Сибирский федеральный университет
Институт космических и информационных технологий
Кафедра вычислительной техники

Универсальный анализатор трафика. Система предотвращения/обнаружения вторжений (IPS/IDS)

Выполнил: Студент группы КИ18-01-5М, Шнайдер Андрей Викторович
Научный руководитель: Доцент, канд. тех наук, Казаков Федор Александрович

Цель:

Создание модуля обнаружения аномалий для системы обнаружения вторжения «Snort», на основе нейросетевого метода анализа сетевой активности.

Задачи:

-Исследование существующих систем обнаружения сетевых атак и разработка структуры интеллектуального нейросетевого модуля;

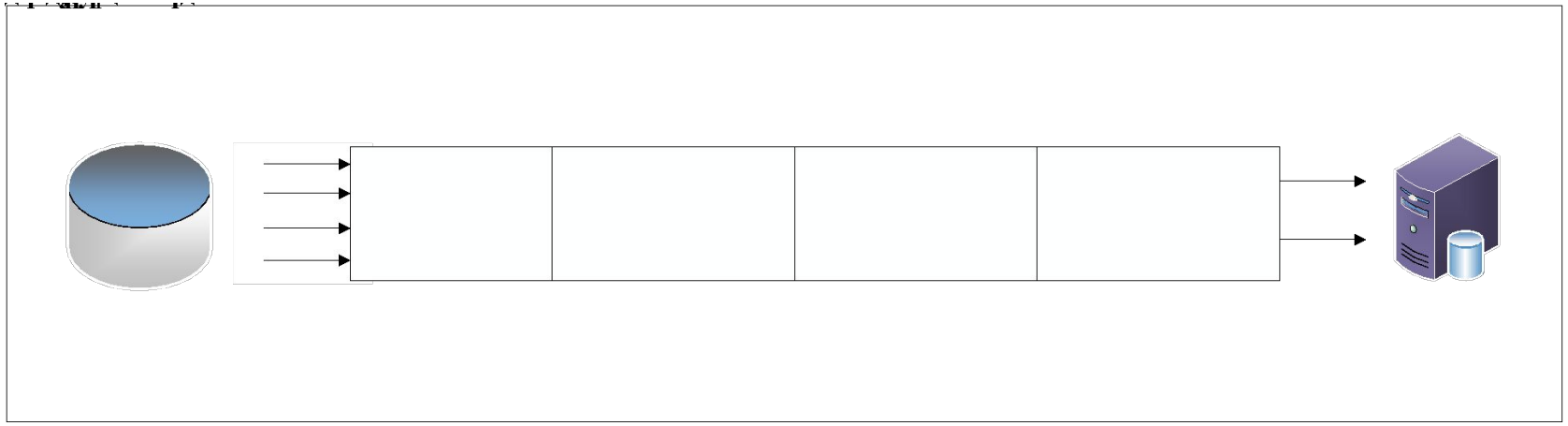
- Сопоставление технологий выявления сетевых атак в трафике в условиях априорной информации;

- Разработка структуры и алгоритма интеллектуального нейросетевого модуля;

