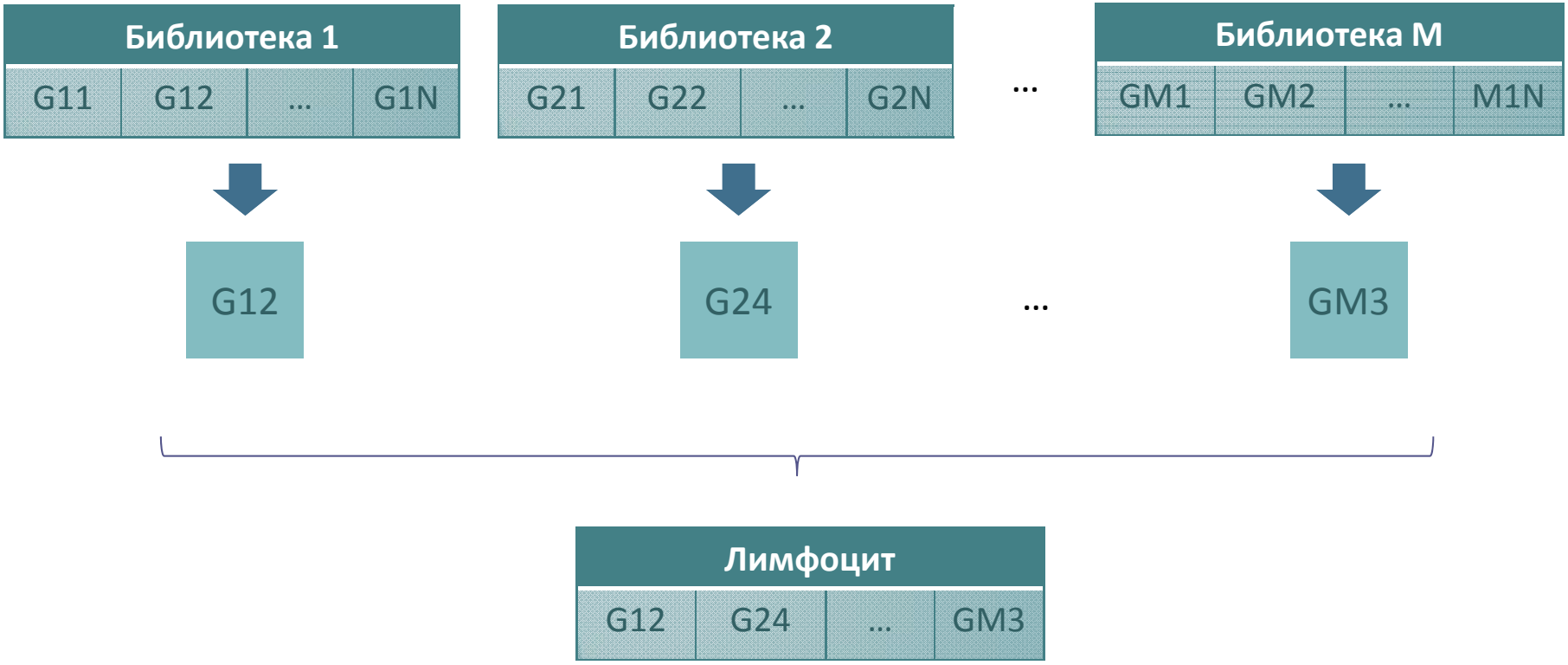
Аффинность

Аффинность – степень соответствия между антигеном и лимфоцитом.

