Поиск вредоносной активности в DNS трафике

Студент: Меньших И.А.
Руководитель: Солодушкин С.И.

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Уральский федеральный университет имени
первого Президента России Б. Н. Ельцина»

Институт математики и компьютерных наук
Кафедра вычислительной математики

Постановка задачи

Дано:

1. DNS-логи
   - source_ip
   - domain
   - rcode
2. Белый список (Alexa, Quancast)
3. Черный список (SkyDNS)

Необходимо:

1. Найти вредоносные домены
2. Выделить общие паттерны взаимодействия клиентов и вредоносных доменов
3. Реализовать полученные подходы в виде программного кода и внедрить результат в производство

Обзор подходов

1. Поэтапная фильтрация
2. Анализ pDNS и WHOIS
3. Sandbox

Методы решения

1. Групповая активность
2. Ранжирование доменов
3. Поиск и анализ паттернов взаимодействия

Групповая активность

Предположения:

1. Зараженных хостов в сети фиксированное количество.
2. Взаимодействие зараженных хостов и C&C сервера происходит периодически.
3. Подозрительно, когда на один и тот же домен в разное время запрашивает узкий круг хостов.

Групповая активность

Алгоритм поиска групповой активности

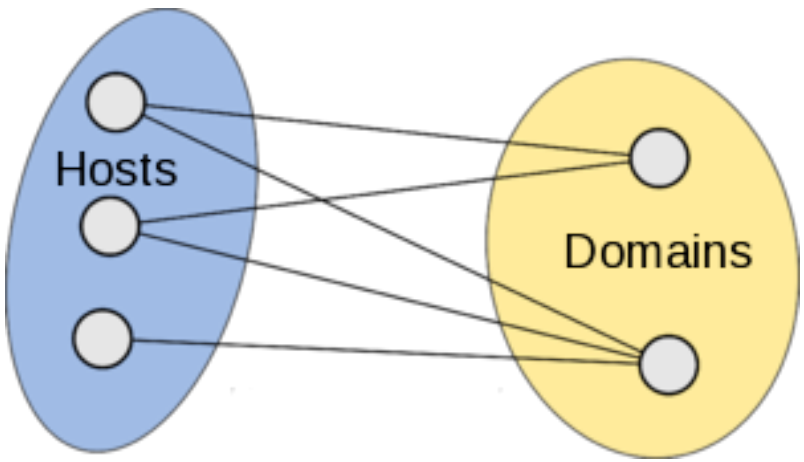
1. Делим логи на «окна» фиксированного размера.
2. Группируем хосты по домену.
3. Фильтруем по черным/белым спискам и количеству уникальных пользователей.
4. Сравниваем группы пользователей одного и того же домена в разных «окнах», если группы сильно схожи - домен подозрительный.

Ранжирование доменов

Идея: рассмотрим запросы пользователей за некоторый промежуток времени как граф.

Definition (Граф запросов)

Двудольный неориентированный граф $(H \times D, E)$, где H - множество хостов, D - множество доменных имён, $(h_i, d_j) \in E$, если пользователь h_i запрашивал домен d_j.



Ранжирование доменов

Инициализируем начальные значения, опираясь на белый/черный список и итеративно будем вычислять оценки для доменов:

$$\text{black\_score}(h_i) = \sum_{d_j:(h_i,d_j)\in E} \frac{\text{black\_score}(d_j)}{\deg(d_j)} \quad (1)$$

