

В таблице представлен полный список признаков, использованных в процессе экспериментов.  
Признаки, которые были добавлены авторами выделены **полужирным шрифтом**.

*Таблица. Список извлеченных признаков*  
*Table. List of the extracted features*

Признак	Описание	Признак	Описание
L4_tcp	Используется TCP или нет (1 или 0).	var_e	Дисперсия случайной величины PCK_size. Рассчитывается для 20 последних пакетов.
L4_udp	Используется UDP или нет (1 или 0).	q3_e	Третий квартиль. Рассчитывается для 20 последних пакетов.
L7_http	Используется HTTP или нет (1 или 0).	q1_e	Первый квартиль. Рассчитывается для 20 последних пакетов.
L7_https	Используется HTTPS или нет (1 или 0).	iqr_e	Разница между третьим и первым квартилем PCK_size.
port_class_src	Нет порта = 0. Общеизвестный порт (0–1023) = 1. Зарегистрированный порт (1024–49151) = 2. Динамический порт (49152–65535) = 3.	inter_arrival_time	Время между текущим и предыдущим пакетом.
port_class_dst	Класс номера порта назначения.	skew_et	Значение асимметрии ethernet_frame_size. Рассчитывается для 20 последних пакетов.
pck_size	Полный размер пакета в байтах, включая заголовки IP, встроенные заголовки протоколов и данные.	kurt_et	Коэффициент эксцесса ethernet_frame_size. Рассчитывается для 20 последних пакетов.
ttl	TTL (Время жизни)	skew_e	Значение асимметрии PCK_size. Рассчитывается для 20 последних пакетов.
protocol	Номер протокола.	kurt_e	Коэффициент эксцесса PCK_size. Рассчитывается для 20 последних пакетов.
source_port	Порт источника.	<b>unique_ip_dst_count</b>	Количество уникальных IP за последние 20 пакетов (как назначения, так и источника).
dest_port	Порт назначения.	<b>unique_ip_src_count</b>	Количество уникальных IP за последние 20 пакетов (как назначения, так и источника).
DNS_count	Количество DNS-запросов в 20 последних пакетах.	<b>L3_ip</b>	Является ли IP пакетом (1 или 0).
NTP_count	Количество NTP-запросов в 20 последних пакетах.	<b>packet_rate</b>	Количество пакетов в секунду.
ARP_count	Количество ARP-запросов в 20 последних пакетах.	<b>number_of_servers</b>	Подсчет количества уникальных IP адресов серверов для 20 ближайших пакетов.
most_freq_prot	Протокол, который используется чаще всего в 20 последних пакетах.	<b>tcp_window</b>	Размер буфера.
most_freq_sport	Номер порта источника, используемый чаще всего в 20 последних пакетах.	<b>tcp_data_offset</b>	Смещение данных.
most_freq_dport	Номер порта назначения, используемый чаще всего в 20 последних пакетах.	<b>NTP</b>	Является ли пакет NTP (1 или 0).
sum_et	Сумма ethernet_frame_size 20 последних пакетов.	<b>ntp_interval</b>	Время между этим и прошлым запросом NTP.
min_et	Минимальный ethernet_frame_size среди 20 последних пакетов.	<b>DNS</b>	Является ли пакет DNS (1 или 0).
max_et	Максимальный ethernet_frame_size среди 20 последних пакетов.	<b>dns_interval</b>	Время между этим и прошлым запросом DNS.
med_et	Медиана ethernet_frame_size для 20 последних пакетов.	<b>is_icmp</b>	Является ли пакет ICMP (1 или 0).
average_et	Средняя арифметическая ethernet_frame_size для 20 последних пакетов.	<b>icmp_type</b>	Тип ICMP.
var	Дисперсия случайной величины ethernet_frame_size. Рассчитывается для 20 последних пакетов.	<b>is_eapol</b>	Является ли пакет EAPOL (1 или 0).
q3	Третий квартиль. Рассчитывается для 20 последних пакетов.	<b>eapol_type</b>	Тип ICMP.
q1	Первый квартиль. Рассчитывается для 20 последних пакетов.	<b>wifi</b>	Является ли пакет Wi-Fi (1 или 0).
iqr	Разница между третьим и первым квартилем ethernet_frame_size.	<b>wifi_sub_type</b>	Тип Wi-Fi.
sum_e	Сумма PCK_size для 20 последних пакетов.	<b>zigbee</b>	Является ли пакет zigbee (1 или 0).
min_e	Минимальный PCK_size для 20 последних пакетов.	<b>zigbee_type</b>	Тип zigbee.
max_e	Максимальный PCK_size для 20 последних пакетов.	<b>tcp_payload_size</b>	Полезная нагрузка TCP.
med	Медиана PCK_size для 20 последних пакетов.	<b>total_length</b>	Размер всего IP-пакета, включая заголовок и данные.
average	Средняя арифметическая PCK_size для 20 последних пакетов.		