

Аналитический отчёт по сервису защиты от DDoS - атак КТТК за 2021 год



ТТК

Создаем цифровое будущее **вместе**

О КОМПАНИИ

Услуга Защита от DDoS - атак

Компания **ТрансТелеКом**, один из ведущих провайдеров цифровых сервисов в России, обеспечивает информационную безопасность бизнеса и государственных структур с помощью услуги "Защита от DDoS - атак".

Сервис "**Защита от DDoS - атак**" компании ТрансТелеКом - это многоуровневая система фильтрации входящего трафика, которая включает в себя защиту интернет каналов, сетевого оборудования и веб - ресурсов. Решение позволяет обнаруживать и блокировать зловредный трафик на уровнях от L3 до L7 с производительностью более **160 Гбит/с**. Это даёт возможность обеспечить непрерывную работу интернет - сервисов в условиях DDoS - атаки. Поддерживаются режимы защиты от DDoS - атак с непрерывной очисткой трафика особо критичных клиентских сервисов либо с перенаправлением трафика после обнаружения DDoS - атак.

В данном отчёте представлены результаты анализа DDoS - атак за 2021 год.

Специалисты компании ТрансТелеКом отследили динамику изменения количества, мощности и продолжительности аномалий в течение года.

Количество атак

В течение 2021 года (с 1-го по 4-ый кварталы) число DDoS - атак на компании, информационную безопасность которых обеспечивает ТрансТелеКом, увеличилось в **более чем 2 раза**.



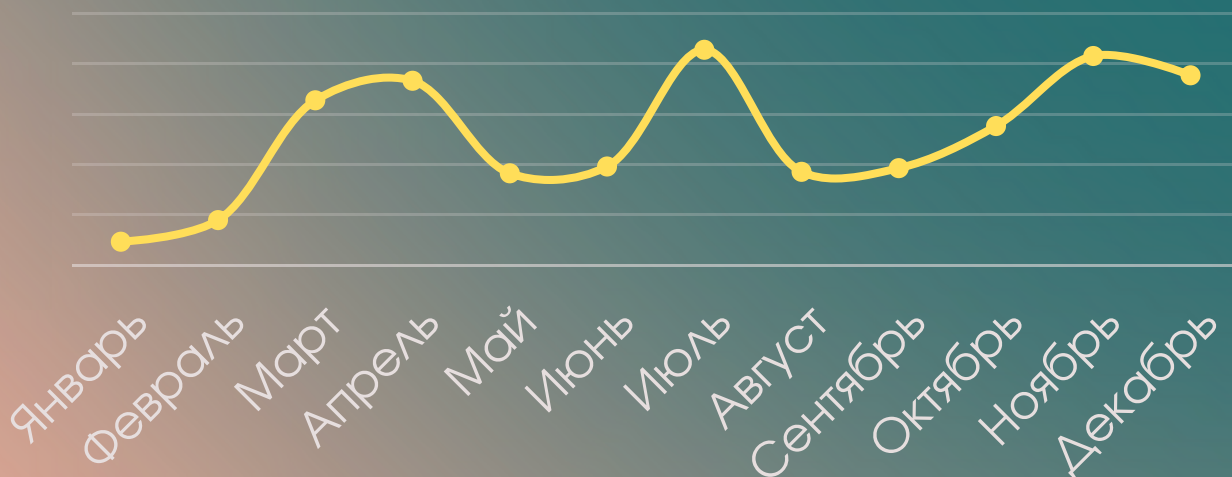
Распределение атак по длительности

Более 70% атак продолжались до 15 минут, 20% - длились от 15 минут до 1 часа.