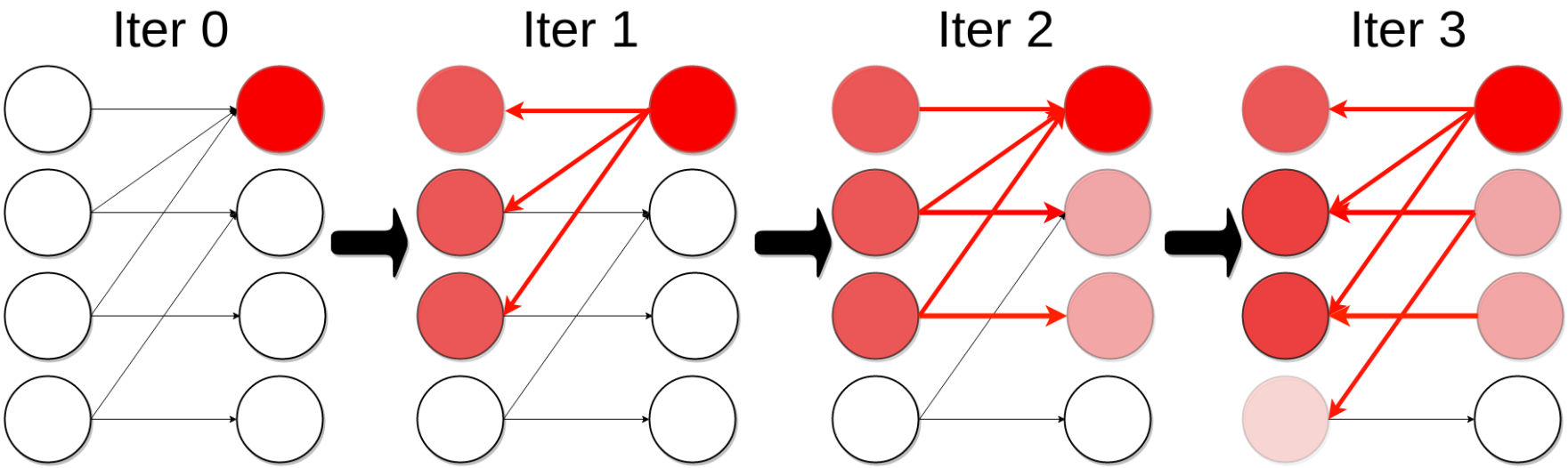
$$\text{white\_score}(h_i) = \sum_{d_j:(h_i,d_j)\in E} \frac{\text{white\_score}(d_j)}{\deg(d_j)} \quad (2)$$

$$\text{union\_score}(d_i) = \frac{\text{black\_score}(d_i)}{\text{black\_score}(d_i) + \text{white\_score}(d_i)} \quad (3)$$

$$\text{rank\_score}(d_j) = \sum_{h_i:(h_i,d_j)\in E} \frac{\text{rank\_score}(h_i)}{\deg'(h_i)} \quad (4)$$

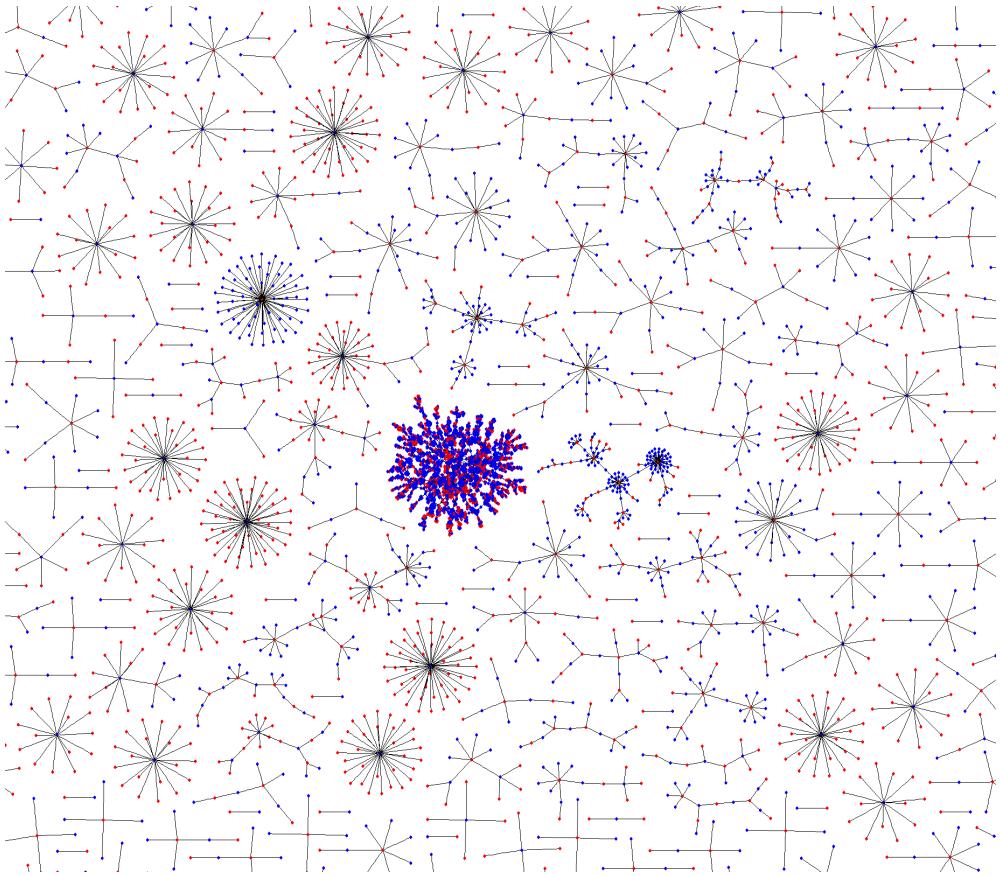
Ранжирование доменов

Процесс, который скрывается за формулами 1 – 4



Анализ паттернов взаимодействия

Идея: будем рассматривать в графе только ребра, соответствующие неудачным запросам и искать «плотные» подграфы

