

# Система защиты от DDoS атак на основе анализа логов

Цель:

- Обеспечение кибер-защиты от DDoS атак.

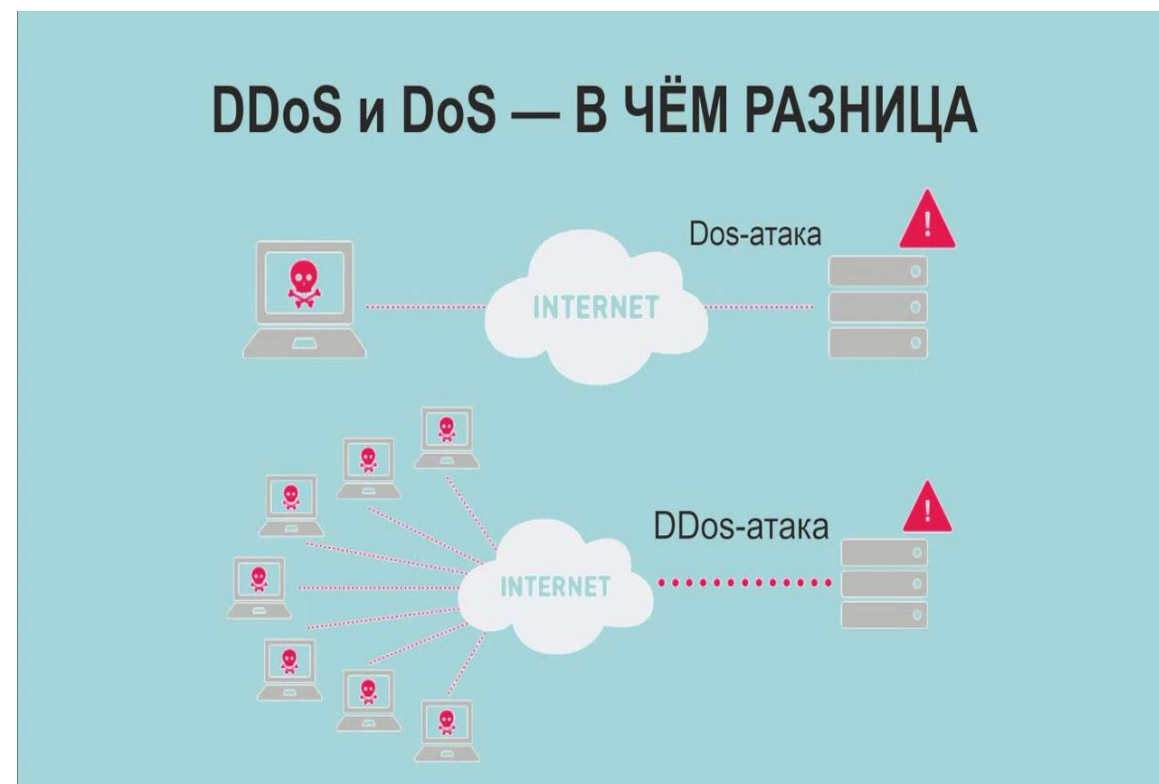
Задачи:

- Рассмотреть существующие средства анализа логов.
- Провести сравнительный анализ существующих программных решений и сделать выводы.
- Разработать ПО, способное к автономному функционированию, а также, на основе данных логов, способное определить нагрузочные атаки на сайт (DDoS) и провести контрмеры.

# DoS и DDoS атаки

**DoS атака (отказ в обслуживании)** – это атака, приводящая к парализации работы сервера или ПК вследствие огромного количества запросов, с высокой скоростью поступающих на атакуемый ресурс.

**DDoS атака (распределённый отказ в обслуживании)** – это разновидность DoS атаки, которая организуется с помощью большого числа компьютеров, именуемых “зомби”, из-за чего атаке могут быть подвержены серверы даже с очень большой пропускной способностью каналов.



# Зачем нужны DDoS атаки

**Главная цель любой DDoS атаки** – вывести атакуемый ресурс из строя. Тем самым осуществив простой ресурса или потерю репутации владельцев.

Осуществляются атаки с помощью таких запросов, как:

- флуд;
- пустые запросы;
- случайные поисковые запросы, и т.д.

