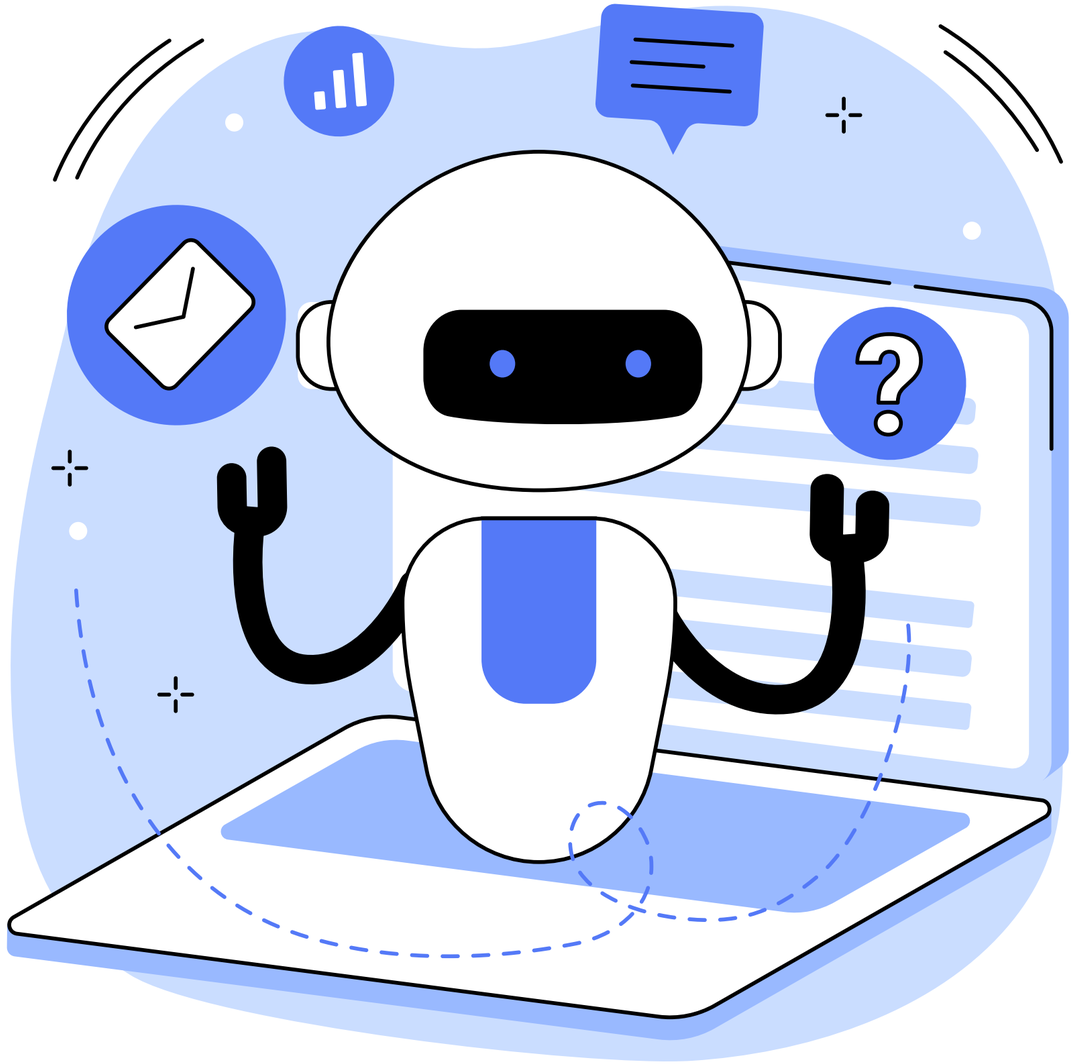
АРХИТЕКТУРА И ФУНКЦИОНИРОВАНИЕ DNS

Выполнила студентка группы НПИбд-01-22
Ситникова Диана Александровна
ст. б. №1032201746