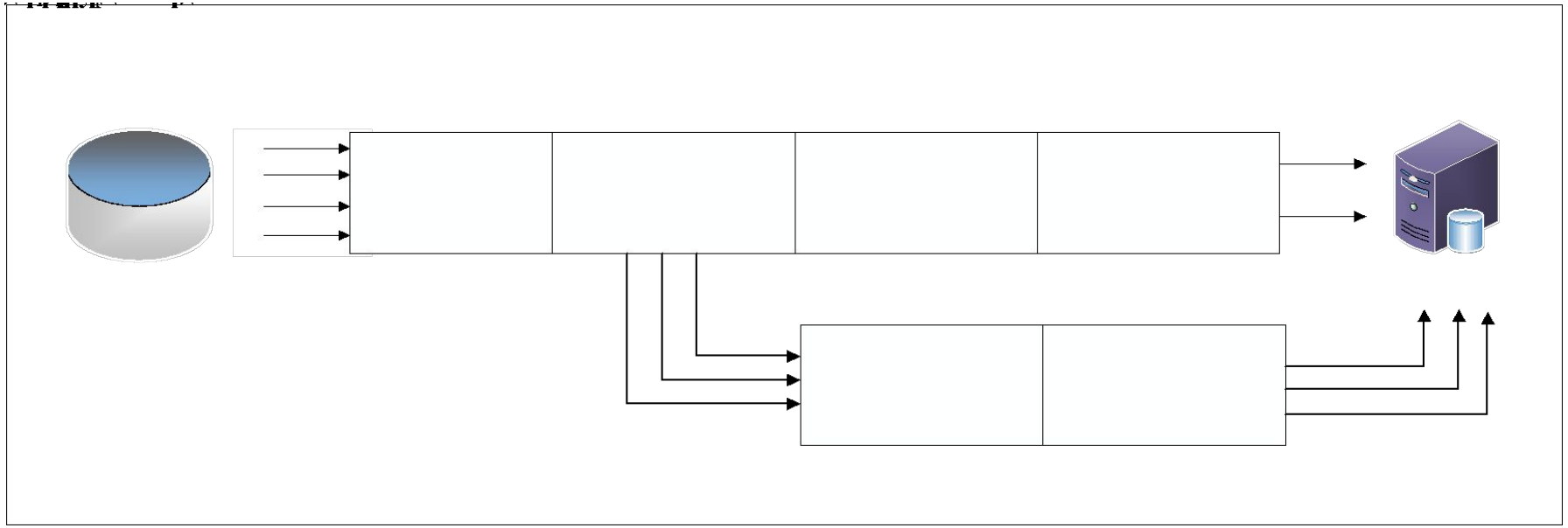
- Экспериментальная проверка программной реализаций нейросетевого алгоритма выявление сетевых атак.

Разнообразие систем IDS/IPS

Функциональная схема системы обнаружения вторжения IDS Snort



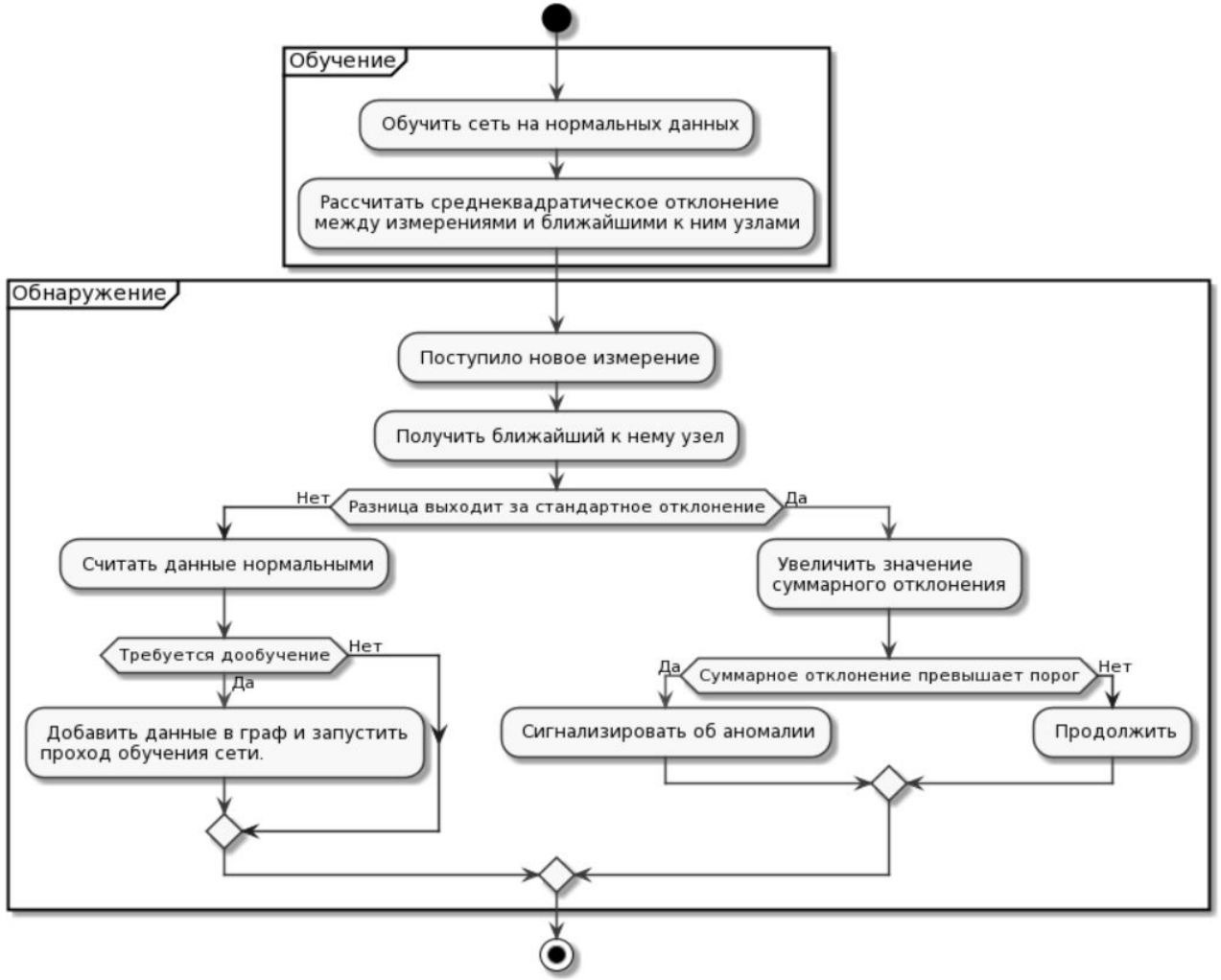
Функциональная схема системы обнаружения вторжения IDS Snort с разработанным адаптивным модулем



