Selectel

Аналитический отчет по DDoS за 2025 год

Количество и мощность DDoS-атак ежегодно растут, ставя под угрозу доступность публичных и корпоративных сервисов. Для бизнеса это оборачивается не только прямыми финансовыми потерями, но и серьезным репутационным ущербом.

Инфраструктура Selectel объединяет более 31 000 клиентов, которые генерируют легитимный сетевой трафик объемом свыше 500 Гбит/с. **Анализ атак на проекты такого масштаба дает уникальные данные для оценки ландшафта угроз в облачных средах**.

Мы в Selectel подготовили аналитический отчет о DDoS-атаках за 2025 год и отдельно рассмотрели показатели за второе полугодие. **Эти данные помогают компаниям оценить динамику угроз для облачной инфраструктуры** и вовремя скорректировать настройки IT-систем и средств защиты.

Статистика собрана на основе данных об атаках, направленных **на сетевой (L3) и транспортный (L4) уровни модели OSI** и отраженных с помощью бесплатного сервиса защиты. А **для уровня приложений (L7)** доступны партнерские сервисы для защиты веб-приложений и решения от DDoS-атак и ботов.

Ключевые выводы

По результатам анализа показателей 2025 года мы наблюдаем **непрерывный значительный рост всех показателей**: количества, длительности, мощности и скорости атак. Инциденты носят массовый характер, а в случае выбора конкретной цели злоумышленники атакуют инфраструктуру в течение длительного времени — сотни часов, а количество инцидентов на один сервис или организацию исчисляется тысячами.

140 628	22 743	569	193
атак	часов	Gbps	Mpps

Детальную аналитику с ключевыми показателями за предыдущие периоды вы можете посмотреть в отчетах за первое полугодие 2024 года, в полном отчете за 2024 год, а также в отчете за первое полугодие 2025 года.

При сравнении с 2024 годом ключевые показатели 2025 года демонстрируют **устойчивый рост год к году (YoY)**. Количество DDoS-атак увеличилось на 25% — с 112 171 до 140 628. Общая длительность изменилась еще более заметно — на 67%, с 13 613 до 22 743 часов.

Динамика изменения показателей год к году (YoY)

	2024	2025	YoY
Количество атак	112 171	140 628	+25%
Общая длительность, ч	13 613	22 743	+67%
Максимальный объем, Gbps	412	569	+38%
Максимальная скорость, Mpps	166	193	+16%

Выросли показатели и **максимального объема и скорости атак** — с 412 до 569 Гбит/с и с 166 до 193 млн пакетов в секунду — на 38% и 16% соответственно. А самыми популярными атаками стали **TCP SYN Flood** и **TCP PSH/ACK Flood**. Их доля в общем объеме к концу года увеличилась с 60% **до 87% всех инцидентов**.
При этом атаки UDP Flood, занимавшие в 2024 году до 26%, практически исчезли — лидерство перехватил **TCP SYN Flood**, увеличив долю **до 65%.**

По результатам 2025 года мы наблюдаем рост всех ключевых показателей как в сравнении с первым полугодием, так и в сравнении с 2024 годом. Более заметным стал паттерн «зондирующих» и «ковровых» атак — слабых, но частотных. Они были направлены на разведку и обнаружение наиболее уязвимых элементов IT-инфраструктуры. После обнаружения таких целей злоумышленники проводят по ним длительные и мощные атаки. Это заметно как по общей длительности атак за период, так и по показателю максимального количества и длительности атак на одного клиента: 7 172 инцидентов и 863 часов соответственно.

