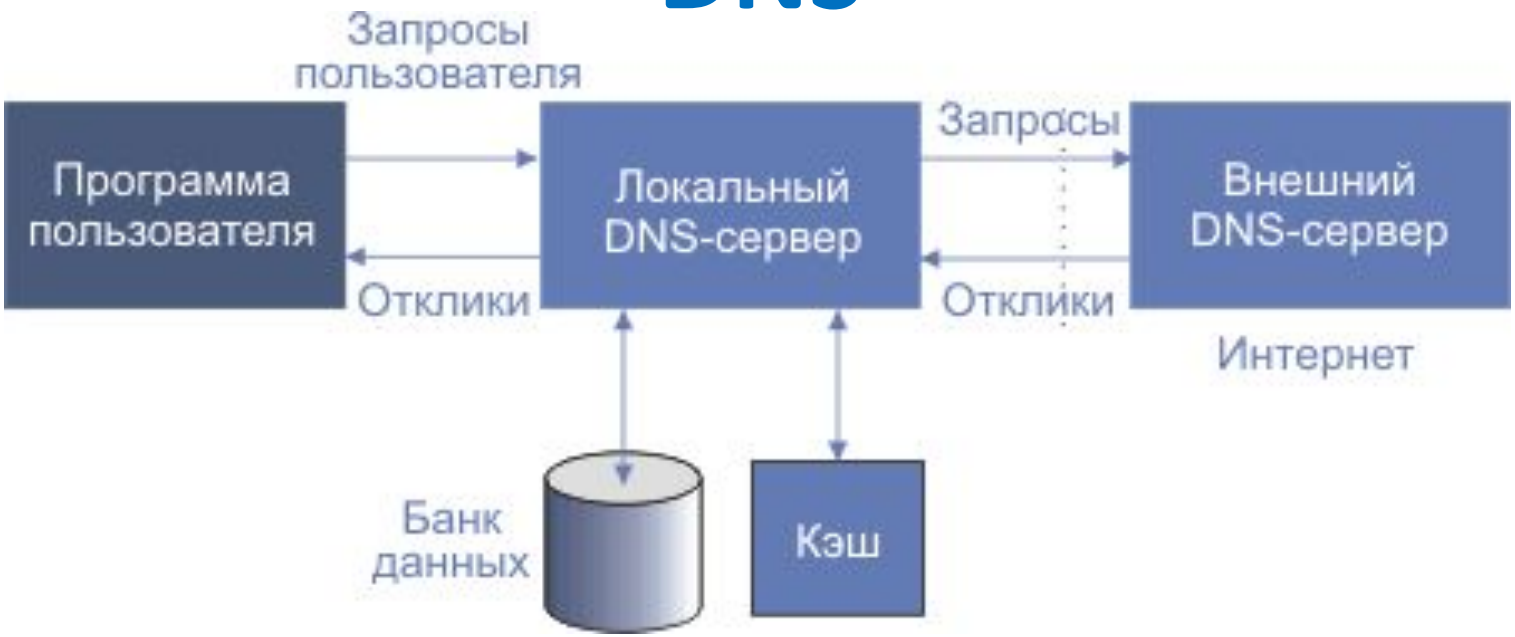
DNS



(RFC-4033(RFC-4033, -4034(RFC-4033, -4034, -4035(RFC-4033, -4034, -4035, -5155) RFC2536, RFC2671, RFC2672, RFC2929, RFC2931, RFC3110, RFC3225, RFC3226 и RFC3597.

Сервер имен это программа управления распределенной базой данных, в которой хранятся символьные имена сетей и ЭВМ вместе с их IP-адресами.

BIND (Berkrley Internet Name Domain)

В качестве транспорта используется UDP или TCP, порт 53

Дерево имен

I - домен первого уровня; II - второго уровня

В 2010 году появился русскоязычный домен **.рф**

Каждому узлу (прямоугольнику на рисунке) соответствует имя, которое может содержать до 63 символов. Только самый верхний, корневой узел не имеет имени.