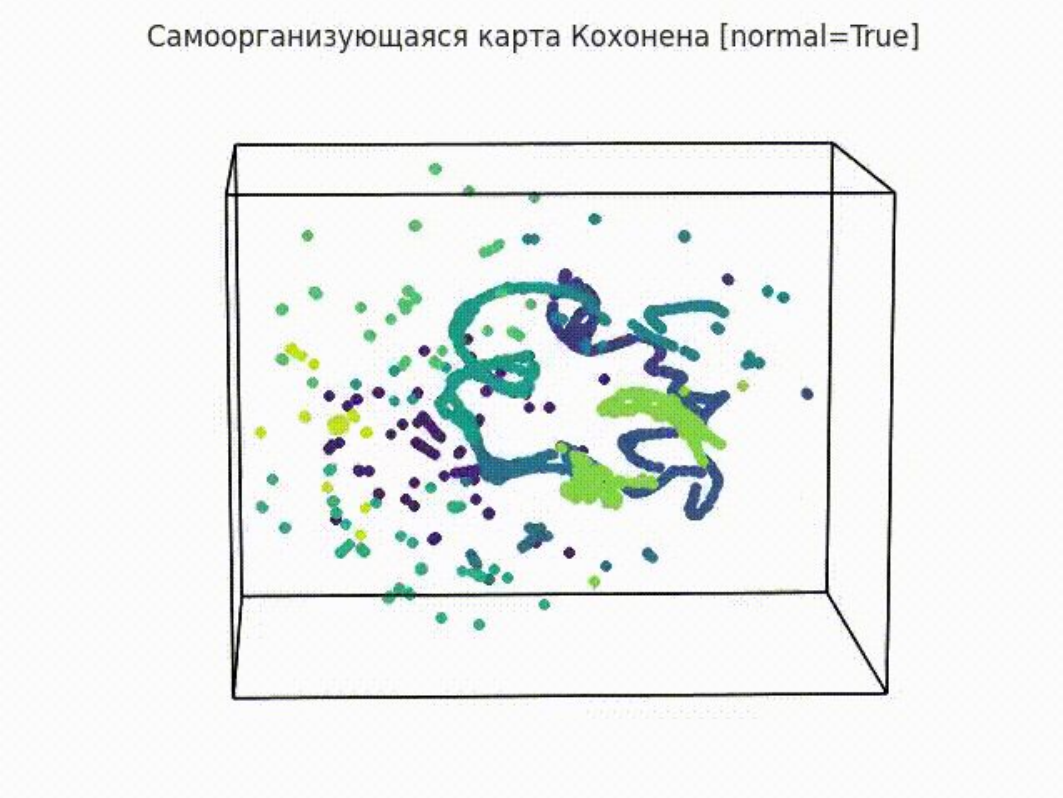
Список входных параметров, использованные для обучения