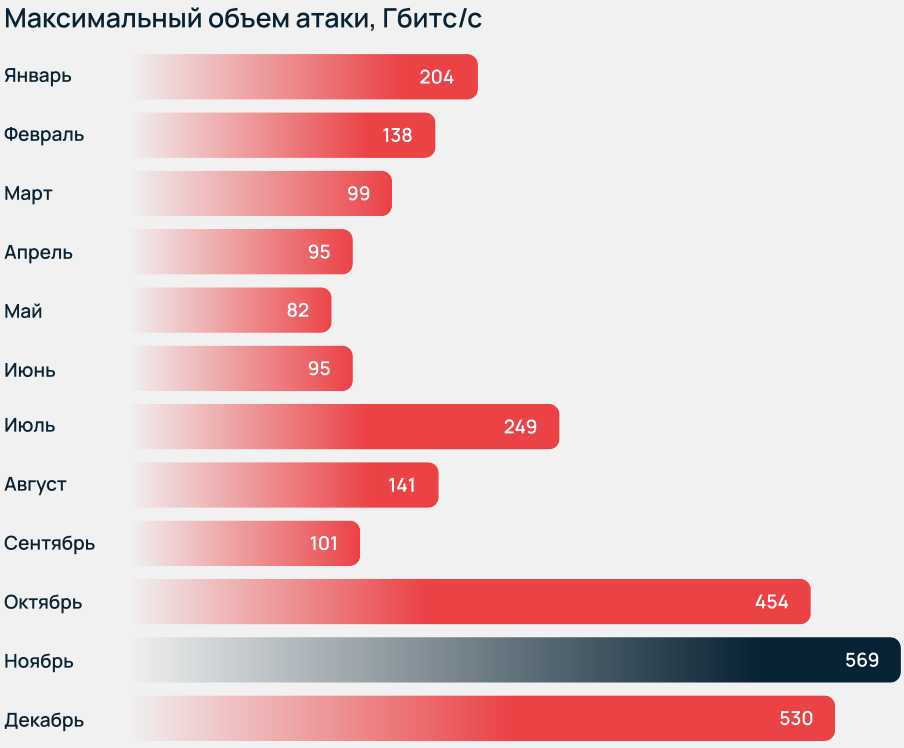
Антон Ведерников
Руководитель направления продуктовой безопасности

Сдвиг в сторону более продолжительных атак действительно заметен. Короткие всплески вредоносного трафика уступили место затяжным кампаниям — по данным DDoS-Guard, в 2025 году доминировали атаки длительностью 20–60 минут, а число многочасовых и сверхдолгих выросло на 25% и 17% соответственно.

Дмитрий Никонов
Директор по продуктам DDoS-Guard

Всего за 2025 год мы отразили **140 628 атак на клиентов облачной инфраструктуры**. Подобный объем невозможно отбить вручную, поэтому базовая бесплатная защита — **важная часть услуг облачного провайдера**.

Основные характеристики инцидента DDoS, определяющие его мощность на сетевом и транспортном уровнях, — **это объем и скорость**. Атаки большого объема, измеряемого в количестве переданных бит за одну секунду, направлены на переполнение полосы пропускания. **Максимальный объем зафиксирован в ноябре — 569 Гбит/с (+38 YoY)**, а **максимальная скорость — 193 млн пакетов в секунду (+16% YoY), зафиксирована в декабре**. Именно атаки с большой скоростью направлены на исчерпание вычислительных ресурсов сетевого оборудования.



Вместе с увеличением количества инцидентов выросла и их длительность. Общее время, в течение которого мы отражали активные атаки на наших клиентов, составило **22 743 часа**. Среднее время одной атаки менялось на протяжении года незначительно. В 2025 году показатель максимальной общей длительности атак на одного клиента достиг **863 часов** — почти 36 календарных дней (+75% YoY). Максимальное время одной атаки увеличилось до **353 часов** — это около 15 дней непрерывного воздействия (+75% YoY).