СОДЕРЖАНИЕ

DOMAIN NAME SYSTEM

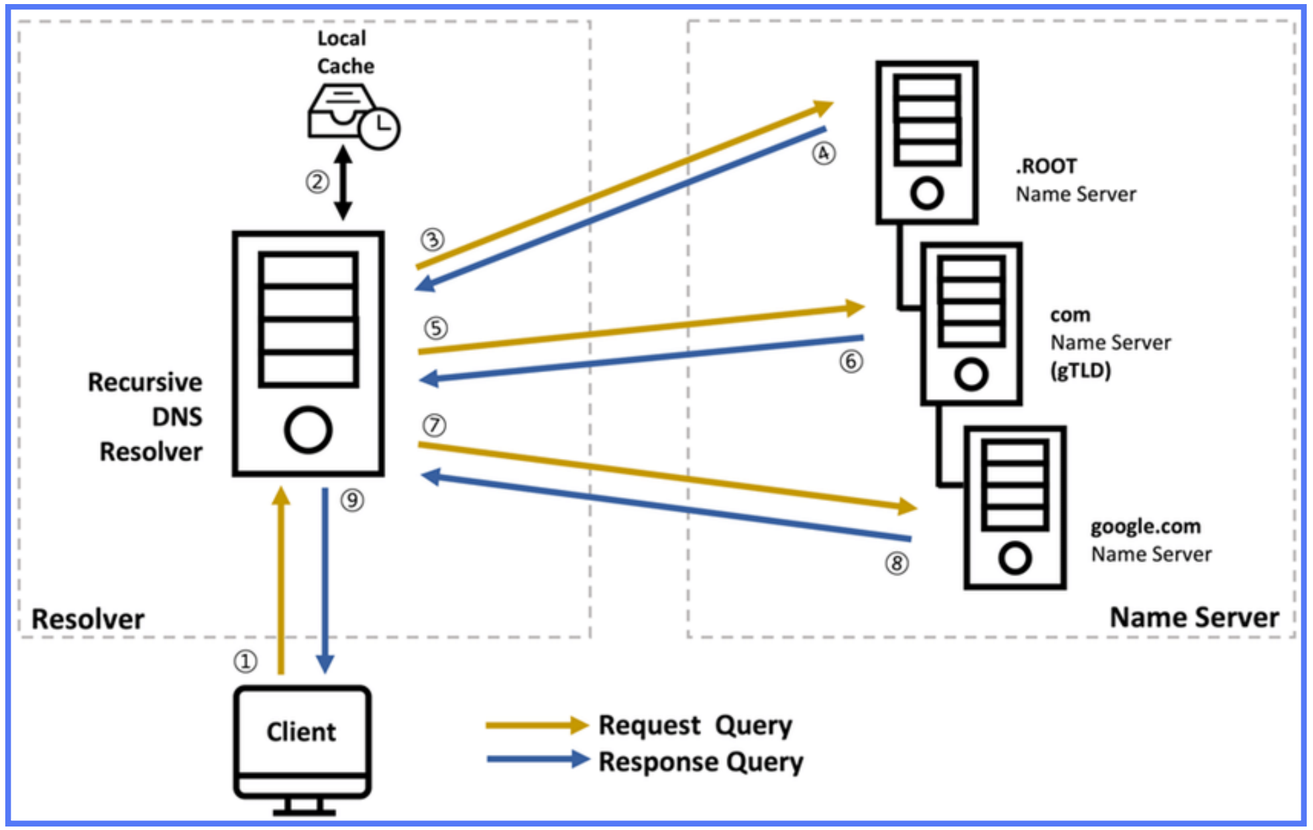
Архитектура DNS (Domain Name System) — это иерархическая и распределенная система, способная преобразовывать доменные имена в машинно-читаемые IP-адреса.



АРХИТЕКТУРА DNS

Корневые серверы (A, B, C и т.д.)

Авторитетные сервера (A, AAAA, MX, CNAME и т.д.)