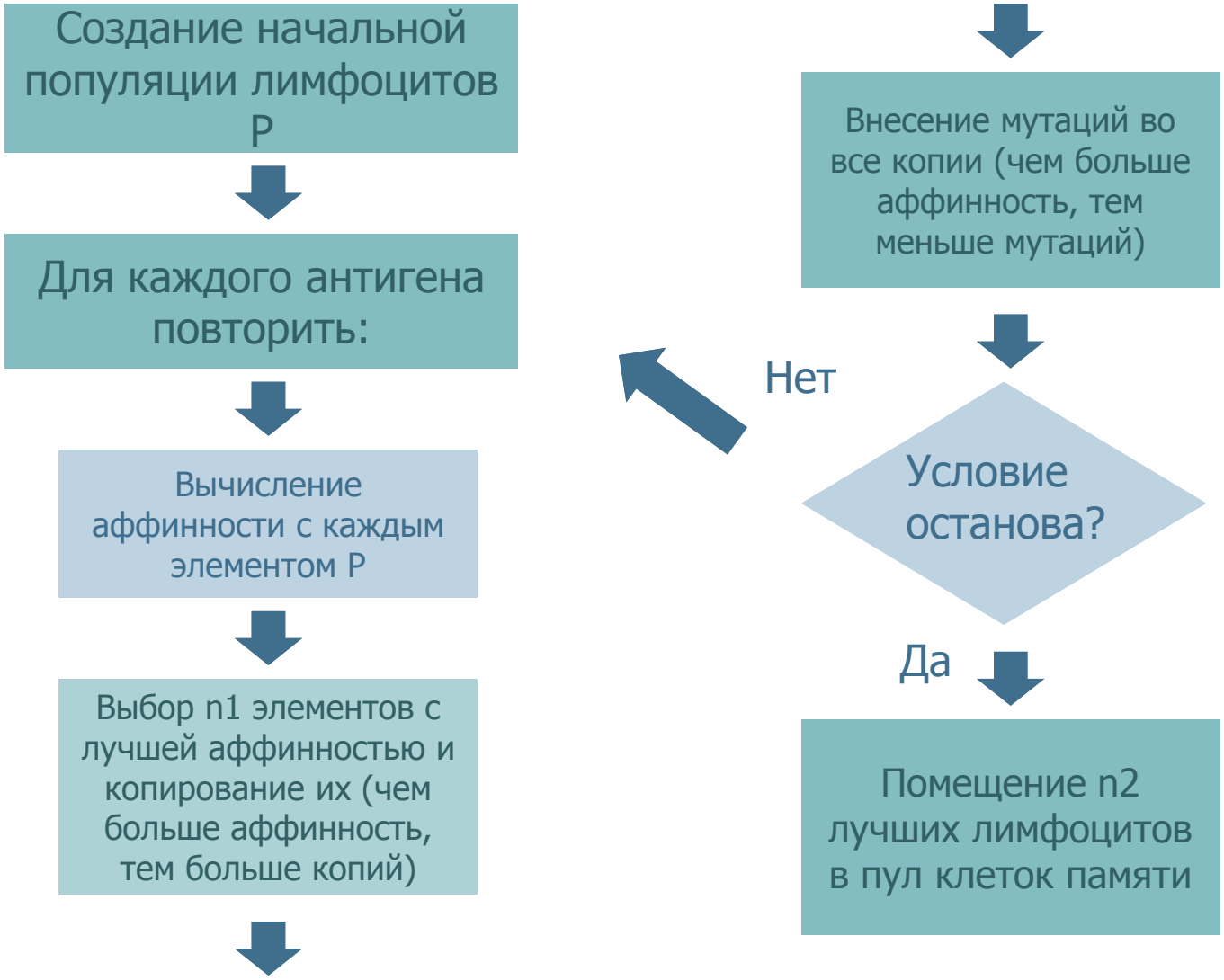
Используемые виды аффинности:

Правило r-смежных совпадений	Расстояние по Хэммингу	Расстояние по Чебышеву
• Аффинность равна максимальному числу совпадений в смежных позициях двух паттернов	• Аффинность равна числу совпадающих элементов в одинаковых позициях	• Аффинность равна наибольшему модулю разности элементов паттернов
1**242**33043 3**242**14246 Аффинность = 3	1**242**3304**3** 3**242**1424**6** Аффинность = 4	12423304**3** 32421424**6** |3-6|=3 Аффинность = 3

Модель костного мозга



Алгоритм клональной селекции



Классификация систем обнаружения вторжений

Системы обнаружения вторжений

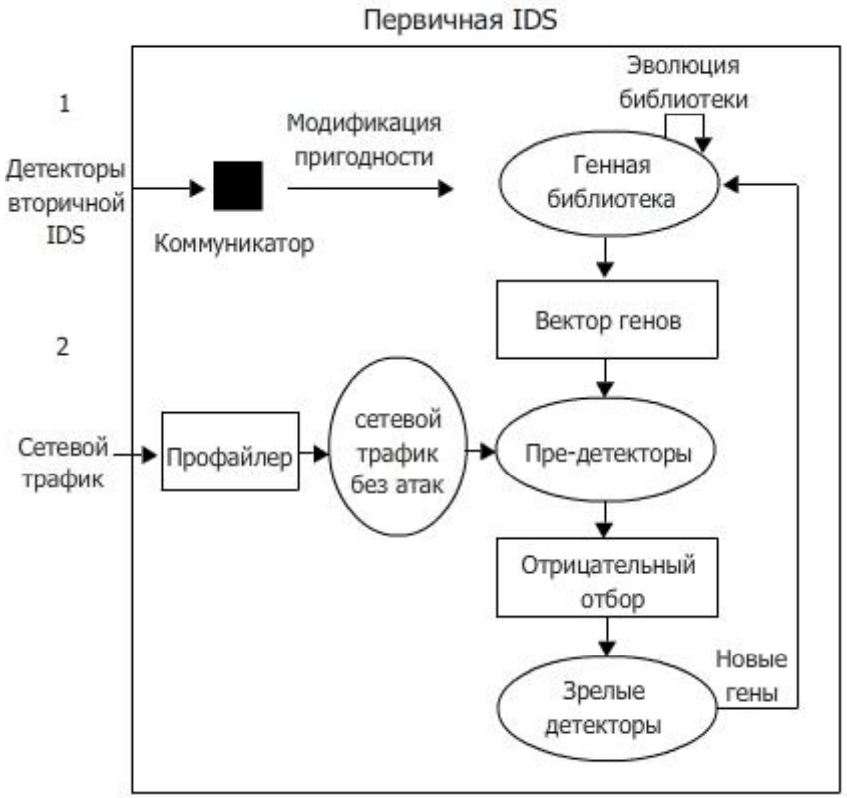
По способу обнаружения

- Поведенческие
  - Статистические средства, методы искусственного интеллекта
- Сигнатурные
  - Поиск совпадений по шаблонам известных вторжений

По типу мониторинга

- Узловые
  - Мониторинг одного компьютера
- Сетевые
  - Мониторинг сетевого трафика