Стандартизованные суффиксы имен

- **.aero** Фирма или организация, относящаяся к сфере авиации
- **.arts** Культура и досуг
- **.biz** Организация, относящаяся к сфере бизнеса
- **.com** Коммерческая организация
- **.coop** Кооперативная организация
- **.firm** Коммерческое предприятие
- **.gov** Государственное учреждение (США)
- **.info** Открытая TLD-структура (регистрация имен доменов)
- **.org** Бесприбыльная организация
- **.edu** Учебное заведение
- **.jobs** Работодатели
- **.mil** Военное предприятие или организация
- **.mobi** Сайты и сервисы, для мобильных и беспроводных устройств
- **.museum** Имя домена музея
- **.name** Имя домена частного лица
- **.net** Большая сеть
- **.pro** Профессионал, достойный доверия. Управляется RegistryPro

DNS-суффиксы (продолжение)

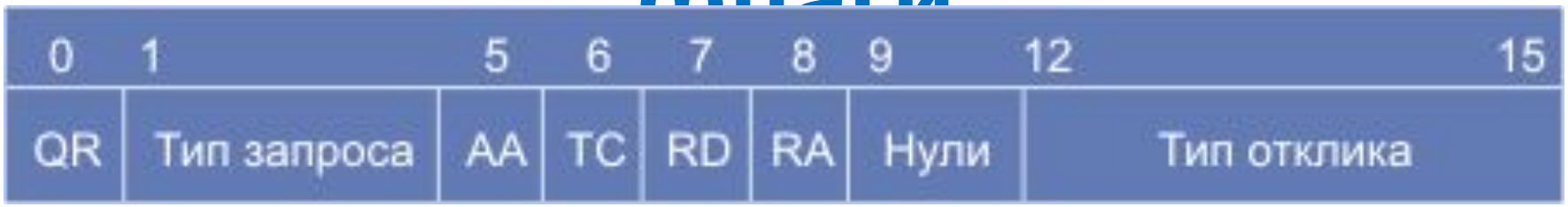
- **.int** Международная организация
- **.rec** Развлечения
- **.tel** Хранение и управление персонал. и корпоративн. данными
- **.travel** Турагенства
- **.tv** Телевидение. Хотя существует домен bbc.tv, а регистрация в этой зоне в РФ процветает (см. Ru center, официального статуса в качестве TLD этот домен не получил. В базе данных IANA (см. Национальные коды доменов в Интернет этот домен записан по-прежнему за TUVALU
- **.arpa** Специальный домен для преобразования IP в имя
- **.web** Организация, возвлеченная в WEB активность

Секции **.mil**и **.gov** принадлежат исключительно американским сетям (хотя и многие другие трехсимвольные секции адреса, например **.edu**, чаще, но не всегда, принадлежат американским университетам и другим учебным организациям

Заголовок DNS

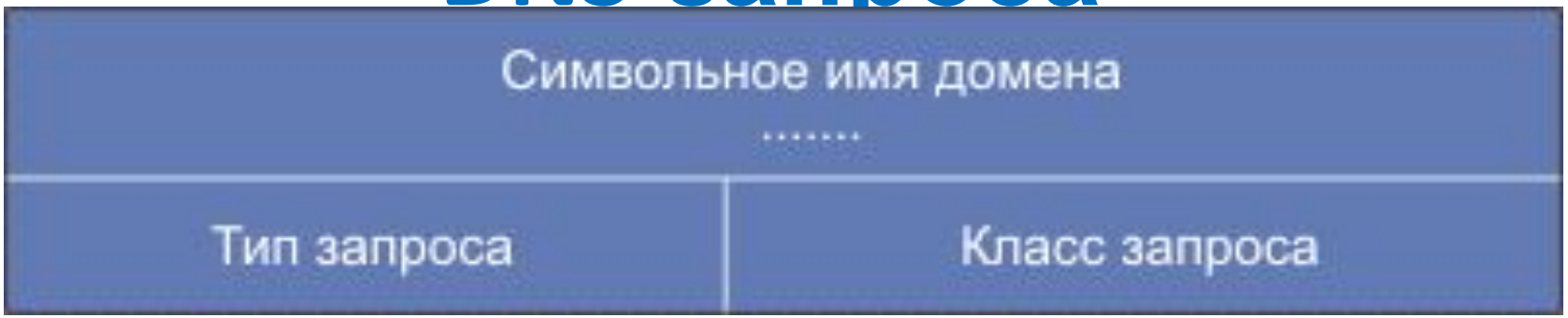
Поле ***идентификация***, позволяющее связать в пару запрос и отклик.
Поле ***флаги*** определяет характер запрашиваемой процедуры, а также кодировку отклика. Каждый вопрос состоит из символьного имени домена, за которым следует ***тип запроса*** и ***класс запроса***