Пространство имен DNS

Рекурсивные резольверы

Делегация зон

ФУНКЦИОНИРОВАНИЕ DNS

Ввод доменного имени

Рекурсивный револьвер

Кэширование

Запрос к корневым серверам

Получение информации о **TLD**

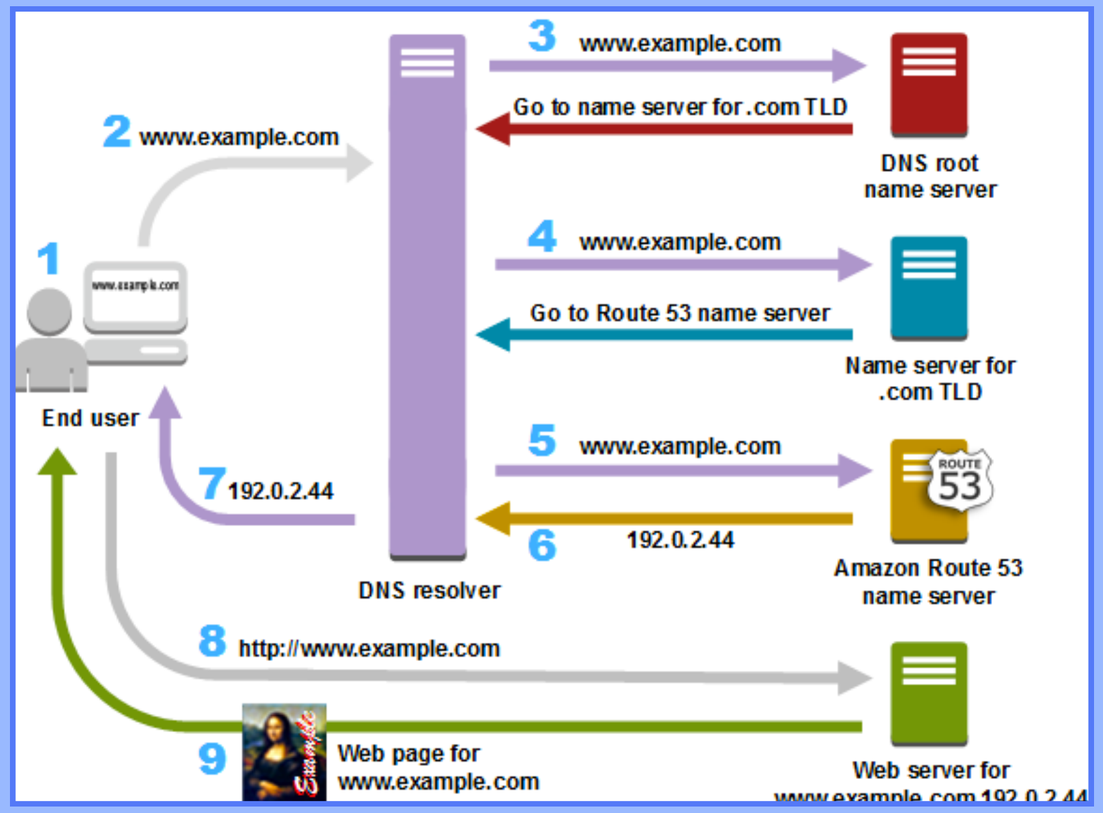
Запрос к серверам **TLD**

Установление связи

Возврат результата

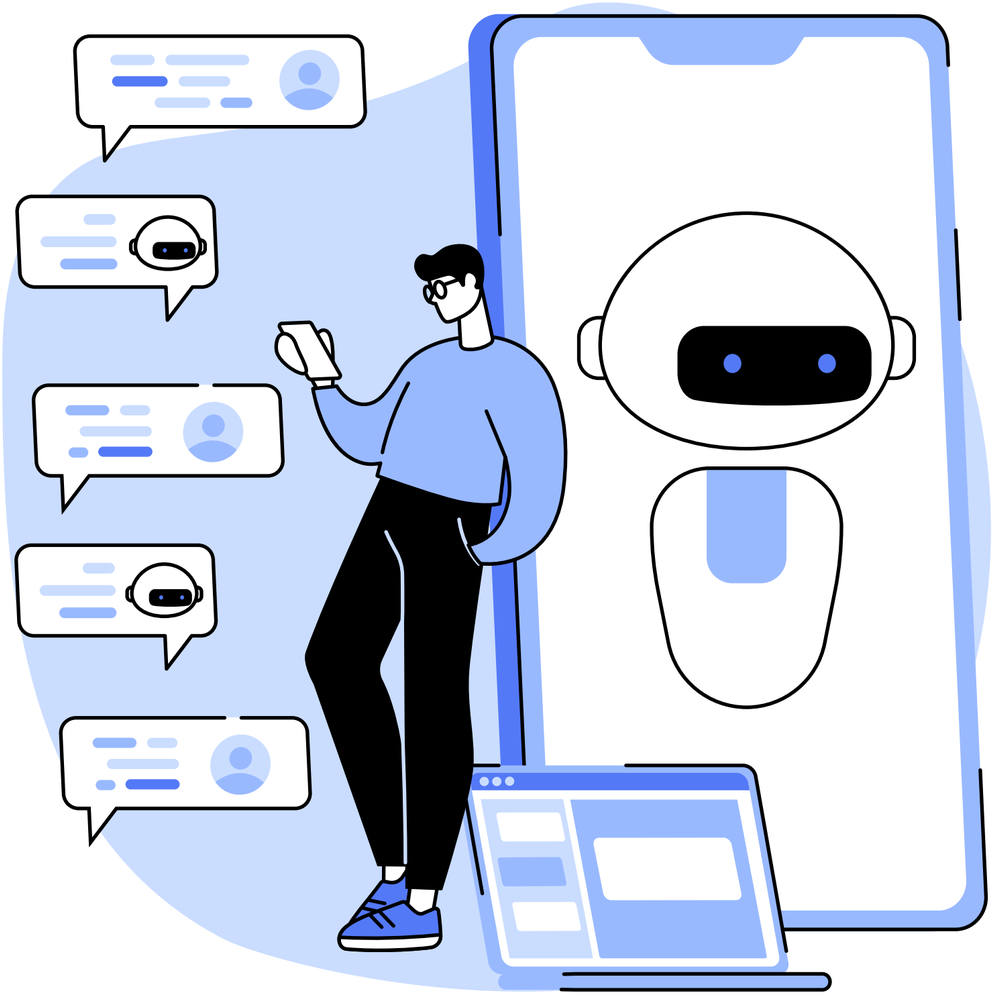
Получение ответа

Запрос к авторитетным серверам домена

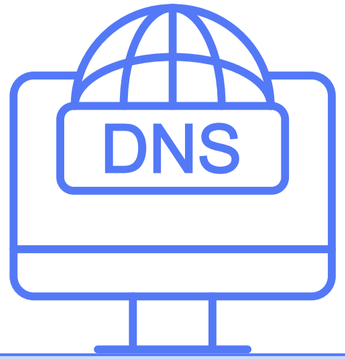


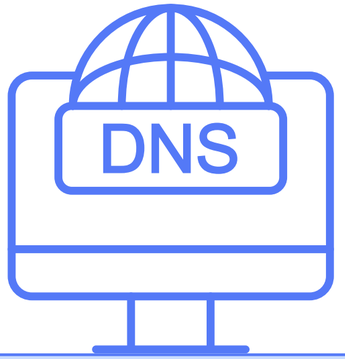
РЕСУРСНЫЕ ЗАПИСИ DNS

Ресурсные записи **DNS (Domain Name System)** представляют собой специальные записи в базе данных **DNS**, которые хранят информацию о доменах и связанных с ними ресурсах, включая **IP**-адреса, почтовые серверы и другие службы.



ТИПЫ РЕСУРСНЫХ ЗАПИСЕЙ DNS





A
(Address)

Устанавливает соответствие между доменным именем и IPv4-адресом, что позволяет маршрутизаторам найти соответствующий ресурс

AAAA
(IPv6 Address)

Аналогично записи A, но используется для связи с IPv6-адресами

CNAME
(Canonical Name)

Позволяет создавать альтернативные доменные имена для существующих, что упрощает управление ресурсами

MX
(Mail Exchanger)

Указывает, какой почтовый сервер должен принимать электронные письма для домена

БЕЗОПАСНОСТЬ DNS

DNS подвержен различным угрозам, включая мошенничество, атаки распределенного отказа в обслуживании (**DDoS**), отравление кэша **DNS** и другие виды атак. Для защиты **DNS** и обеспечения его безопасности принимаются различные меры и используются стандарты.