Модель иммунной системы для обнаружения вторжений



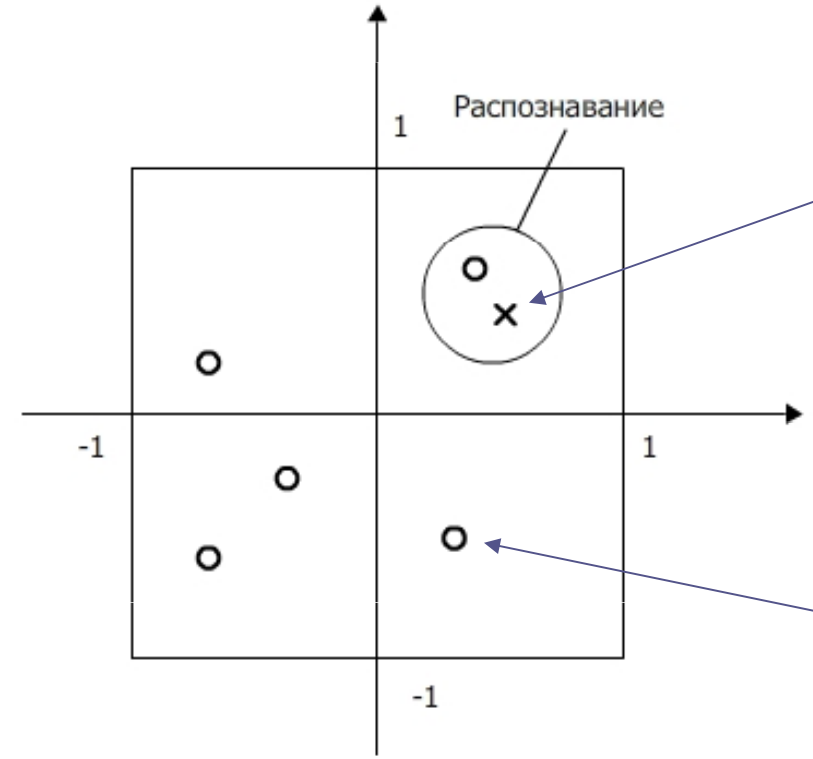
Клональная селекция

Вторичная IDS

Formal Immune Network

Формальная иммунная сеть (FIN)	Набор клеток FIN=(V_1…V_m)
Клетка, V	V=(c(V),P(V)), c(V) – класс клетки, P(V) – точка в Евклидовом пространстве
Расстояние между клетками, d	Расстояние по Чебышеву
Распознавание клетки V1 клеткой V2	Если c(V1)=c(V2) и d(V1, V2) < dmin, то клетка V1 «узнает» V2
Апоптоз	Если V_1 узнает V_2, то V_1 удаляется из FIN
Иммунизация	Если V_1 ближайшая к V_2 среди остальных клеток, но классы этих клеток различны, то V_1 добавляется в FIN