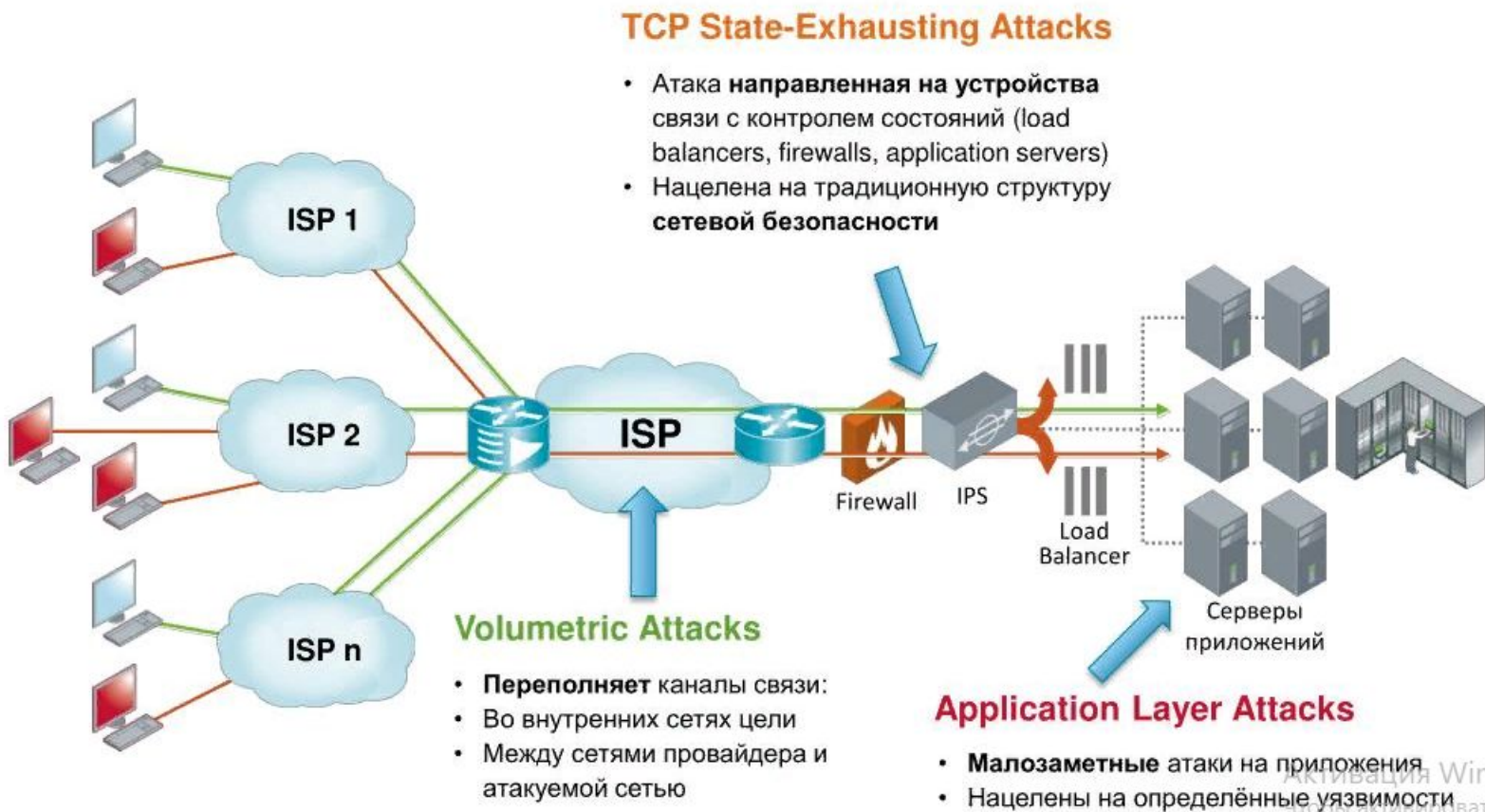


# Виды DDoS атак

Как и какие части сетевой инфраструктуры атакуют?

Атаки разделяются на три основных вида, по принципу воздействия:

- **Переполнение канала** — это ICMP-флуд, UDP-флуд, DNS-амплификация.
- **Использование незащищенности стека сетевых протоколов** — «пинг смерти», ACK/PUSH ACK-флуд, SYN-флуд, TCP null/IP null атака.
- **Атака на уровне приложений** — HTTP-флуд, медленные сессии, фрагментированные HTTP-пакеты.