АСПЕКТЫ БЕЗОПАСНОСТИ DNS

DNSSEC (Domain Name System Security Extensions)

Он предоставляет механизмы для проверки целостности и аутентичности DNS-записей.

DNS-over-HTTPS (DoH) и DNS-over-TLS (DoT)

Эти технологии обеспечивают защищенное и конфиденциальное соединение между клиентами и DNS-резольверами. Они шифруют данные между клиентом и резольвером

Anycast

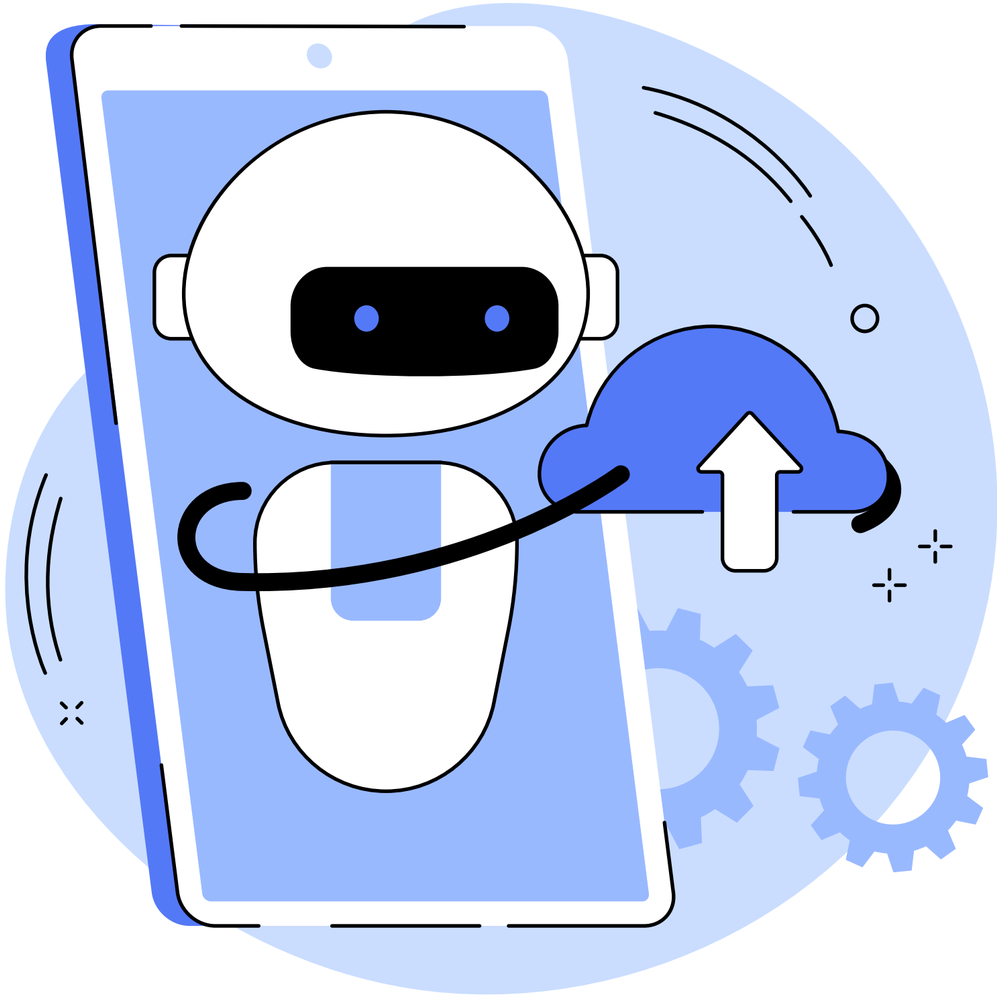
Техника Anycast позволяет размещать несколько экземпляров DNS-серверов на различных местоположениях по всему миру