К концу года картина атак изменилась значительно: доля TCP SYN Flood увеличилась с 26% до 65%. Атаки типа TCP PSH/ACK Flood сократились до 22% с предыдущих 37%. Практически исчезли и атаки UDP Flood, в первом полугодии составлявшие 12%

Эксперты о трендах DDoS-атак

2025 год стал переломным в истории DDoS-атак. Многие компании в России и по всему миру впервые столкнулись с беспрецедентными вызовами. Мощность DDoS-атак теперь все чаще превышает значения, которые ранее считались рекордными. Причем рекорды бьют даже ковровые бомбардировки, которые ранее не демонстрировали таких объемов вредоносного трафика.
В России ситуация особенно тревожная: количество «зондирующих» атак, которые предваряют полномасштабную DDoS-атаку, стало больше в 5 300 раз, а их доля в общем объеме инцидентов по данным StormWall выросла в восемь раз — с 4% до 33%.

Это значит, что каждая третья атака начинается с разведки. Злоумышленники чаще действуют целенаправленно, а не хаотично. Политической мотивации стало меньше, а стремления заработать на атаке — больше. Главной мишенью злоумышленников в России остается телеком-сфера, которая находится в лидерах уже несколько лет. Рекордные по мощности сетевые DDoS-атаки направляются именно на телеком-компании. Также, по нашим данным, в тройку наиболее пострадавших отраслей в 2025 году в России вошли финансы и ритейл.

Рамиль Хантимиров
CEO и сооснователь StormWall

Повышенное внимание атакующих приковано к онлайн-играм — по данным DDoS-Guard, число инцидентов
в этом сегменте выросло на 310% (по сравнению с 2024 годом). Часто с помощью DDoS-атак ведется конкурентная борьба за аудиторию. С развитием ботнетов доступность такого инструмента только усилится, как и мощность самих атак и их влияние на индустрию.

Дмитрий Никонов
Директор по продуктам DDoS-Guard

Данные за 2025 год показывают качественный перелом в развитии DDoS-угроз. Речь уже идет не о постепенном росте мощности атак или усложнении отдельных техник, а о смене масштаба и логики атакующей инфраструктуры. DDoS окончательно закрепляется как инструмент нанесения прямого финансового ущерба и конкурентного воздействия, а не как демонстрация технических возможностей атакующих.

Ключевым риском становится экосистемная уязвимость. Доступность цифровых сервисов все чаще определяется не устойчивостью отдельной компании, а надежностью всей цепочки поставщиков — от облачных платформ и CDN до DNS-провайдеров и сторонних API. DDoS-атаки будут все чаще нацелены на конечный бизнес не напрямую, а на элементы его экосистемы, создавая каскадные сбои и эффект домино, при котором один успешный инцидент приводит к недоступности десятков сервисов и затрагивает компании, не являвшиеся изначальной целью атаки.

Эдгар Микаелян
Директор по клиентским решениям CURATOR

DDoS-атаки во II полугодии 2025 года

Подробный анализ статистики по DDoS-атакам за второе полугодие 2025 года указывает на наличие **тенденции к резкому увеличению объема и скорости атак**, а также значительному **росту их количества и длительности** относительно первого полугодия.

79 416	13 091	569	193
атак	часов	Gbps	Mpps

За период с июля по декабрь 2025 года бесплатным сервисом защиты от DDoS были отражены **79 416 атак общей продолжительностью 13 091 часов**. Максимальный объем атаки составил 569 Гбит/с, а скорость — 193 млн пакетов в секунду. В среднем мы отражали 13 236 атак ежемесячно, а самыми популярными были инциденты типа TCP SYN Flood и TCP PSH/ACK Flood, которые занимают 87% от общего числа атак.