# Как защищаться от DDoS атак?

**Основной способ защиты** – фильтрация трафика на основе его содержимого, IP-адресов и других параметров. Реализовать его можно двумя путями:

- Установить собственный сервер и программное обеспечение. Такой подход позволяет не зависеть от третьих лиц и позволяет полностью контролировать свою инфраструктуру, настраивая все под собственные нужды.
- Приобрести защиту от DDoS в виде услуги у сторонней компании. Этот путь дает возможность снизить издержки на обслуживание своего оборудования, снимает необходимость в найме профильных специалистов безопасности внутри компании.

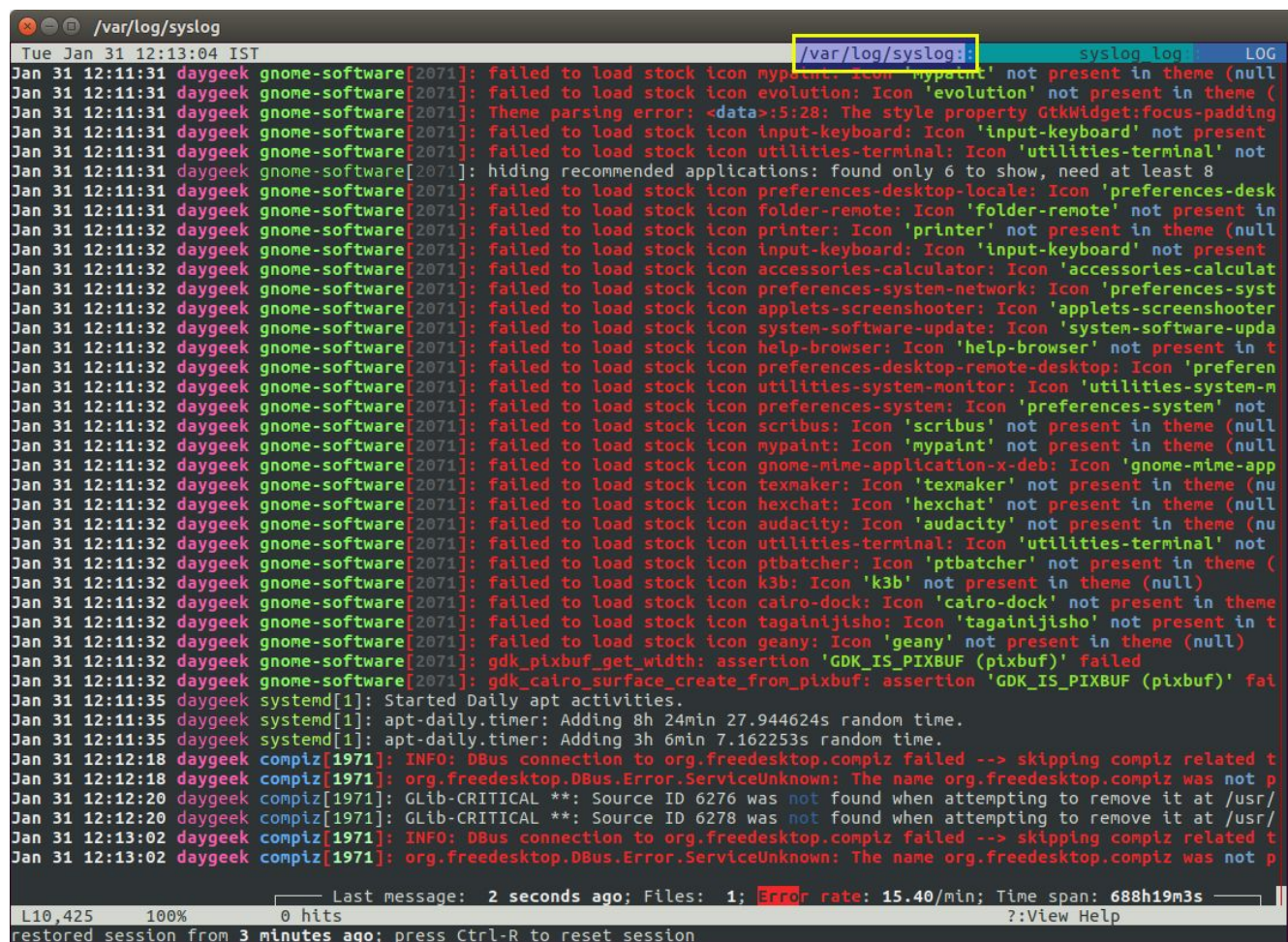


[Заказать защиту от DDoS атак](#)