Классификация с помощью иммунной сети

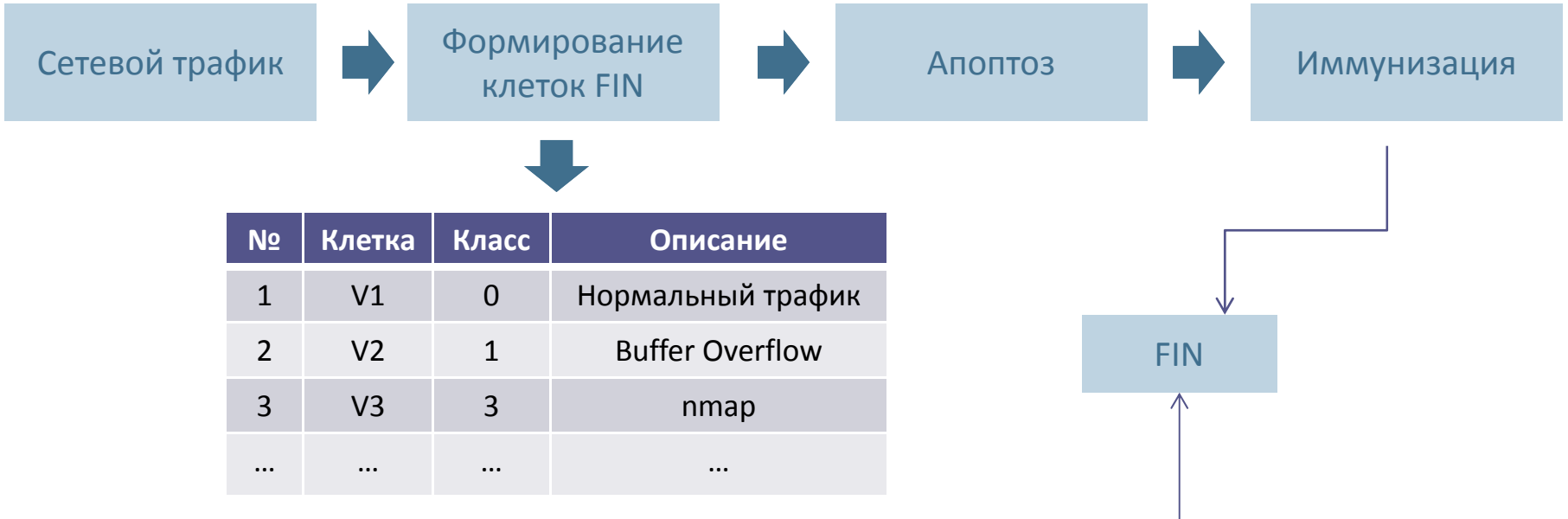


Вновь поступившему антигену назначается класс ближайшей к нему клетки FIN

Каждой клетке FIN соответствует класс