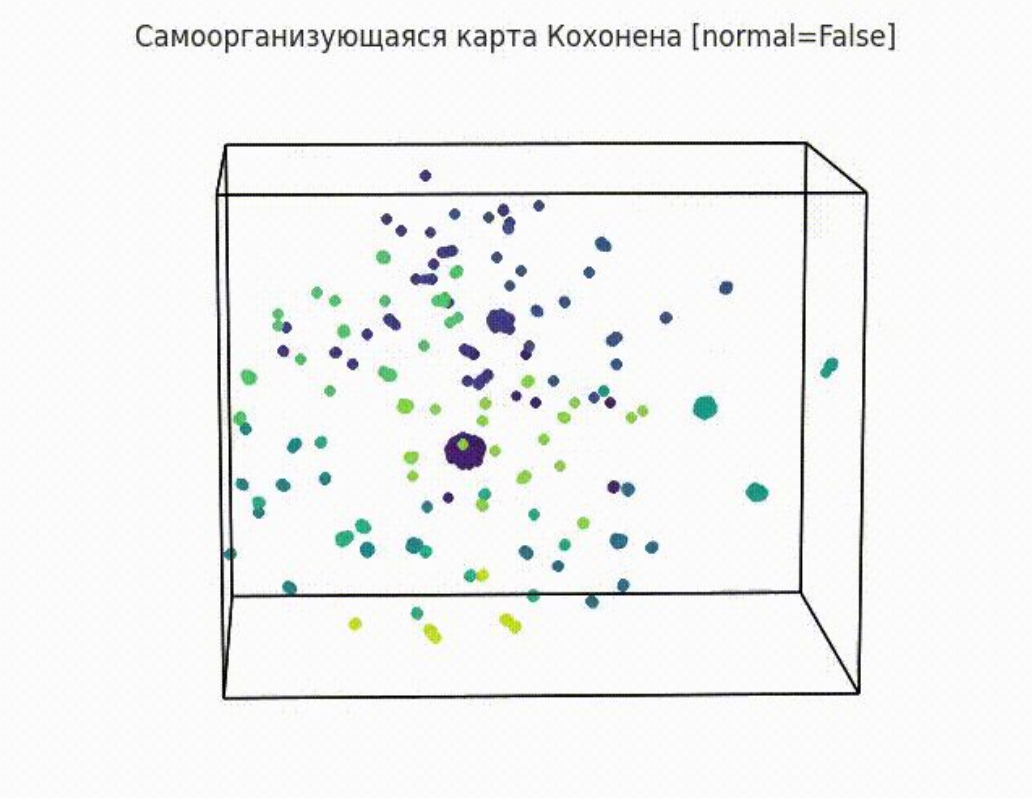
Название	Описание
duration	Продолжительность соединения в секундах
protocol_type	Тип используемого протокола, т.е. TCP, UDP и пр.
service	Тип используемых сервисов, т.е. http, ftp, telnet и пр
flag	Флаг соединения: норма или ошибка
scr_bytes	Число байт данных от источника к получателю
dst_bytes	Число байт данных от получателя к источнику
land	1 если соединение из/на таком же хосте/порте
wrong_fragments	Количество "неверных" фрагментов
urgent	Количество срочных (urgent) пакетов
count	Число подключений к этому хосту за последние 2 секунды
srv_count	Число подключений к этому сервису за последние 2 сек.
serror_rate	Процент подключений с SYN ошибками
diff_srv_rate	Процент подключений к различным сервисам
srv_diff_hast_rate	Процент подключений к различным хостам
dst_host_srv_count	Количество соединений к локальному хосту, установленных удаленной стороной и использующих одну и ту же службу