Динамика изменения показателей год к году (YoY)

	H1 2025	H2 2025	YoY
Количество атак	61 612	79 416	+29%
Общая длительность, ч	9 652	13 091	+36%
Максимальный объем, Gbps	204	569	+179%
Максимальная скорость, Mpps	100	193	+93%

Аналитика атак

Количество

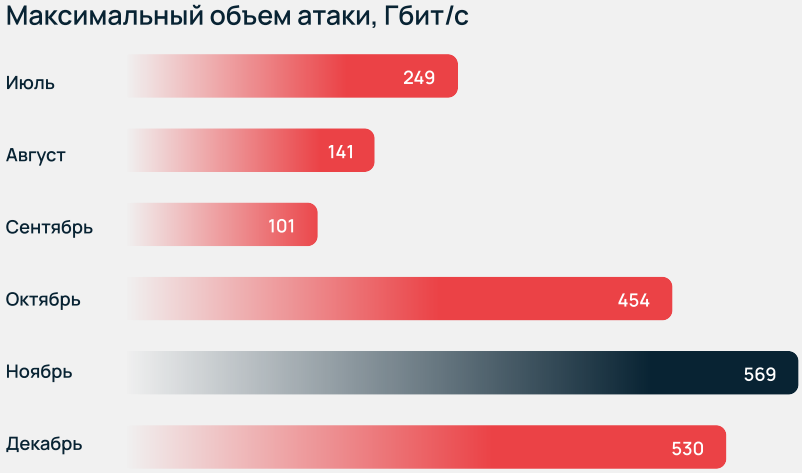
За период с июля по декабрь бесплатным сервисом защиты от DDoS-атак Selectel были отражены **79 416 атак**. При этом наибольшее число инцидентов пришлось на июль. В среднем мы отражали **13 236 атак в месяц** и **64 — на каждого атакованного клиента**.

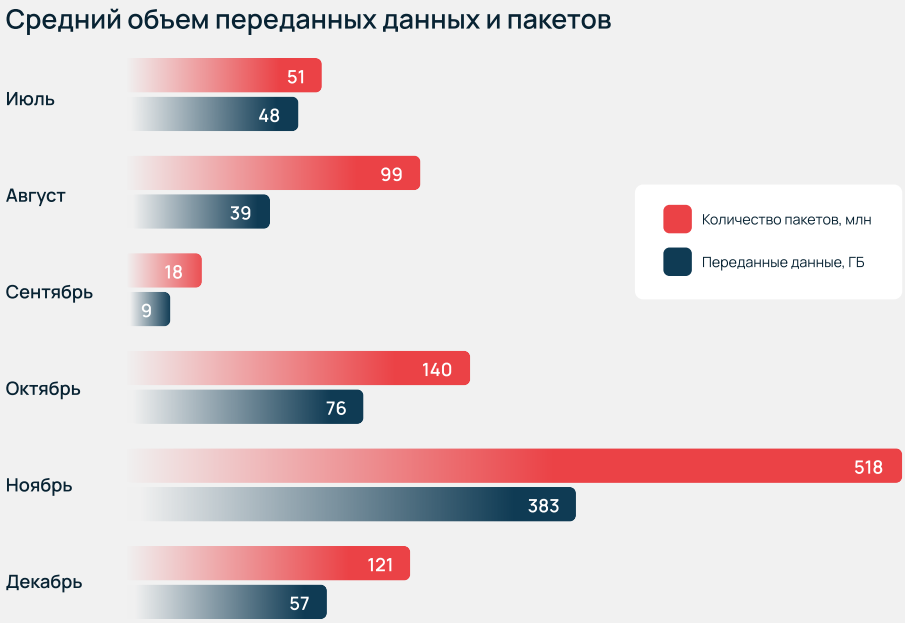
Общее количество атак на инфраструктуру

Максимальное количество атак на одного клиента во втором полугодии 2025 года изменялось незначительно и в среднем составляло **6 321 инцидент**. А наибольшее значение пришлось на декабрь — **7 172 инцидента**.

Мощность

Наибольший объем был достигнут **в ноябре** и составил **569 Гбит/с**. Наравне с максимальным объемом атаки, в ноябре достигли своего максимума и другие показатели. Наибольшее значение среднего объема переданных данных за атаку достигло **383 Гб**, а максимальное количество переданных пакетов — **518 млн**. Различие с другими месяцами составляет **42 и 28 раз** соответственно.