Иммунокомпьютинг в обнаружении вторжений

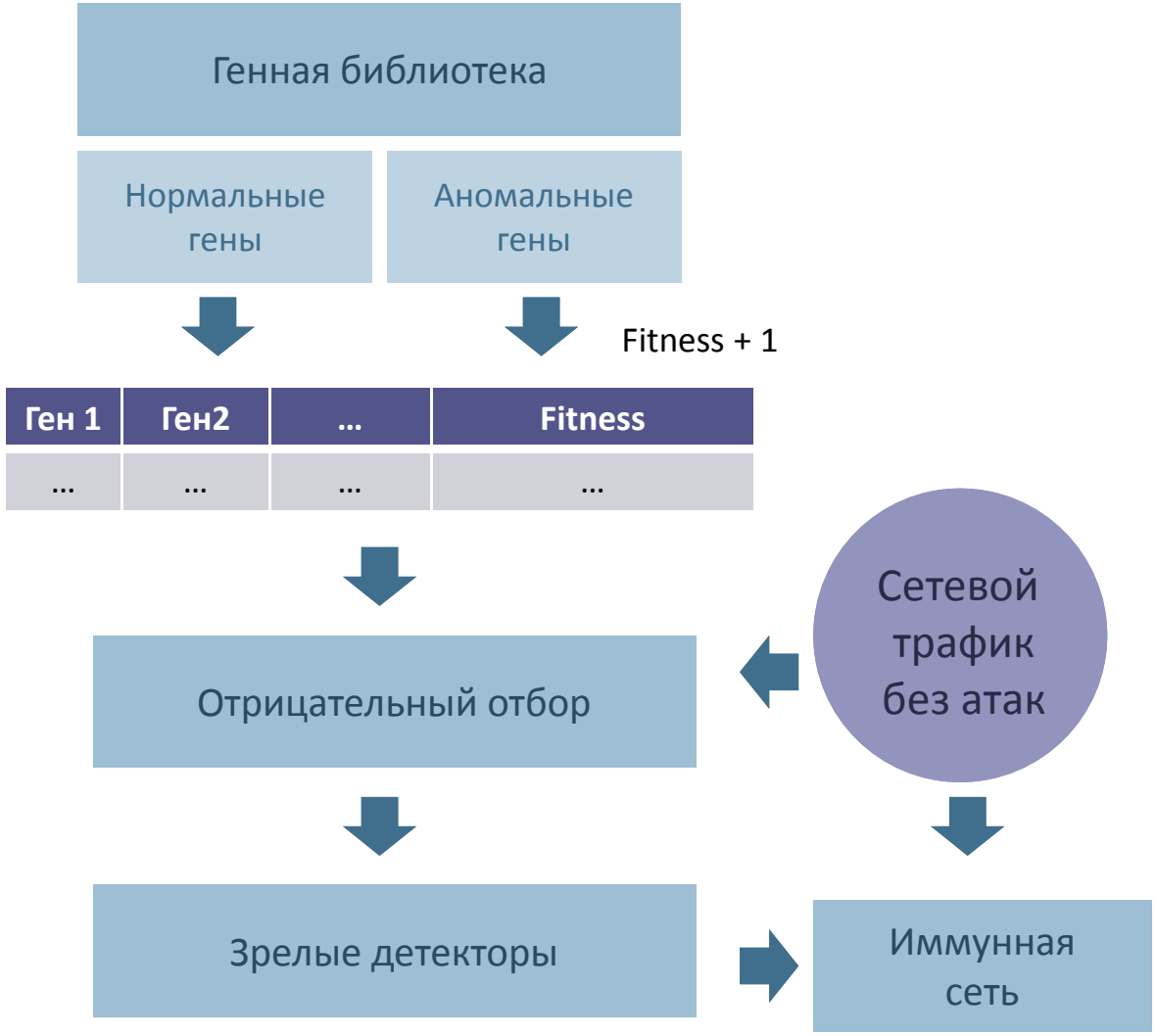
Обучение



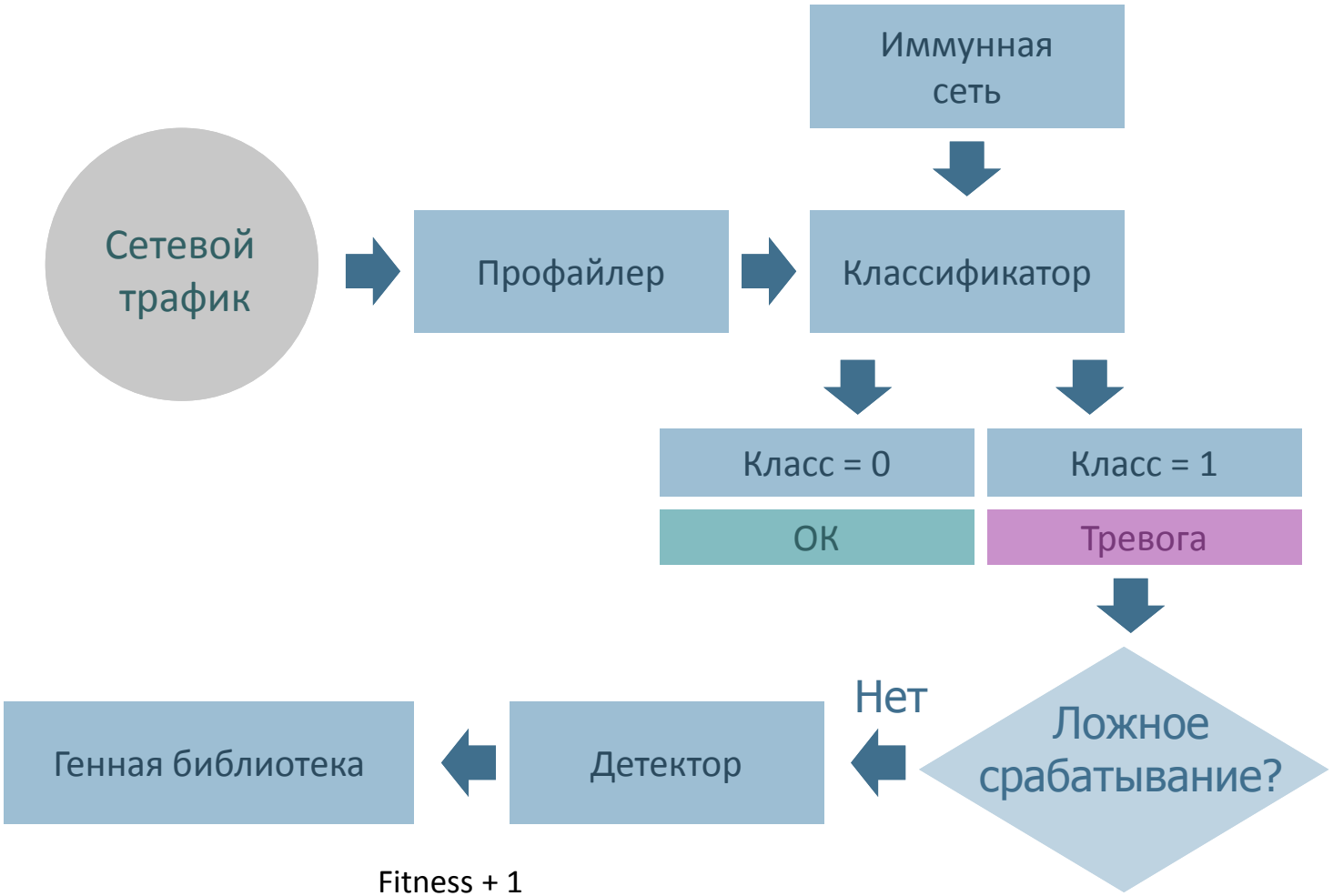
№	Клетка	Класс	Описание
1	V1	0	Нормальный трафик
2	V2	1	Buffer Overflow
3	V3	3	nmap
…	…	…	…