Реализация алгоритма работы нейросетевого модуля

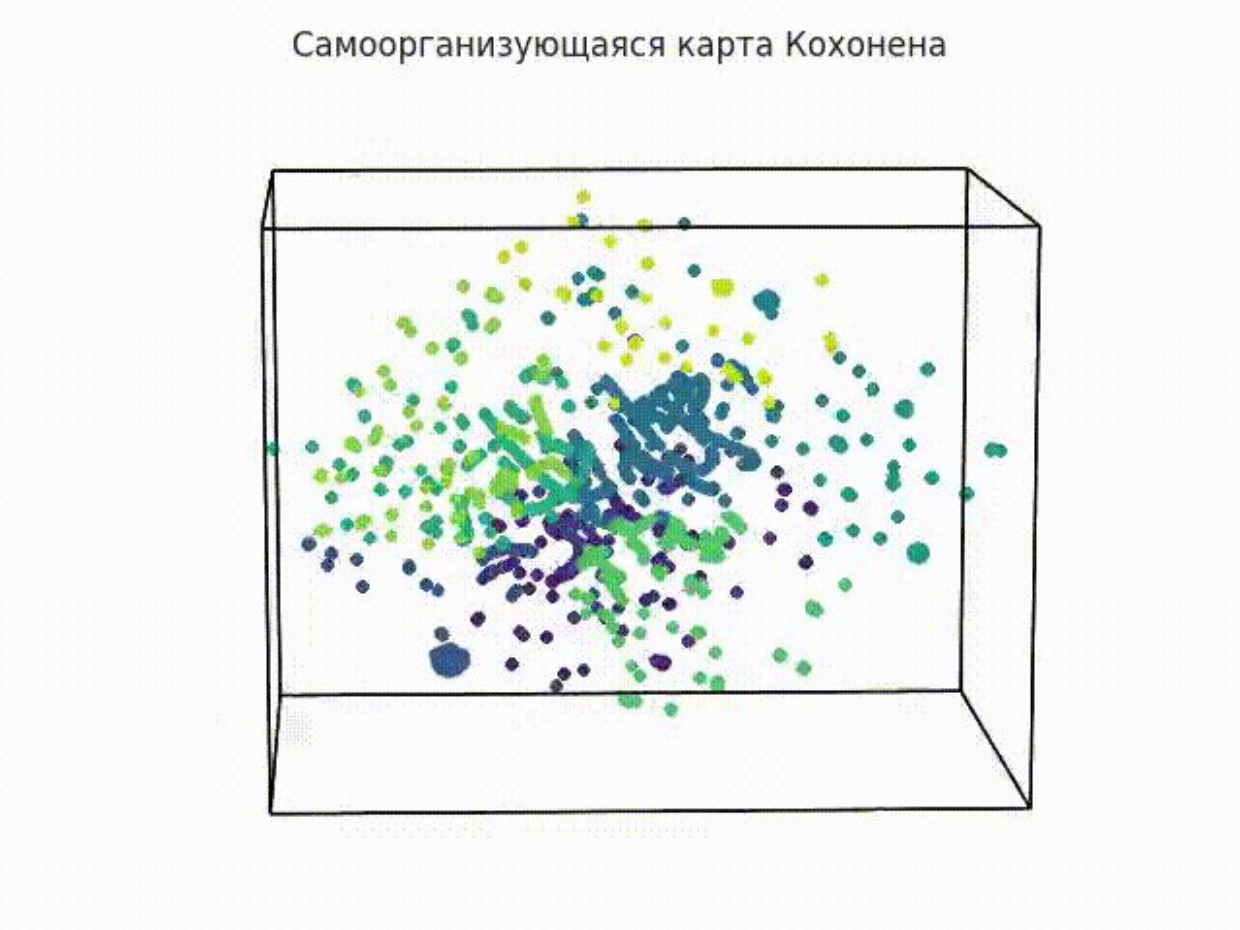


Визуализации карт сетевой активности, построенные на тестовом наборе данных





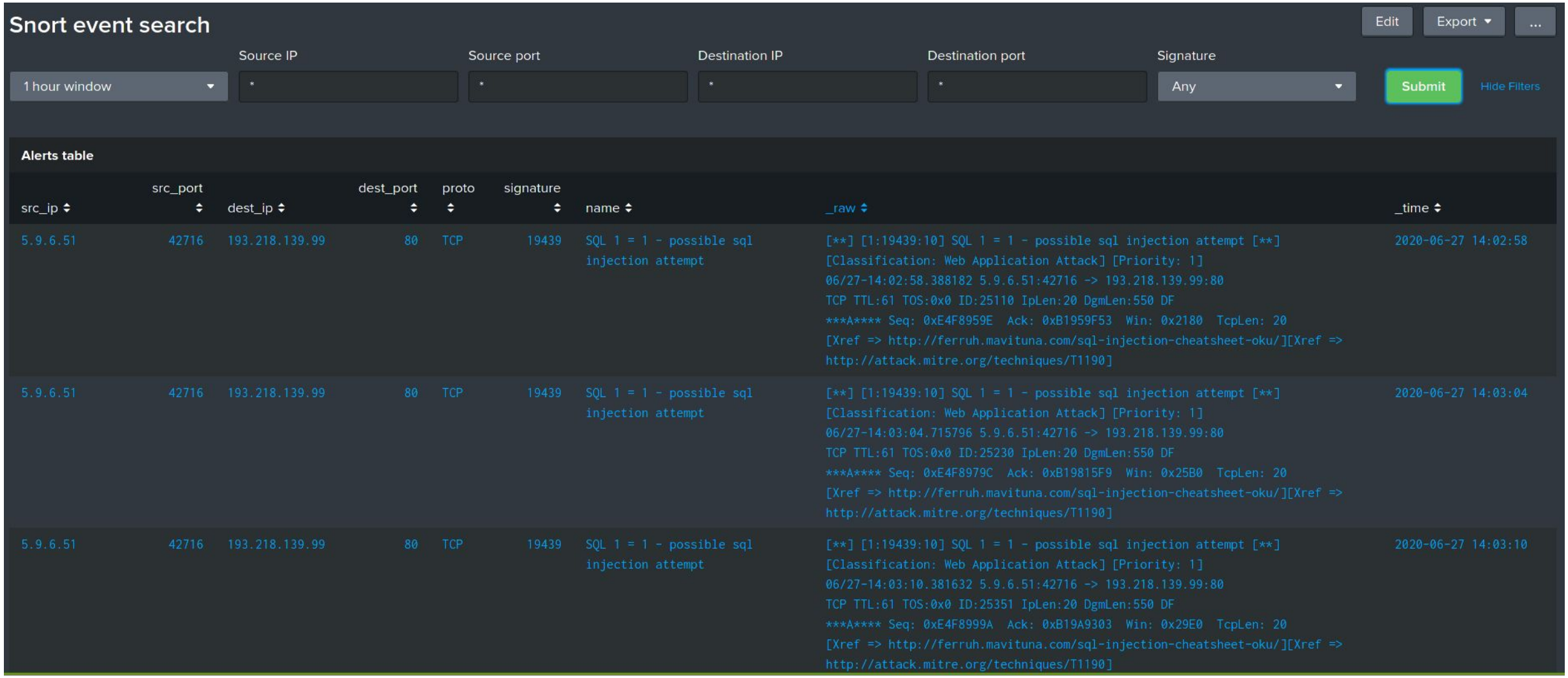
Карта сетевой активности, построенная на полной обучающей выборке



РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТА

Переменная	Значение	Описание
l_time	1869,00	Время обучения в секундах
te_l_time	0.39	Время проверки в секундах на наборе, из которого была сформирована обучающая выборка
te_t_time	4,61	Время проверки в секундах на полном наборе данных тестовой выборки