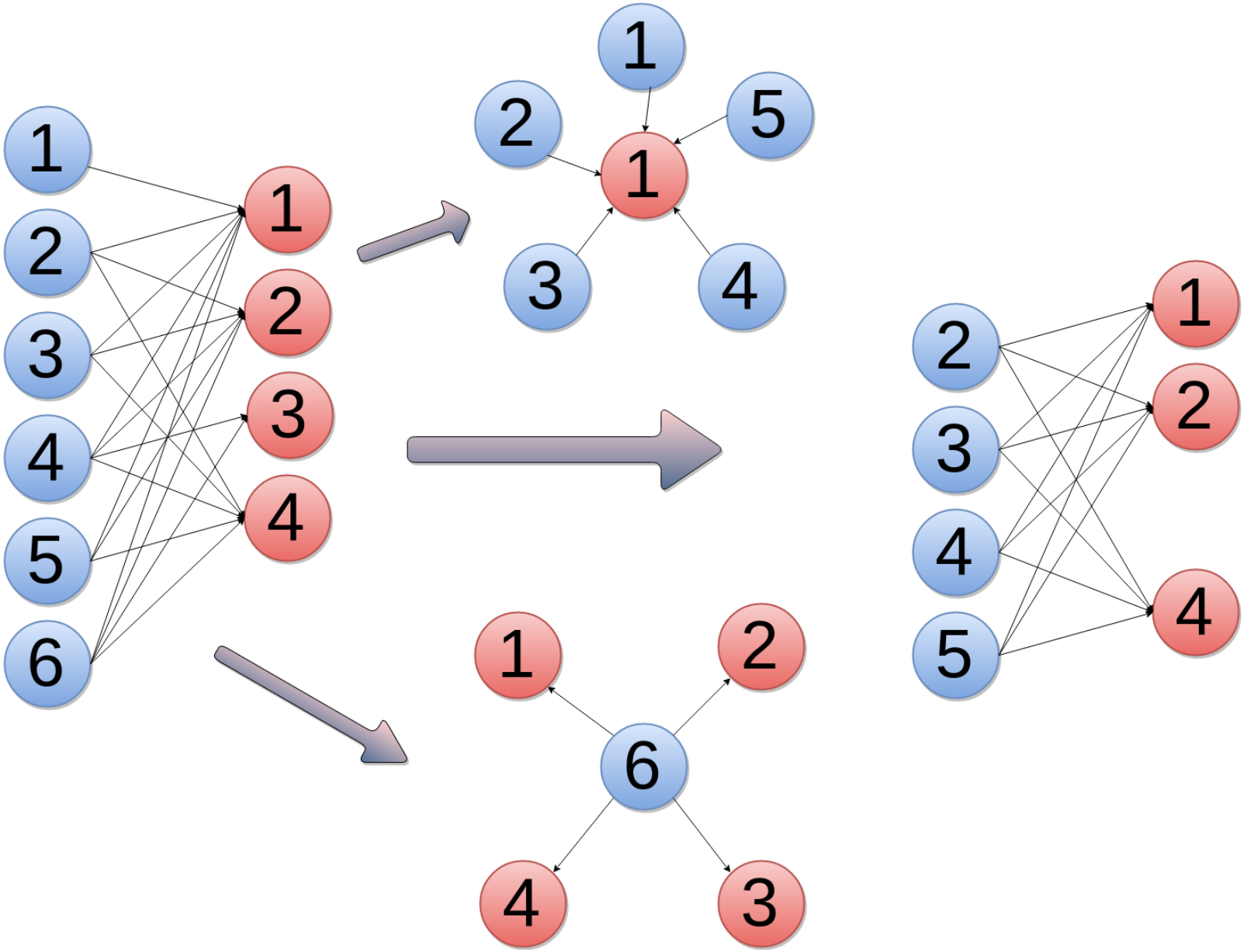


Анализ паттернов взаимодействия

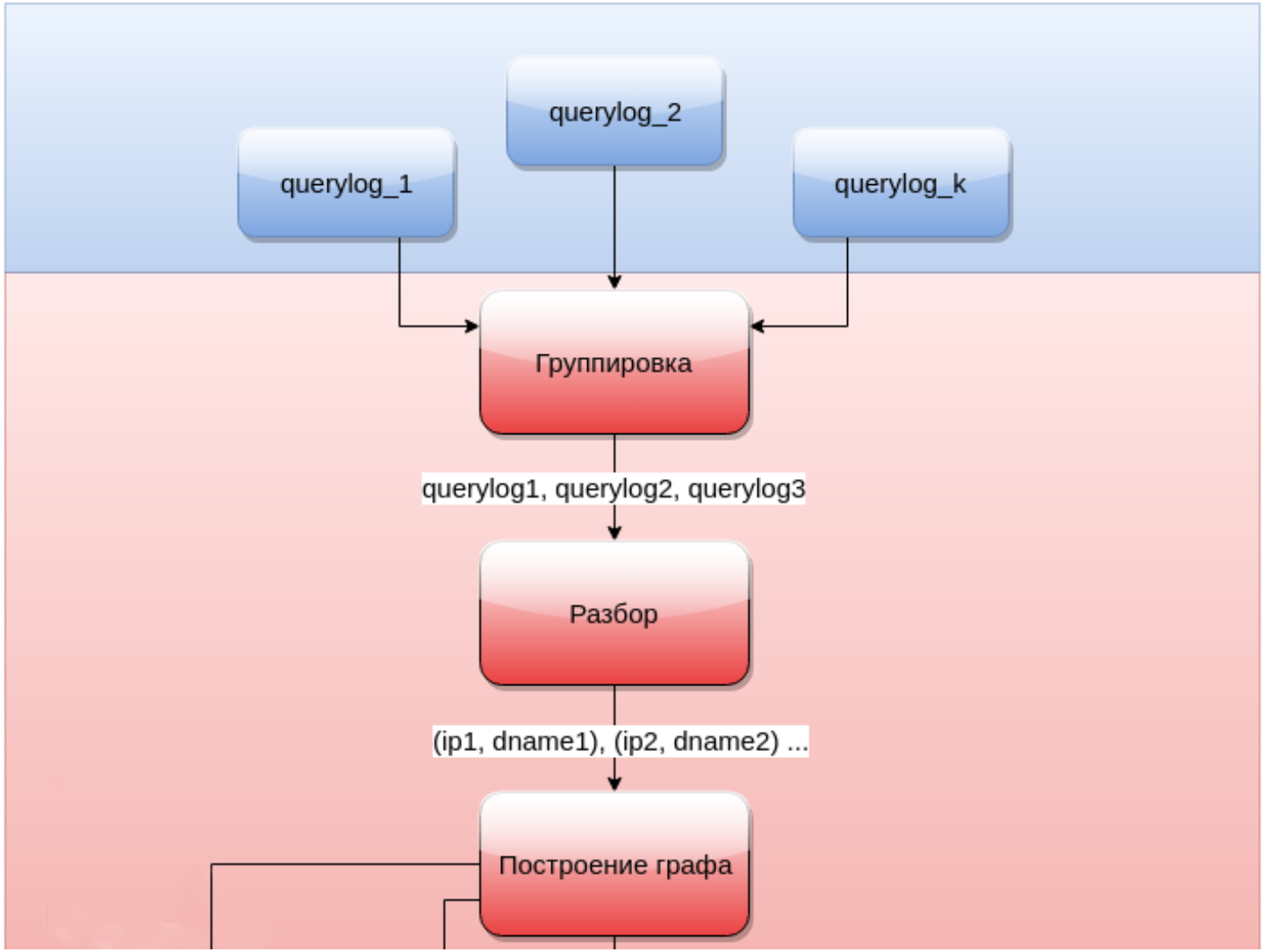
Алгоритм декомпозиции графа

1. Удаляем ребра (DNS-Overload, SERVFAIL, etc)
2. Находим все компоненты связности (BFS)
3. Для каждой компоненты связности
   1. Ищем плотные подграфы (3-NMF или иное)
   2. Вычисляем
   $$\text{density} = \frac{|\text{E}|}{|\text{H}| * |\text{D}|}$$
   3. Удаляем те подграфы, которые либо маленькие, либо имеют малый density