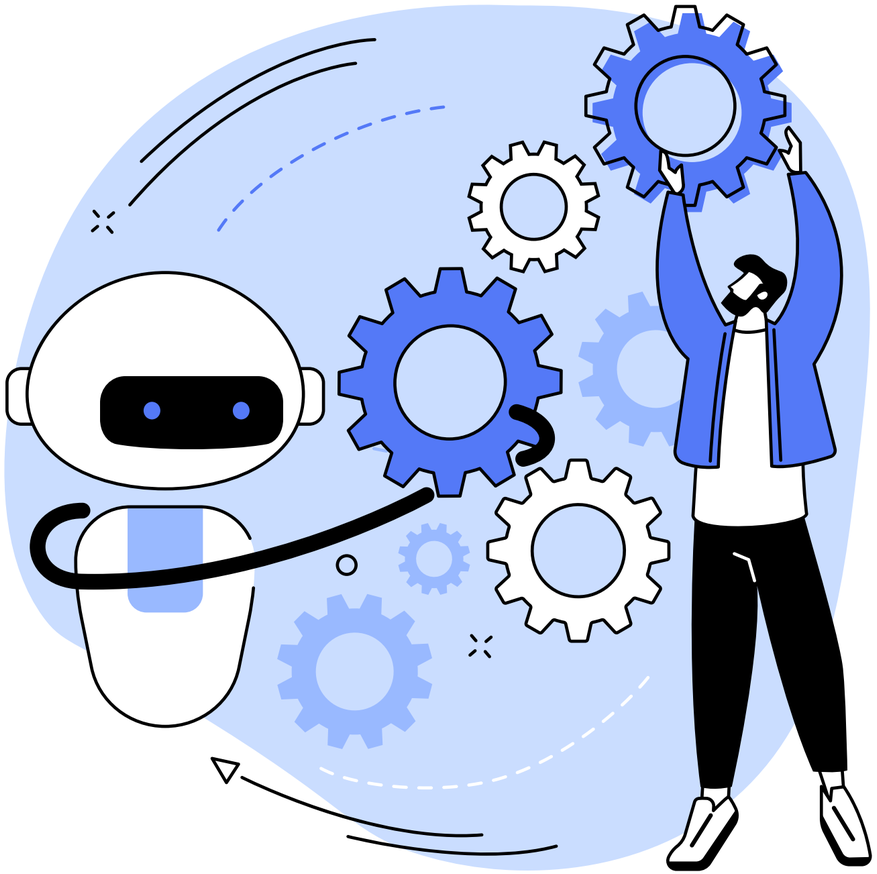
Rate Limiting и Filtering

DNS-серверы могут использовать ограничения скорости и фильтрацию запросов, чтобы защитить себя от злоумышленных атак и ненормального трафика

БУДУЩЕЕ DNS

- Улучшение безопасности;
- Повышение производительности;
- Интеграция с новыми технологиями;
- Сокращение задержек;
- Эффективное управление большим объемом данных.





ЗАКЛЮЧЕНИЕ

Рассмотрение архитектуры и функционирования **DNS (Domain Name System)** позволяет нам понять важную роль, которую эта система играет в современном интернете. **DNS** служит виртуальной адресной книгой, переводя человеко-читаемые доменные имена в **IP**-адреса, обеспечивая тем самым удобство и доступность сетевых ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. Mockapetris, P. (1987). RFC 1035 - Domain names - implementation and specification. Internet Engineering Task Force.
2. Pappas, C., Zervas, E., & Georgiadis, L. (2018). DNS Security: A Survey. IEEE Communications Surveys & Tutorials, 18(3), 2037-2061.
3. Kato, A. S., & Yoshida, S. (2018). DNS Traffic Analysis for Abnormal Domain Name Detection. IEEE/ACM Transactions on Networking, 24(5), 2947-2960.
4. Farah, M. M., & Zhang, X. (2019). DNS-over-HTTPS: Benefits and Challenges. IEEE Internet Computing, 21(6), 66-71.

THANK YOU FOR LISTENING!