# Анализ логов

Логи (log) – это специальные текстовые файлы, в которых в хронологическом порядке фиксируется информация обо всех действиях программы или пользователей. Проще говоря, это журнал регистрации всех событий происходивших в системе:

- **ошибки сервера (сбои)**, возникающие при обращении к некоторым функциям сайта или задачам;
- **данные о доступе** – запись о подключении (или попытке входа) каждого пользователя, откуда и как он попал на сайт;
- **прочие**, записывающие информацию о работе компонентов сервера.



```

Tue Jan 31 12:13:04 IST
Jan 31 12:11:31 daygeek gnome-software[2071]: failed to load stock icon mypaint: Icon 'mypaint' not present in theme (null)
Jan 31 12:11:31 daygeek gnome-software[2071]: failed to load stock icon evolution: Icon 'evolution' not present in theme (
Jan 31 12:11:31 daygeek gnome-software[2071]: Theme parsing error: <data>:5:28: The style property GtkWidget:focus-padding
Jan 31 12:11:31 daygeek gnome-software[2071]: failed to load stock icon input-keyboard: Icon 'input-keyboard' not present
Jan 31 12:11:31 daygeek gnome-software[2071]: failed to load stock icon utilities-terminal: Icon 'utilities-terminal' not
Jan 31 12:11:31 daygeek gnome-software[2071]: hiding recommended applications: found only 6 to show, need at least 8
Jan 31 12:11:31 daygeek gnome-software[2071]: failed to load stock icon preferences-desktop-locale: Icon 'preferences-desk
Jan 31 12:11:31 daygeek gnome-software[2071]: failed to load stock icon folder-remote: Icon 'folder-remote' not present in
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon printer: Icon 'printer' not present in theme (null
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon input-keyboard: Icon 'input-keyboard' not present
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon accessories-calculator: Icon 'accessories-calculat
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon preferences-system-network: Icon 'preferences-syst
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon applets-screenshooter: Icon 'applets-screenshooter
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon system-software-update: Icon 'system-software-upda
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon help-browser: Icon 'help-browser' not present in t
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon preferences-desktop-remote-desktop: Icon 'preferen
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon utilities-system-monitor: Icon 'utilities-system-m
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon preferences-system: Icon 'preferences-system' not
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon scribus: Icon 'scribus' not present in theme (null
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon mypaint: Icon 'mypaint' not present in theme (null
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon gnome-mime-application-x-deb: Icon 'gnome-mime-app
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon texmaker: Icon 'texmaker' not present in theme (nu
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon hexchat: Icon 'hexchat' not present in theme (null
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon audacity: Icon 'audacity' not present in theme (nu
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon utilities-terminal: Icon 'utilities-terminal' not
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon ptbatcher: Icon 'ptbatcher' not present in theme (
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon k3b: Icon 'k3b' not present in theme (null)
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon cairo-dock: Icon 'cairo-dock' not present in theme
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon tagainijisho: Icon 'tagainijisho' not present in t
Jan 31 12:11:32 daygeek gnome-software[2071]: failed to load stock icon geany: Icon 'geany' not present in theme (null)
Jan 31 12:11:32 daygeek gnome-software[2071]: gdk_pixbuf_get_width: assertion 'GDK_IS_PIXBUF (pixbuf)' failed
Jan 31 12:11:32 daygeek gnome-software[2071]: gdk_cairo_surface_create_from_pixbuf: assertion 'GDK_IS_PIXBUF (pixbuf)' fai
Jan 31 12:11:35 daygeek systemd[1]: Started Daily apt activities.
Jan 31 12:11:35 daygeek systemd[1]: apt-daily.timer: Adding 8h 24min 27.944624s random time.
Jan 31 12:11:35 daygeek systemd[1]: apt-daily.timer: Adding 3h 6min 7.162253s random time.
Jan 31 12:12:18 daygeek compiz[1971]: INFO: DBus connection to org.freedesktop.compiz failed --> skipping compiz related t
Jan 31 12:12:18 daygeek compiz[1971]: org.freedesktop.DBus.Error.ServiceUnknown: The name org.freedesktop.compiz was not p
Jan 31 12:12:20 daygeek compiz[1971]: Glib-CRITICAL **: Source ID 6276 was not found when attempting to remove it at /usr/
Jan 31 12:12:20 daygeek compiz[1971]: Glib-CRITICAL **: Source ID 6278 was not found when attempting to remove it at /usr/
Jan 31 12:13:02 daygeek compiz[1971]: INFO: DBus connection to org.freedesktop.compiz failed --> skipping compiz related t
Jan 31 12:13:02 daygeek compiz[1971]: org.freedesktop.DBus.Error.ServiceUnknown: The name org.freedesktop.compiz was not p

Last message: 2 seconds ago; Files: 1; Error rate: 15.40/min; Time span: 688h19m3s
0 hits
restored session from 3 minutes ago; press Ctrl-R to reset session
?:View Help
```

