StormWall

Ландшафт DDoS-атак **и современные инструменты противодействия**

Дмитрий **Белянин**
Руководитель направления Pre-sale,
StormWall

StormWall — это

Защита от **DDoS- и хакерских атак**

11 лет на рынке

1 000+ клиентов

Российская разработка

Актуальные **киберугрозы**

- DDoS-атаки
- Боты, автоматизированные действия
- Переборные атаки

- Атаки на API
- Неправильная конфигурация серверов, сетей или приложений
- Целевые атаки на веб-системы по методологии OWASP Top 10

Атаки на L3-L4 и L7: разница

Особенности	L3-L4	L7
Цель	Перегрузка пропускной способности сетевых ресурсов	Истощение ресурсов приложения и производительности сервера
Разновидности атак	SYN Flood, UDP Flood, DNS Amplification	HTTP Flood, Slowloris, Application-Specific Attacks
Сложность обнаружения	Легко обнаружить	Более сложно обнаружить
Трафик	Большой объём и часто нелегитимный	Запросы из множества источников, кажущиеся легитимными
Потребление ресурсов	Истощение пропускной способности сети	Истощение ресурсов сервера и приложения
Воздействие на сервисы	Нарушение доступности сети	Замедляют или полностью останавливают отдельные сервисы
Примеры атак	DNS Amplification, UDP Flood, SYN Flood	HTTP floods, целевые атаки на приложение

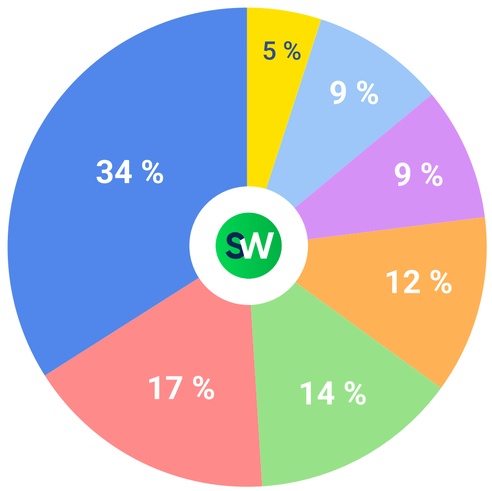
DDoS-атаки в России в 2024*

Прирост DDoS-атак **в 2024 году** по сравнению с 2023:

Q1 — **73 %**
Q2 — **76 %**
Q3 — **103 %**

- Россия **вошла в 10-ку** стран, наиболее пострадавших от DDoS-атак
- Общий прирост атак в России в 2024 — **85%**
- Нами обнаружен ботнет мощностью в **1.5 Тбит/с** из **более 100 тыс. устройств**
- На **L7** приходятся **90% DDoS-атак**

Статистика DDoS-атак **по отраслям**



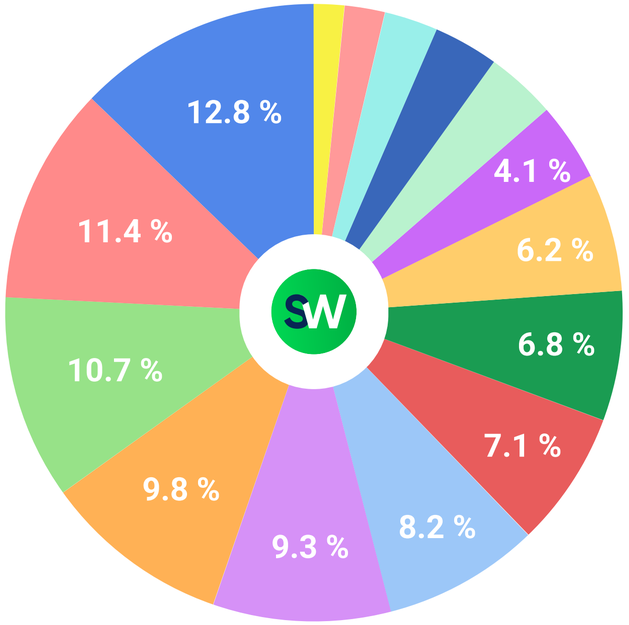
Телекоммуникации	34 %
Образование	17 %
Ритейл	14 %
Госсектор	12 %
Сфера развлечений	9 %
Энергетика	9 %
Другое	5 %