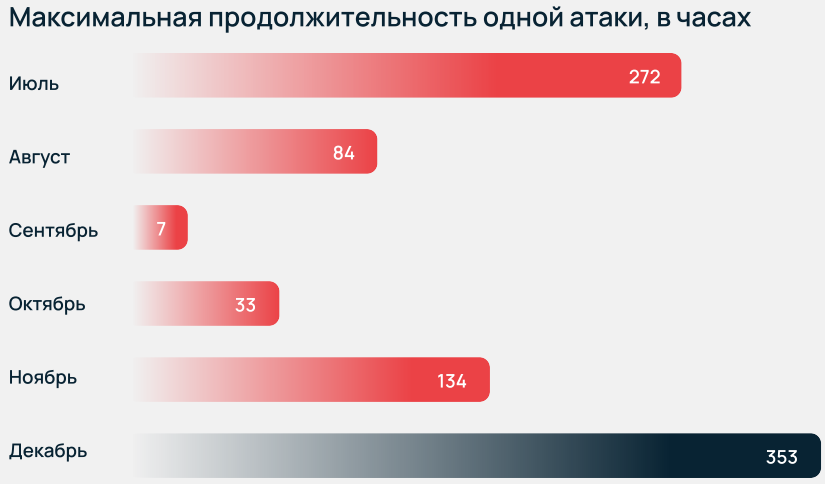


Самая скоростная атака была зафиксирована **в декабре** и достигла **193 миллионов пакетов в секунду**. Это почти в восемь раз больше, чем максимальная скорость атаки в июле.

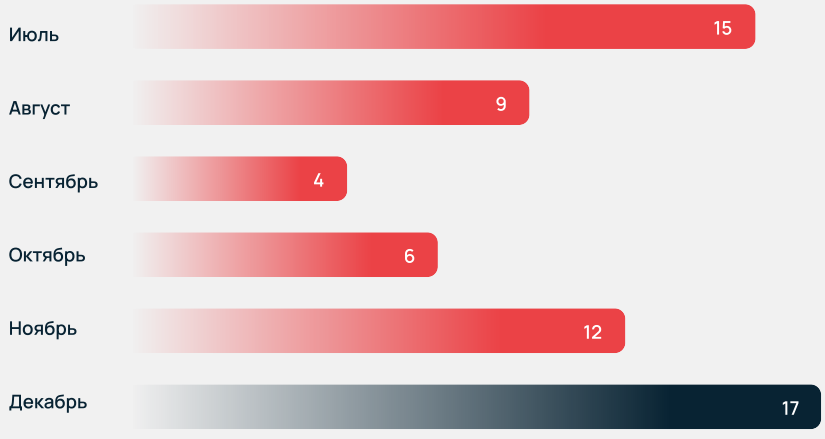
Продолжительность

Суммарная продолжительность атак с июля по декабрь 2025 года составила **13 091 час**. А наибольшая продолжительность зарегистрирована **в декабре** и достигает **4 159 часов**. При этом заметны значительные изменения показателя от месяца к месяцу.

За исключением декабря, средняя длительность атаки не превышала **11 минут**, а максимальная как раз зафиксирована **в декабре** и составляет **353 часа**, что в 50 раз больше значения сентября.