Назначение битов поля флаги



Код поля *флаги*	Описание	
0 (QR)	Операция:	0 Запрос 1 Отклик
1…4	Тип запроса (opcode):	0 стандартный 1 инверсный 2 запрос состояния сервера
5 (AA)	Равен 1 при отклике от сервера (RR), в ведении которого находится домен, упомянутый в запросе.	
6 (TC)	Равен 1 при укорочении сообщения. Для UDP это означает, что ответ содержал более 512 октетов, но прислано только первые 512.	
7 (RD)	Равен 1, если для получения ответа желательна рекурсия.	
8 (RA)	Равен 1, если рекурсия для запрашиваемого сервера доступна.	
9…11	Зарезервировано на будущее. Должны равняться нулю.	
12…15	Тип отклика (rcode):	0 нет ошибки 1 ошибка в формате запроса 2 сбой в сервере 3 имени не существует

Формат секции вопросов DNS-запроса



2	n	s	4	i	t	e	p	2	r	u	0

Поле *символьное имя домена* имеет переменную длину, содержит одно или более субполей, начинающихся с байта длины (0-63). Поле завершается 0. В реальной нотации байты длины субполя могут иметь два старших бита равные 1, что преобразует интервал значений из 0-63 в 192-255.
Существует два вида запросов: *рекурсивные* и *итеративные*. Первый вид предполагает получение клиентом IP-адреса, а второй - адреса сервера, который может сообщить адрес.

DNS

- Если имя домена не завершено символом точки, DNS может попытаться его дополнить, например имя ns может быть преобразовано в ns.itep.ru.
- Каждый сервер содержит лишь часть дерева имен. Эта часть называется зоной ответственности сервера. *Зона* представляет собой часть субдерева имен
- Первичный и вторичный серверы должны быть независимыми и работать на разных ЭВМ, так чтобы отказ одного из серверов не выводил из строя систему в целом.
- Число вторичных серверов не лимитировано

Тип запроса

- Тип запроса Код запроса Описание

  A 1 IP-адрес

  NS 2 Сервер имен.

  CNAME 5 Каноническое имя

  SOA 6 Начало списка серверов. Большое число полей, определяющих часть иерархии имен

  MB 7 Имя домена почтового ящика.

  WKS 11 well-known service - стандартная услуга.

  PTR 12 Запись указателя.

  HINFO 13 Информация об ЭВМ.

  MINFO 14 Информация о почтовом ящике или списке почтовых адресов.

  MX 15 Запись о почтовом сервере

  TXT 16 Связывает имя ЭВМ с адресом ISDN.

  ISDN 16 Не интерпретируемая строка ASCII

  AXFR 252 Запрос зонного обмена

  * или ANY 255 Запрос всех записей

  Поле ***класс*** запроса позволяет использовать имена доменов для

Формат ресурсных записей в DNS (RR)

Всего существует **20** различных типов RR-записей.
Значение параметра **Type** (тип) для ресурсной записи DNSKEY равно 48.
CNAME - каноническое имя узла или ЭВМ, иногда называемое также псевдонимом (alias).
Поле ***время жизни*** (TTL) содержит время (в секундах), в течение которого запись о ресурсах может храниться в буферной памяти (в кэше). Обычно это время соответствует двум дням.
Ресурсная запись **SOA** говорит о том, что сервер имен является источником данных для данного домена. Записи SOA содержат электронный адрес администратора данной зоны.