Мониторинг

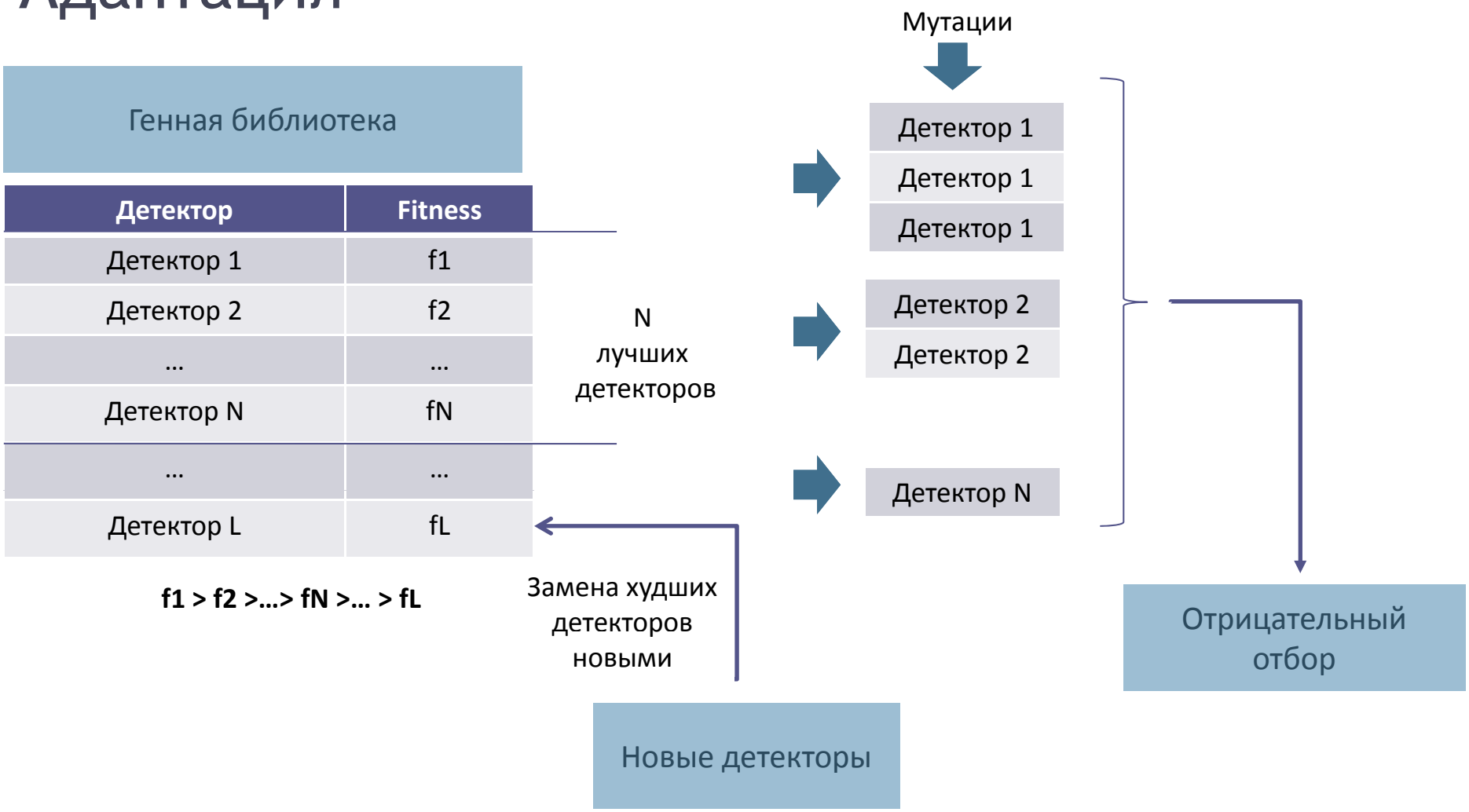
Предлагаемый подход. Обучение



Предлагаемый подход. Обнаружение вторжений



Предлагаемый подход. Адаптация

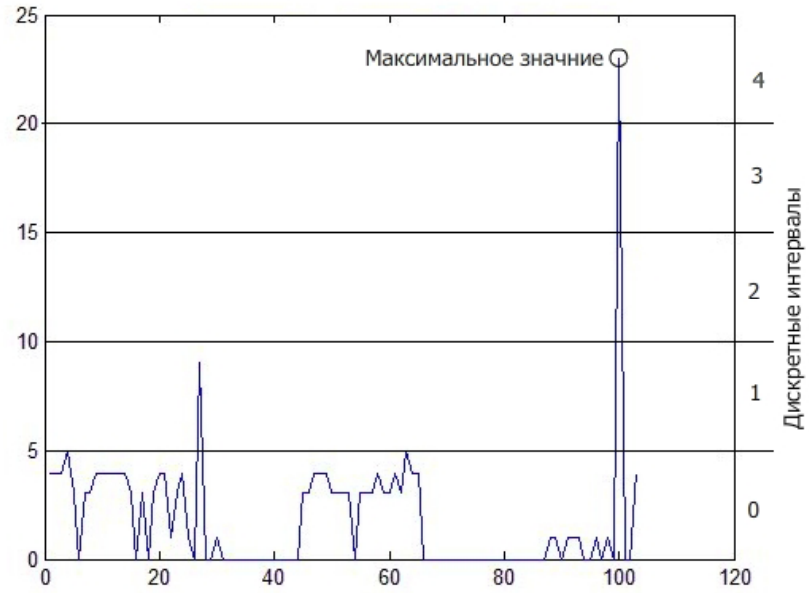


Представление данных

Сетевой трафик

Паттерн сетевой активности						
id	сервис	Байты от клиента серверу	Байты от сервера клиенту	Пакеты от клиента серверу	Пакеты от сервера клиенту	Среднекв. отклонение времени между пакетами