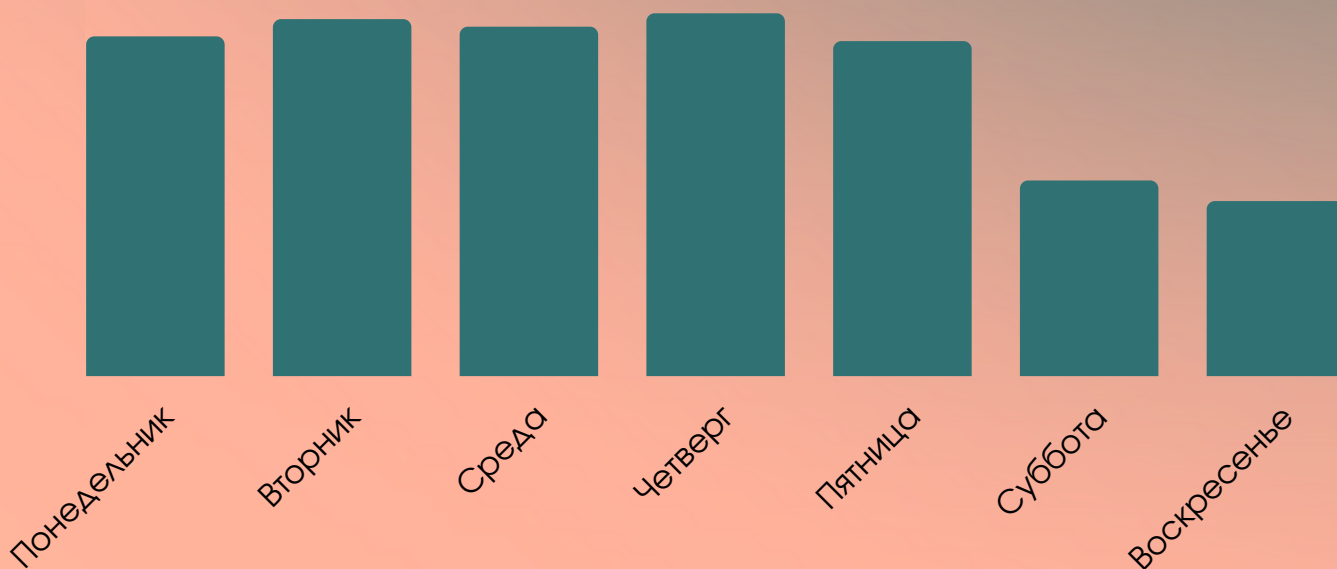
Распределение атак по месяцам

Месяц - лидер по количеству DDoS - атак за 2021 год - **Июль**, с небольшим отрывом следуют Ноябрь и Декабрь, что подтверждает стремительный рост числа аномалий под конец года.