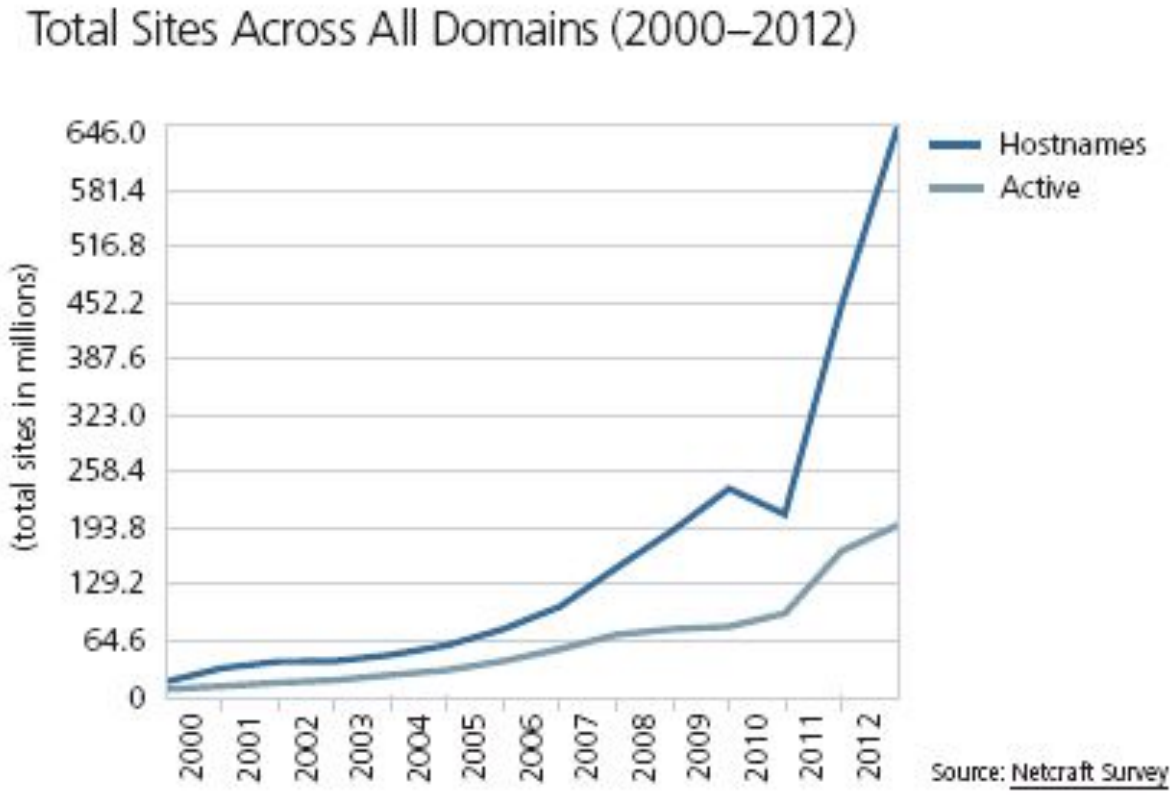
MX-записи

- Обмен MX-записями производится в следующих случаях:
- Локальная сеть или ЭВМ не имеет непосредственной связи с Интернет, но желает участвовать в почтовом обмене.
- Адресат не доступен и предпринимается попытка доставить почтовое сообщение альтернативной ЭВМ.
- Создание виртуальных ЭВМ, куда можно пересылать почту.
- Обычно реализация сервера имен предполагает наличие трех конфигурационных файлов:
- **named.boot** - файл начальной загрузки сервера имен;
  named.local - стартовый файл клиента DNS;
  named.ca - исходный буфер имен и адресов.
- В последнее время развивается технология DDNS динамического обновления ресурсных записей зоны DNS внешними ЭВМ или процессами (Dynamic DNS; RFC-2136).
- *host -t hinfo ns.itep.ru*

Зоны

- *Зоной* называется первичный домен универсальной совокупности имен, делегированный некоторому DNS-серверу с административной целью. Например, itep.ru - зона, а ns.itep.ru - конкретная машина в этой зоне. Зона может состоять из одного домена или нескольких субдоменов. В субдоменах могут быть свои серверы имен.
- **Базовая версия протокола DNS имеет ряд уязвимослей, которые позволяют хакерам предпринять атаки:**
- Осуществить разведку, просматривая DNS-отклики.
- В случае версии Man-in-the-middle перехватывать поток и фальсифицировать отклики с целью перенаправления запросов клиентов на вредоносные сайты.
- Перенаправлять запросы на фальшивые DNS-серверы.