Дискретизация



Создание клеток FIN

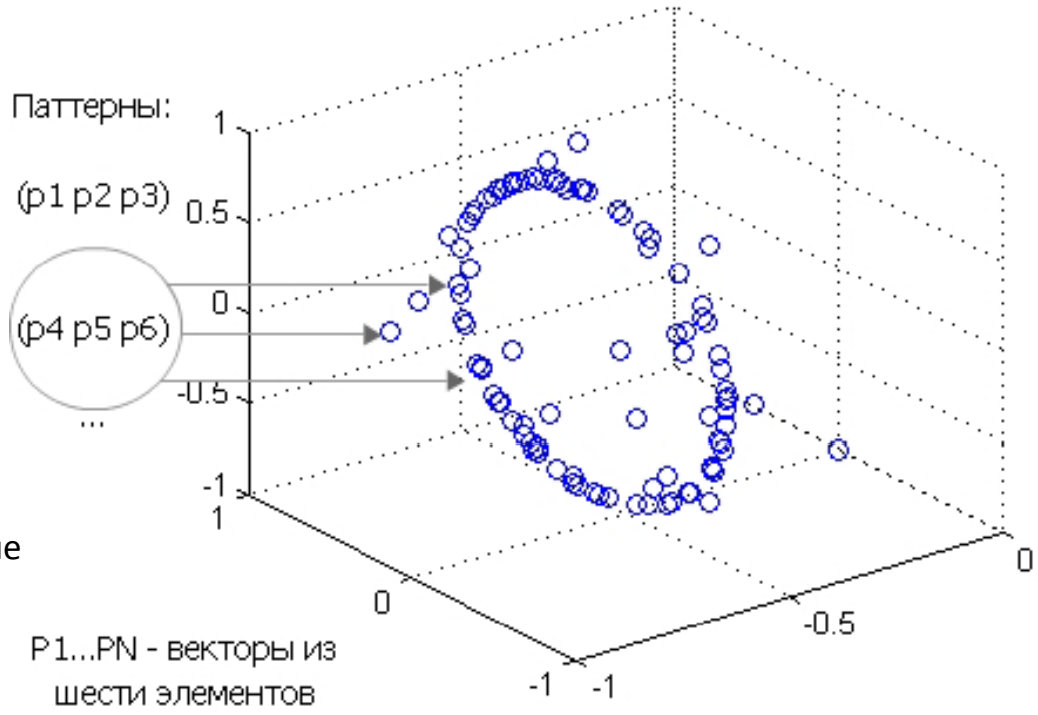
Представление данных. Клетки FIN

Паттерны сетевой активности					
P11	P12	P13	P14	P15	P16
P21	P22	P23	P24	P25	P26
…	…	…	…	…	…
P31	P32	P33	P34	P35	P36

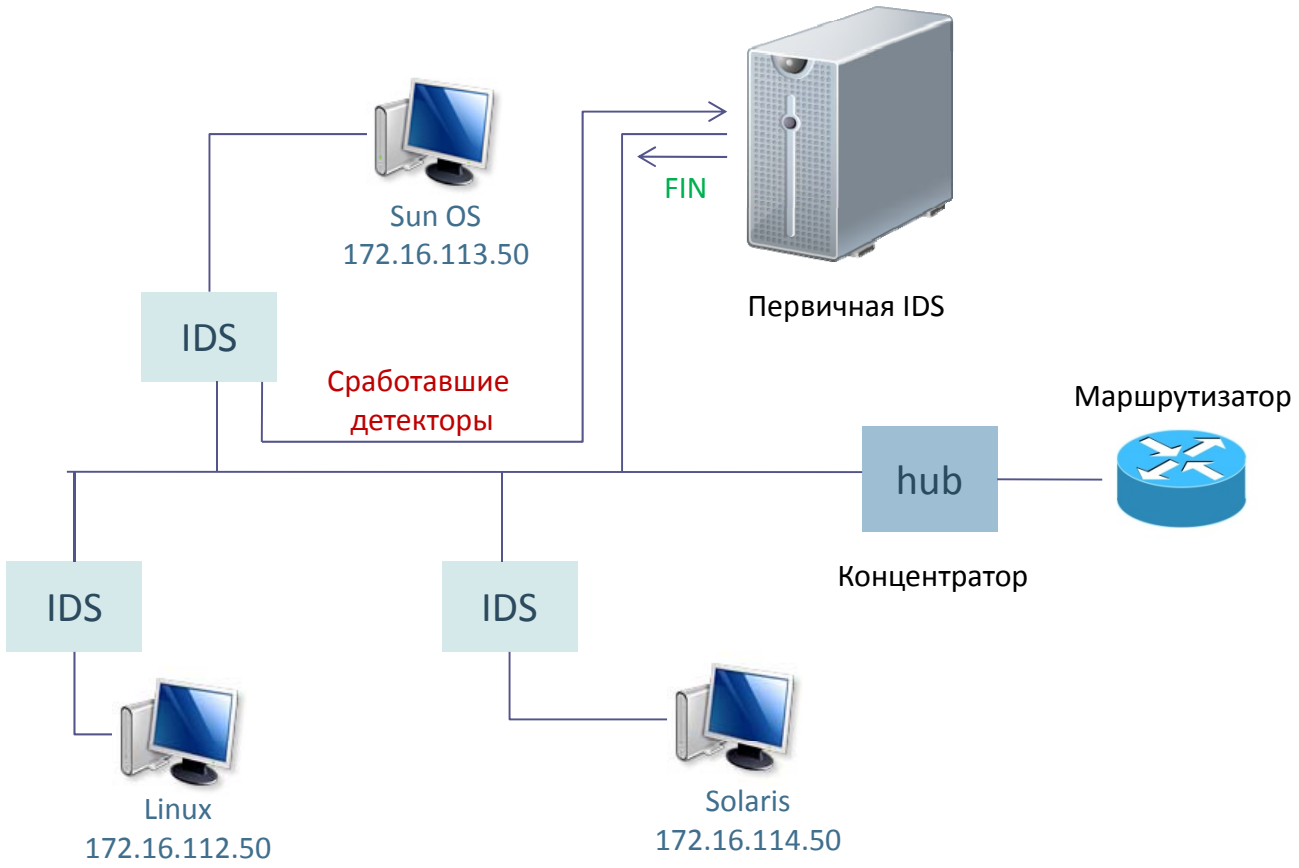
P11	P21	P21
P12	P22	P22
P13	P23	P23
P14	P24	P24
P15	P25	P25
P16	P26	P26

Сингулярное разложение

Правые сингулярные вектора



Расположение датчиков в сети



*** Для экспериментов использованы данные имитационной сети DARPA**

Эксперименты

Проверка уровня обнаружения вторжений в зависимости от временного окна

- Уровень обнаружения - отношение числа распознанных вторжений к общему числу аномальных паттернов