** Квартальные отчёты StormWall о DDoS-атаках, 2024 г.*

DDoS-атаки в мире **в 2024***

- Многовекторные атаки выросли на **142%**
- **4 из 5** DDoS-атак — многовекторные
- Рост ковровых бомбардировок — **237%**
- Рост количества DNS-атак — **62%**

Статистика DDoS-атак **по странам**

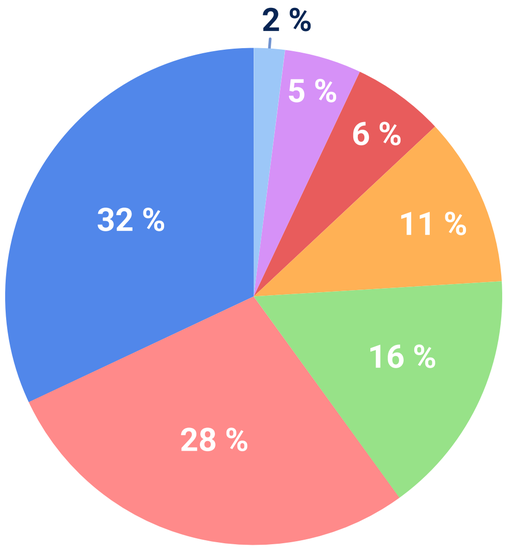


США	12.8 %
Индия	11.4 %
Китай	10.7 %
Великобритания	9.8 %
Австрия	9.3 %
Франция	8.2 %
Израиль	7.1 %
ОАЭ	6.8 %
Россия	**6.2 %**
Сингапур	4.1 %

** Квартальные отчёты StormWall о DDoS-атаках, 2024 г.*

Векторы атак на L3-L4 за 2024*

Распределение типов DDoS-атак



Атаки на L3/L4

DNS Flood	32 %
UDP Flood	28 %
SYN Flood	16 %
TCP Flood	11 %
SYN/ACK Flood	5 %
ICMP Flood	2 %
Другие	6 %

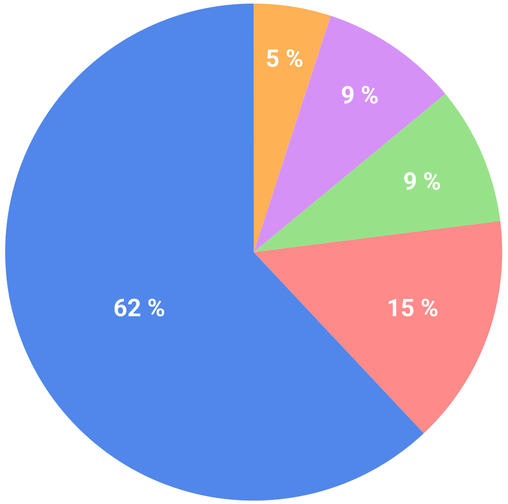
Продолжительность атак на уровне сети

Менее 10 минут	78 %
10-30 минут	8 %
30-60 минут	6 %
1-3 часа	5 %
Более 3 часов	3 %

*по состоянию на ноябрь 2024

Векторы атак **на L7 за 2024***

Распределение **типов DDoS-атак**



Атаки на L7

HTTP Flood	62 %
Application-Specific Attacks	15 %
Slowloris	9 %
Slow Read Attacks	5 %
Другие	9 %

Продолжительность атак **на уровне приложений**

Менее 10 минут	82 %
10-30 минут	5 %
30-60 минут	4 %
1-3 часа	2 %
Более 3 часов	7 %

*по состоянию на ноябрь 2024

Почему DDoS-атаки на L7 **сложно обнаружить и фильтровать**

1. **Маскировка** трафика:

Затрудняется выявление угроз для систем, основанных на детекции объёма трафика, так как вредоносный трафик часто имитирует легитимные запросы.