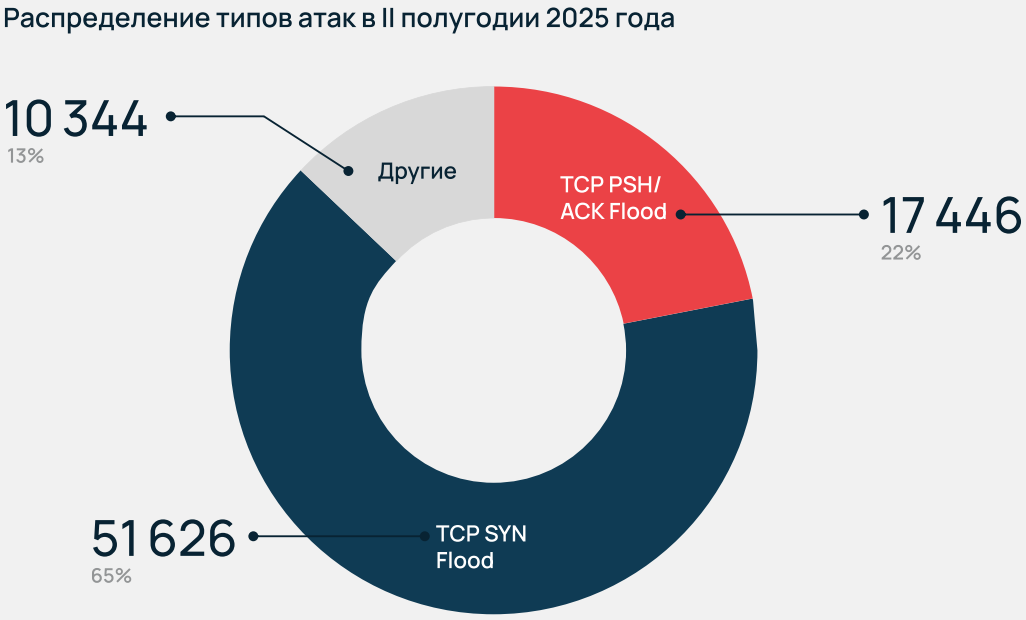
Средняя общая продолжительность атак на одного клиента не превышала **17 часов**. Максимальная же превысила **863 часа за один календарный месяц**, захватив начало следующего периода.



Средняя общая продолжительность атак на одного клиента не превышала **17 часов**. Максимальная же превысила **863 часа за один календарный месяц**, захватив начало следующего периода.

Типы атак

Распределение типов атак по месяцам менялось незначительно. Самыми популярными были атаки типа **TCP SYN Flood** и **TCP PSH/ACK Flood**. Они занимают 87% от общего количества атак. Заметно увеличилась доля атак **TCP SYN Flood**, которая составила 65% от общего количества, при этом атаки UDP Flood практически исчезли.



Заметно изменился и вектор — теперь это TCP, что отражает и общемировую тенденцию. Косвенно это можно связать и с ростом HTTP/API-атак, в основе которых лежит установление TCP-соединений. Доля UDP снижается из-за относительно простого обнаружения и блокировки, но такие атаки все еще есть и бывают довольно мощными.

Актуальная статистика подтверждает, что предельные значения мощности достаточно велики, и не вся on-premise инфраструктура способна с этим справиться. Также можно сказать, что DDoS-атаки окончательно перешли от разовых инцидентов в разряд постоянных операционных рисков для бизнеса, а кратковременность «зондирующих» и «ковровых» атак делает реактивный ручной подход бесполезным — к моменту подключения защиты атака будет завершена.