g_l_perc	69.5	Процент найденных аномалий для полного набора, из которого была сформирована обучающая выборка
g_t_perc	78.4	Процент найденных аномалий для полного набора данных тестовой выборки
f_l_perc	0,00	Процент ложных срабатываний для полного набора, из которого была сформирована обучающая выборка
f_t_perc	36.9	Процент ложных срабатываний для полного набора данных тестовой выборки

РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТА



Snort event search

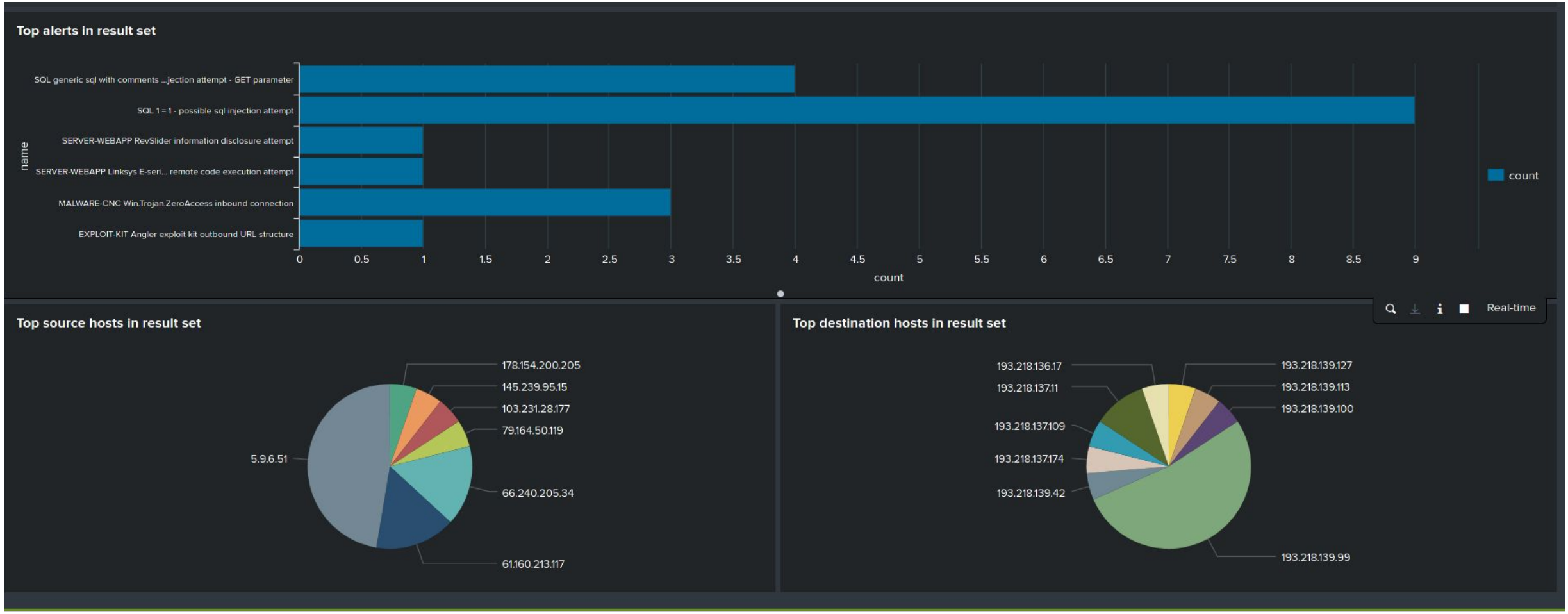
Edit | Export | ...