2. **Сложность** протоколов прикладного уровня:

Традиционные решения безопасности часто не обладают достаточными возможностями для глубокого анализа пакетов.

3. **Адаптивные** подходы:

Злоумышленники меняют паттерны запросов и используют техники для обхода средств защиты. Такая адаптивность затрудняет блокирование вредоносного трафика без ущерба для легитимных пользователей.

4. **Недостаточная** защита:

Многие организации, использующие определённый комплекс услуг, всё равно недостаточно подготовлены к защите от киберугроз. Например, неправильная конфигурация механизмов защиты WAF делает системы уязвимыми для конкретных типов атак.

Эффективные стратегии защиты на L7

Облачные решения:

Использование различных интеллектуальных механизмов на высоких скоростях для обнаружения и устранения объёмных и целевых атак в реальном времени из любой точки мира.

Антибот:

Защита веб-сайтов от автоматического вмешательства на основе анализира сетевой, браузерной и поведенческой информации пользователя.

Ограничение скорости и регулировка запросов:

Контроль объёма и скорости запросов с целью недопустить перегрузки ресурса и защитить его от HTTP-флуда.

CAPTCHA и JavaScript-проверки:

Предотвращение действий ботов, таких как массовая загрузка больших файлов или автоматическая отправка форм.

Таргетирование и фильтрация на основе репутации IP:

Применение ограничений для списка скомпроментированных IP-адресов, полученных из систем анализа и интерпретации данных.

Поведенческая аналитика и машинное обучение:

Формирование паттерна типового трафика и выявление в нём аномалий.

Межсетевые экраны веб-приложений (WAF):

Защита веб-приложений от DDoS-атак с помощью анализа HTTP-трафика и блокировки вредоносных запросов.

Какой функционал должен иметь **современный anti-DDoS сервис**

Комплексное решение на L3-L7	Для защиты от целевых и многовекторных атак
Защита от ботов (Антибот)	Предотвращение активности всех вредоносных ботов
Возможность настройки силами вендора	Чтобы не тратить ресурсы и время на технические вопросы
Личный кабинет для контроля защиты	Прозрачность и управление защитой в реальном времени
Функционал и настройки без ограничений	Гибкость защиты для любых бизнес-задач
Масштабируемость защиты	Адаптация под рост нагрузки и увеличение объёма атак
Быстрая поддержка	Оперативная помощь 24/7
Отечественная разработка	Нет опасности ухода вендора с рынка

К чему готовиться в 2025

Ключевые тенденции:

- Начинается переход от зарубежных ИБ-вендоров к российским
- Увеличивается мощность атак с ростом количества устройств в ботнетах
- Злоумышленники активно используют ИИ для эволюционирования угроз
- APT-группы будут чаще проводить атаки с использованием IoT
- Ужесточение ответственности за утечку персональных данных
- Рост попыток встраивания вредоносного кода в популярные решения open source

Что делать в новом 2025 году:

- Адаптироваться к нормативным требованиям РФ: уходить от иностранных вендоров, выбирать отечественного вендора со всеми лицензиям (ТЗКИ, СЗКИ, телематические услуги)
- Выбирать решения с масштабированием, мониторингом и автоматическим реагированием на угрозы
- Использовать эшелонированный подход: DDoS + защита от хакерских атак
- Тщательно подходить к вопросу защиты ключевых ресурсов

StormWall

8 800 550-89-39 stormwall.pro

Спасибо за внимание!

Розыгрыш мерча на нашем стенде

Для участия отсканируйте **код**

Начинаем в **16.15**