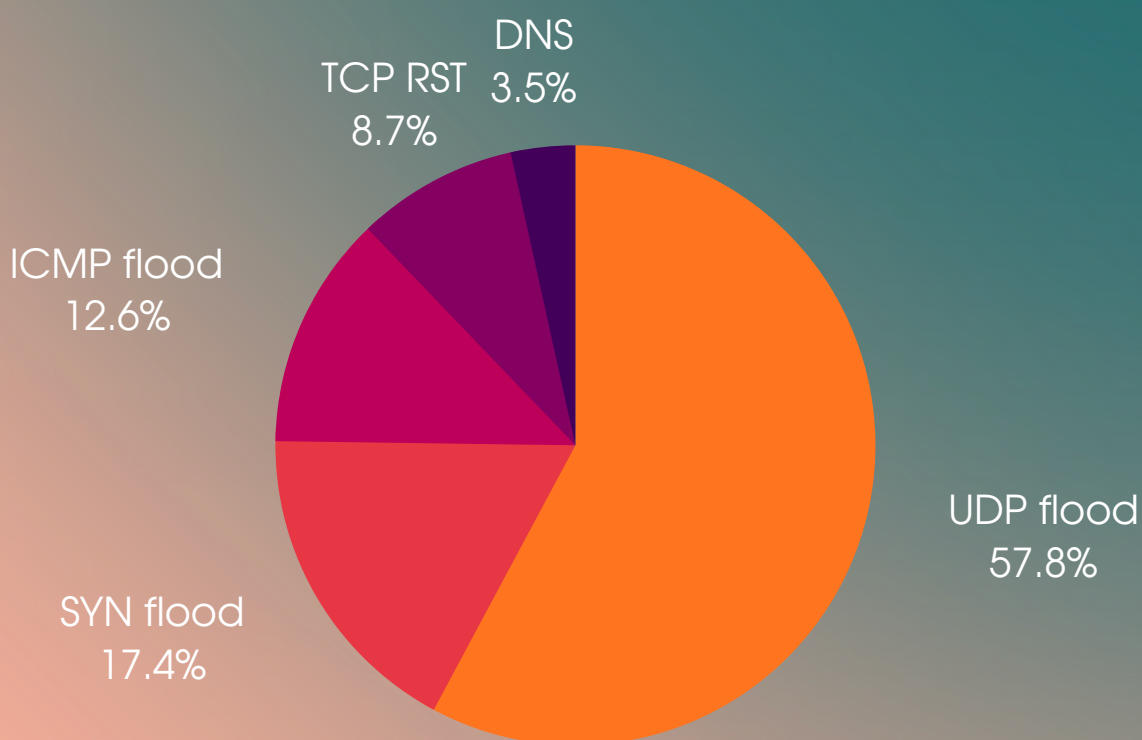
Распределение атак по дням недели

День недели - лидер по количеству DDoS - атак за год - **Четверг**.



Типы атак

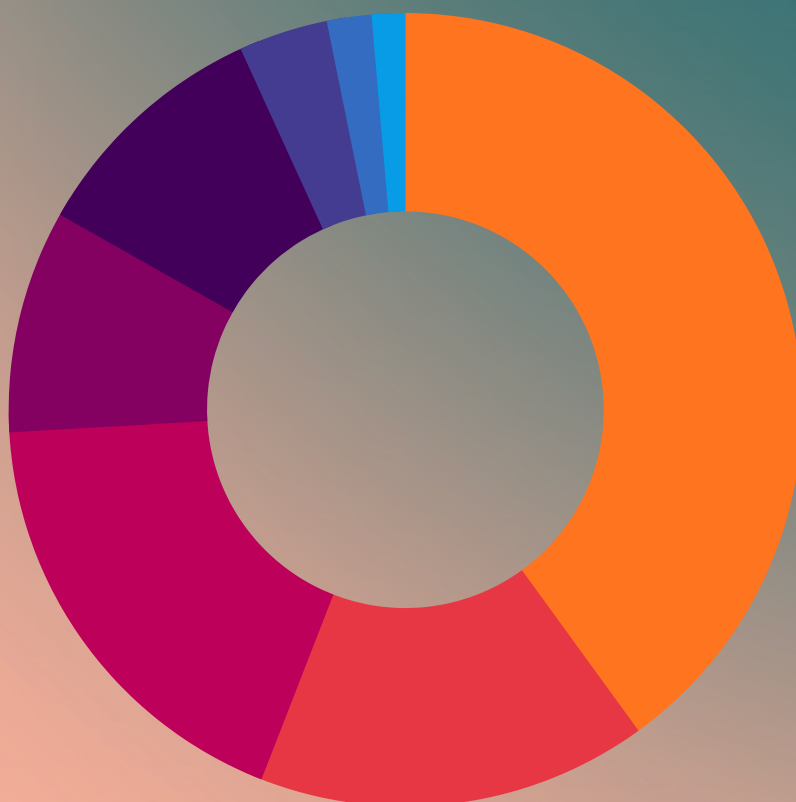
Наиболее встречающийся тип атак за 2021 год - **UDP flood**, следом - **SYN flood**.



Три четвертых атак использовали технологии SYN и UDP, суть которых сводится к отправке большого количества запросов в достаточно короткий срок. В итоге атакуемая система оказывается перегруженной, паразитный трафик захватывает доступную полосу пропускания, а полезному трафику остаётся только небольшая её часть. Сервисы или сайты становятся недоступными, что останавливает нормальный рабочий процесс, пока не закончится или не будет успешно отражена DDoS - атака. Абсолютно для любой компании это грозит срывом многих процессов и несёт финансовые и репутационные риски.

Скорость атак

Больше половины DDoS - атак - **56 %** были небольшой скорости до 200 Мбит/с. Доля атак с наибольшей скоростью составила 1%.



до 100 Мбит/с	40%	от 100 до 200 Мбит/с	16%
от 200 до 500 Мбит/с	18%	от 500 Мбит/с до 1 Гбит/с	9%
от 1 до 5 Гбит/с	10%	от 5 до 20 Гбит/с	4%
от 20 до 100 Гбит/с	2%	более 100 Гбит/с	1%

Создаем цифровое будущее **вместе**

ТТК



8 800 775 66 77

(по России звонок бесплатный)



b2b.ttk.ru



info@ttk.ru