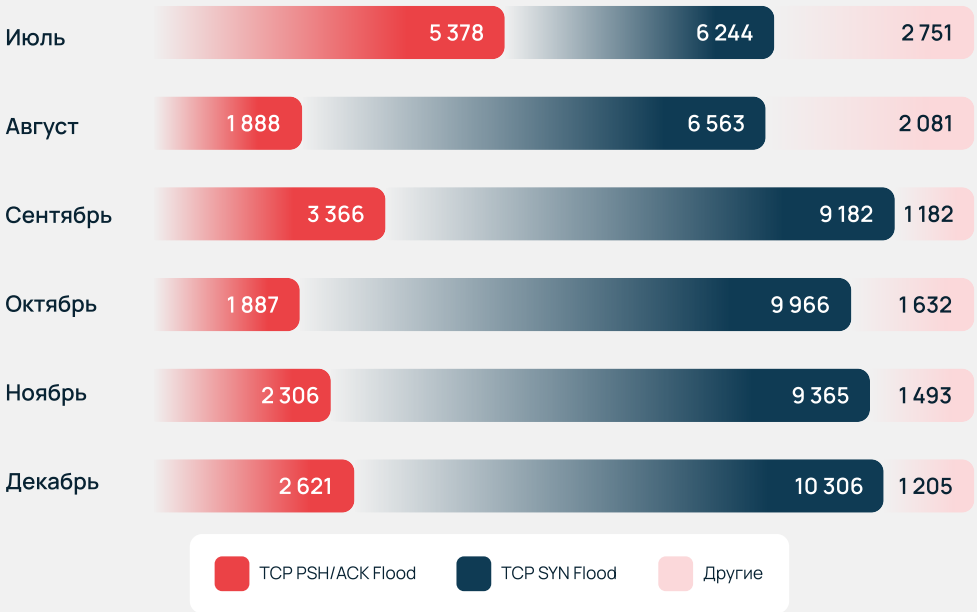
Для эффективного противодействия необходимо переходить к концепции киберустойчивости и проактивного подхода защиты: пересматривать архитектуру своих сервисов, использовать балансировку и геораспределенность, изолировать критичные служебные сервисы, использовать постоянную защиту от DDoS-атак с динамической адаптацией правил фильтрации.

Антон Ведерников
Руководитель направления продуктовой безопасности

TCP SYN Flood реализуется путем отправки множества SYN-запросов на подключение, при этом ответные SYN+ACK пакеты, отправленные сервером, игнорируются. Это приводит к тому, что на сервере появляется очередь из полуоткрытых соединений, которые не позволяют установить новые (легальные) подключения. Как следствие — легитимные пользователи не могут подключиться или сталкиваются с длительным ожиданием ответа.

TCP PSH/ACK Flood реализуется путем отправки множества фальсифицированных ACK-пакетов на определенные или случайные номера портов атакуемого узла, которые не принадлежат ни одной из сессий в списке соединений. Тот, в свою очередь, вынужден тратить вычислительные ресурсы на проверку поддельных пакетов.

Распределение типов атак по месяцам



Методология

Основной источник данных для отчета — **системы защиты от DDoS-атак**, которые мы используем на уровне сетевой инфраструктуры дата-центров Selectel. Весь входящий трафик проходит через узлы очистки и анализируется на наличие вредоносной активности.

Нелегитимные запросы отбрасываются — поступает только очищенный входящий трафик. Обладая информацией об исходящем трафике, система использует дополнительные алгоритмы, которые повышают точность фильтрации при TCP-атаках до 99,9%.

Сервис защиты от DDoS-атак Selectel

Бесплатный сервис защиты от DDoS-атак работает при использовании облачной платформы Selectel, платформенных сервисов, выделенных серверов, включая аттестованные сегменты.

Сервис обеспечивает защиту **на сетевом (L3) и транспортном (L4) уровнях** от:

- атак с отражением на основе UDP (DNS, NTP, memcache и пр.),
- атак с использованием фрагментированного IP-трафика,
- TCP SYN/RST/PSH flood,
- различных типов UDP flood и ICMP flood.

Отдельной атакой считается вредоносная активность, которая направлена на конкретный IP-адрес, относится к одному типу атак и имеет перерывы в активности не более трех минут.

Пример 1. Атаки UDP Flood на один и тот же IP-адрес с промежутком в минуту будут объединены в одну. В течение трех минут после прекращения активности атака будет считаться завершенной.

Пример 2. Одновременно один и тот же IP-адрес атакуют с помощью Flood- и Reflection-атак. Активность продолжается в течение семи минут. В данном случае будет зафиксировано две атаки

Подробнее о том, как работает бесплатный сервис защиты от DDoS, можно узнать на странице. Посмотрим, какие данные об атаках соберет система в 2026 году. **Следите за обновлениями и новостями в Security Center.**