Проверка уровня ложных срабатываний в зависимости от временного окна

- Уровень ложных срабатываний - отношение числа ложных срабатываний к общему числу нормальных паттернов

Зависимость уровней обнаружения вторжений от порогового значения расстояния между клетками FIN

- От порогового значения зависит количество клеток FIN, а также эффективность обнаружения вторжений

Проверка уровней обнаружения вторжений и ложных срабатываний после адаптации

Сравнение с классической моделью иммунной системы

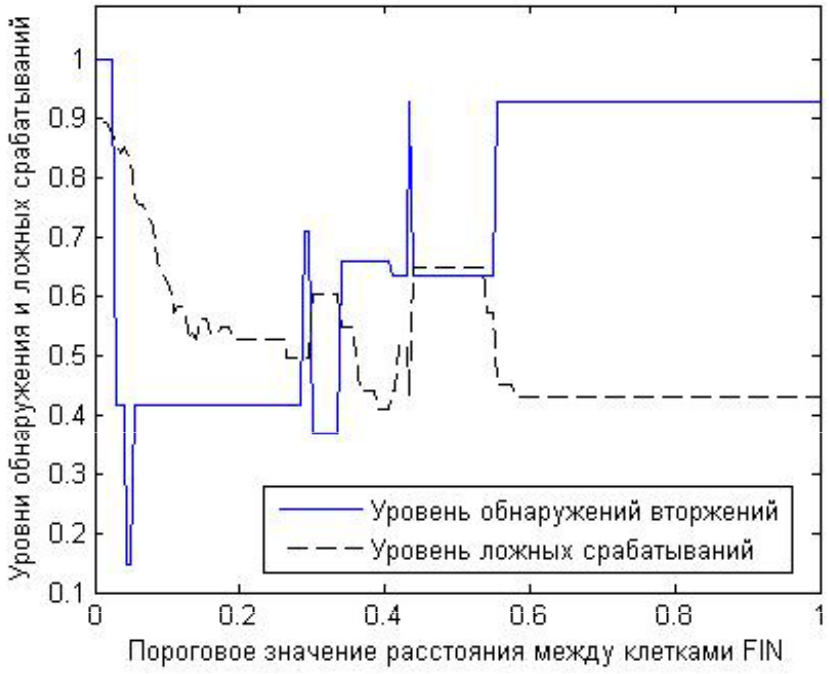
- Определение того, насколько предлагаемый подход лучше классической модели

Результаты

Скользящее временное окно

Размер временного окна	Уровень обнаружений вторжений	Уровень ложных срабатываний	Число клеток FIN
1	0,9268	0,2722	32
2	0,8646	0,1717	90
4	1	0,3643	18
8	1	0,0968	96

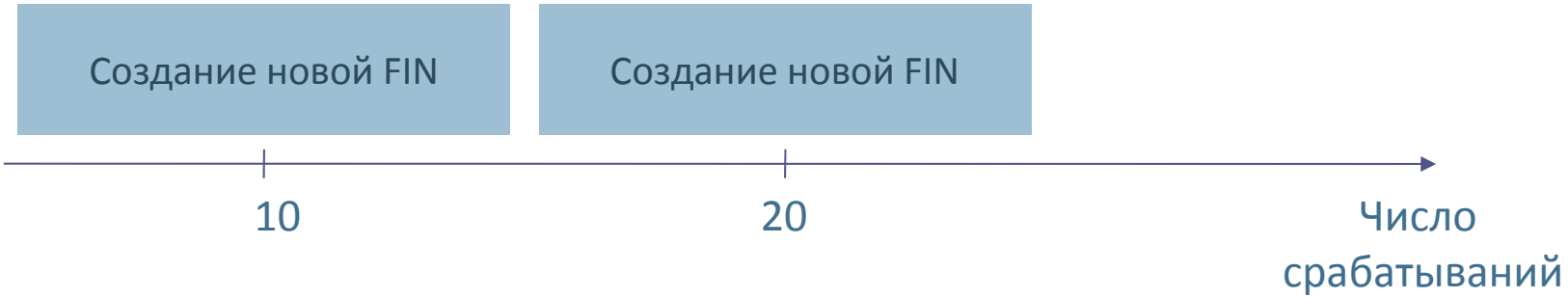
Результаты



Оптимальная величина порогового значения в данном случае выбирается исходя из числа ложных срабатываний

График для временного окна = 8

Результаты



Размер временного окна	Уровень обнаружений вторжений	Уровень ложных срабатываний	Число клеток FIN
1	1	0,1803	76
2	1	0,1214	65
4	1	0,0625	93
8	1	1	114

Сравнение с классической моделью иммунной системы

Работа системы без средств иммунокомпьютинга

Метрика	Уровень обнаружения вторжений	Уровень ложных срабатываний	Число детекторов
Расстояние по Хэммингу	0,0990	0,0196	1000
Правило r-смежных совпадений	0,0127	0,0586	1000

Выводы

- Дискретизация параметров трафика делает возможным создание детекторов
- Отображение паттернов сетевой активности в трехмерное пространство позволяет детекторам покрыть область аномальных паттернов
- Эффективность системы увеличивается благодаря эволюции генной библиотеки

Спасибо за внимание!