1 hour window	Source IP	Source port	Destination IP	Destination port	Signature	Submit	Hide Filters
	*	*	*	*	Any		

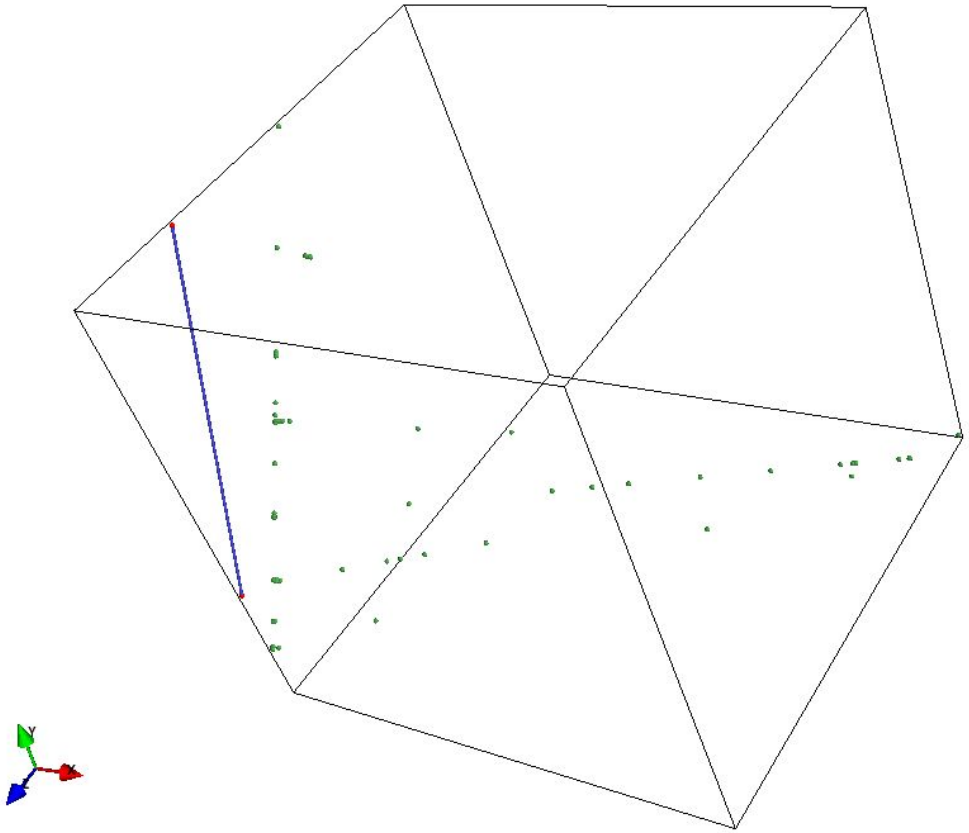
Alerts table

src_ip	src_port	dest_ip	dest_port	proto	signature	name	_raw	_time
5.9.6.51	42716	193.218.139.99	80	TCP	19439	SQL 1 = 1 - possible sql injection attempt	[**] [1:19439:10] SQL 1 = 1 - possible sql injection attempt [**] [Classification: Web Application Attack] [Priority: 1] 06/27-14:02:58.388182 5.9.6.51:42716 -> 193.218.139.99:80 TCP TTL:61 TOS:0x0 ID:25110 IpLen:20 DgmLen:550 DF ***A**** Seq: 0xE4F8959E Ack: 0xB1959F53 Win: 0x2180 TcpLen: 20 [Xref => http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/][Xref => http://attack.mitre.org/techniques/T1190]	2020-06-27 14:02:58
5.9.6.51	42716	193.218.139.99	80	TCP	19439	SQL 1 = 1 - possible sql injection attempt	[**] [1:19439:10] SQL 1 = 1 - possible sql injection attempt [**] [Classification: Web Application Attack] [Priority: 1] 06/27-14:03:04.715796 5.9.6.51:42716 -> 193.218.139.99:80 TCP TTL:61 TOS:0x0 ID:25230 IpLen:20 DgmLen:550 DF ***A**** Seq: 0xE4F8979C Ack: 0xB19815F9 Win: 0x25B0 TcpLen: 20 [Xref => http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/][Xref => http://attack.mitre.org/techniques/T1190]	2020-06-27 14:03:04
5.9.6.51	42716	193.218.139.99	80	TCP	19439	SQL 1 = 1 - possible sql injection attempt	[**] [1:19439:10] SQL 1 = 1 - possible sql injection attempt [**] [Classification: Web Application Attack] [Priority: 1] 06/27-14:03:10.381632 5.9.6.51:42716 -> 193.218.139.99:80 TCP TTL:61 TOS:0x0 ID:25351 IpLen:20 DgmLen:550 DF ***A**** Seq: 0xE4F8999A Ack: 0xB19A9303 Win: 0x29E0 TcpLen: 20 [Xref => http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/][Xref => http://attack.mitre.org/techniques/T1190]	2020-06-27 14:03:10

РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТА



Формирование самоорганизующейся карты и отчет работы, на реальном трафике



```
Image = 0
Training step = 0
Time = 0.0 s
Clusters count = 1
Neurons = 2
Connections = 1
Data records = 516

----------------------------------------------------------------------