# Программы анализа

## Инструменты анализа логов:

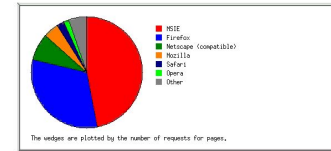
- Analog 6.0
- Apache Log Analyzer 1.0
- Sawmill Enterprise 8.6.2
- WebSpy Vantage Ultimate 2.2.0.84
- WebLog Expert Lite 8.1
- OSSEC
- Prelude Semi



### Browser Summary

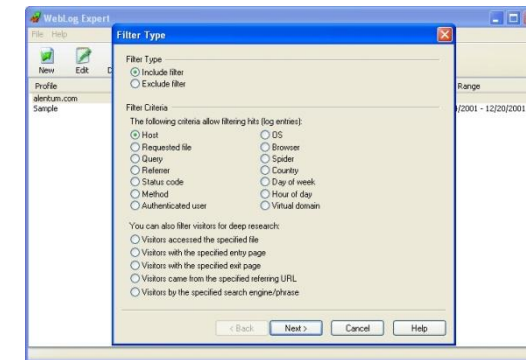
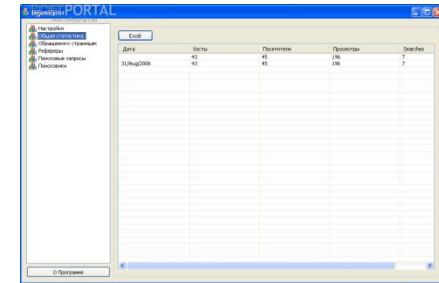
(Go To: Top | Overall Summary | Monthly Report | Daily Report | Hourly Summary | Organization Report | Referrer Report | Search Word Report | Report | Filter Report | Request Report)

This report lists the vendors of visitors' browsers.



Listing the top 20 browsers by the number of requests for pages, sorted by the number of requests for pages.

Rank	Browser	Pages	Requests
1	MSIE	36125	34518
2	Firefox	22121	20518
3	Mozilla	3020	28518
4	Safari	1000	9518
5	Opera	1000	9518
6	Other	1000	9518



# Сравнение инструментов анализа

Название	Уровень доступа	ОС	Тип инструмента	Автономность	Определение угроз	Конфигурирование	Интерфейс	Тип интерфейса
Analog 6.0	open-source	Cross platform	Анализатор	+	-	+	+	Console + html отчёт
Apache Log Analyzer 1.0	open-source	Windows	Анализатор	-	-	-	+	Windows+ xls
Sawmill Enterprise 8.6.2	Shareware	Cross platform	Анализатор	+	-	-	+	WEB
WebSpy Vantage Ultimate	Shareware	Windows	Анализатор	+	-	-	+	WEB
WebLog Expert Lite 8.1	Shareware	Windows	Анализатор	-	-	-	+	WEB
OSSEC	open-source	Cross platform	Система Обнаружения Вторжений	+	+	+	-	WEB-конфигурирование
Prelude Semi	open-source	Cross platform	Система Обнаружения Вторжений	+	+	+	-	От сторонних продуктов



# Принцип работы программы