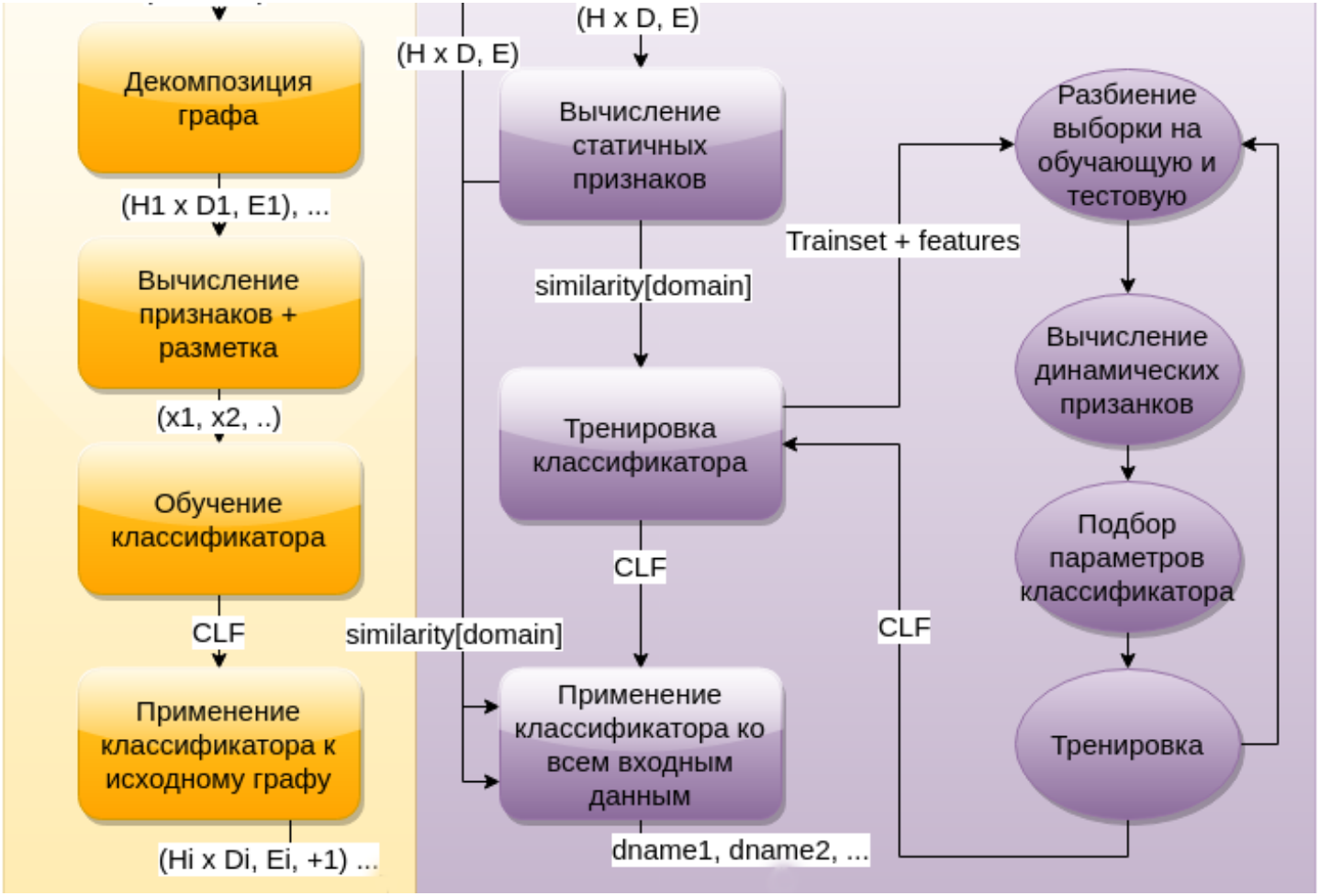
Анализ паттернов взаимодействия



Объединение подходов и автоматизация анализа



Объединение подходов и автоматизация анализа



Результаты

1. Разработан программный продукт, который занимается поиском вредоносных доменов.
2. Продукт внедрен в эксплуатацию в компании SkyDNS и показывает хорошие результаты в реальных условиях.
3. Разработана основная часть системы для ручного анализа вредоносных подграфов.

Планы на будущее

1. Продолжать работу над анализом «плотных» подграфов, автоматизировать этот процесс за счет дополнительной информации о доменах.
2. Улучшать текущий анализатор за счет более тонкой настройки на этапе подбора параметров.