Применение детектора к тестовому набору данных с использованием обученной модели ...
----------------------------------------------------------------------
Чтение тестового набора ...
Количество записей: 736840
Аномальные записи = 0, Нормальные записи = 748,  Время обнаружения = 1.13 с, Время на запись = 0.00112664413452  с
Аномальные записи = 0, Нормальные записи = 1522, Время обнаружения = 2.26 с, Время на запись = 0.00112577366829 с
Аномальные записи = 0, Нормальные записи = 2279, Время обнаружения = 3.38 с, Время на запись = 0.00112768054008 с
Аномальные записи = 0, Нормальные записи = 3776, Время обнаружения = 4.51 с, Время на запись = 0.00112878522873 с
Аномальные записи = 0, Нормальные записи = 5294, Время обнаружения = 5.64 с, Время на запись = 0.00112647589048 с
Аномальные записи = 0, Нормальные записи = 6045, Время обнаружения = 6.76 с, Время на запись = 0.00112660801411 с
Аномальные записи = 0, Нормальные записи = 6796, Время обнаружения = 7.89 с, Время на запись = 0.00112878522873 с
Аномальные записи = 1, Нормальные записи = 8316, Время обнаружения = 9.01 с, Время на запись = 0.00112577366829 с
...

...
Аномальные записи = 14, Нормальные записи = 735298, Время обнаружения = 188.87 с, Время на запись = 0.00112742733955 с
Аномальные записи = 14, Нормальные записи = 736078, Время обнаружения = 189.45 с, Время на запись = 0.00112647589048 с
Аномальные записи = 14, Нормальные записи = 736826, Время обнаружения = 190.91 с, Время на запись = 0.00112592681971 с
Обнаружены аномалии (количество = 14) [нормальные записи = 736826, время обнаружения = 193.45 с, время на запись = 0.00112551166035 с]
```

Заключение

Проведенные эксперименты с использованием разработанной модели нейросетевого модуля показали возможность обнаружения попыток вторжения в сеть. Система выделяет аномальные данные не входящие в кластеры полученные на этапе обучения и позволяет администратору сети в дальнейшем оценить их и принять решения о назначении.

РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТА

Спасибо за внимание!

Выполнил: Студент группы КИ18-01-5М, Шнайдер Андрей Викторович
Научный руководитель: Доцент, канд. тех наук, Казаков Федор Александрович