Рост числа доменов за 2000-2012гг



DNSSEC (RFC-4033)

- ***Цепочка аутентификации***: Чередующаяся последовательность DNS общедоступных ключей (DNSKEY) RRsets и подписантов делегирования (DS) RRsets образуют цепочку подписанных данных, каждый узел цепочки подтверждает корректность предыдущего. Ресурсная запись DNSKEY используется для верификации подписи, покрывающей DS RR, и позволяет DS RR быть аутентифицированной.
- Расширения безопасности протокола DNS (DNSSEC) представляют собой коллекцию новых ресурсных записей (RR) и модификаций протокола, которые реализуют аутентификацию происхождения данных и целостность информации DNS.
- Безопасное расширение система доменных имен (DNS) предоставляет аутентификацию происхождения данных, а

DNSSEC

- DNSSEC обеспечивает аутентификацию путем ассоциирования с DNS RRsets криптографически формируемой подписи. Эти цифровые подписи записываются в новой ресурсной записи - RRSIG.
- Ресурсная запись подписанта делегирования (DS) упрощает некоторые административные задачи делегирования подписания данных при переходе через границы зон ответственности.
- DNSSEC вводит концепцию подписанных зон (signed zones). Подписанная зона имеет записи общедоступного ключа DNS (**DNSKEY**), сигнатуру ресурсной записи (**RRSIG**), Next Secure (**NSEC**), и (опционно) Delegation Signer (подписант делегирования) (**DS**). Зона, которая не имеет этих рекордов, считается неподписанной зоной. DNSSEC требует изменения определения ресурсной записи CNAME ([RFC1035]).

Формат RDATA ресурсной записи DNSKEY (RFC-4034) DNSSEC

Бит 7 поля флаги является флагом ключа зоны (Zone Key). Если бит 7 равен 1, тогда рекорд DNSKEY содержит ключ зоны DNS, а имя владельца ресурсной записи DNSKEY должно быть именем зоны.

DNSSEC обеспечивает аутентификацию путем ассоциирования с DNS **RRsets** криптографически формируемой подписи. Эти цифровые подписи записываются в новой ресурсной записи - **RRSIG**.

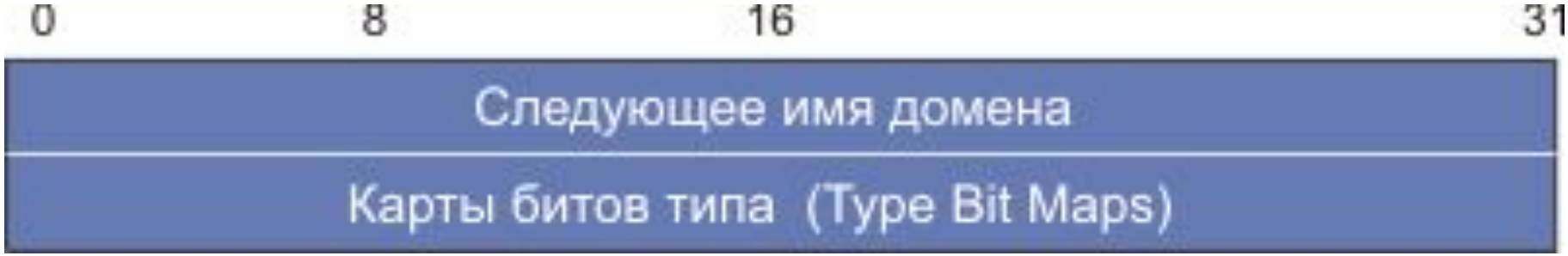
Ресурсные записи для расширений безопасности DNS (RFC-4034)

- DNSSEC вводит концепцию подписанных зон (signed zones). Подписанная зона имеет записи общедоступного ключа DNS (**DNSKEY**), сигнатуру ресурсной записи (**RRSIG**), Next Secure (**NSEC**), и (опционно) Delegation Signer (подписант делегирования) (**DS**).

Формат поля RDATA

Поле **Type Covered** указывает на тип набора RRset, который покрыт для этого рекорда RRSIG.
Поле кода **алгоритма** идентифицирует криптографический алгоритм, использованный при формировании подписи

Формат NSEC RDATA



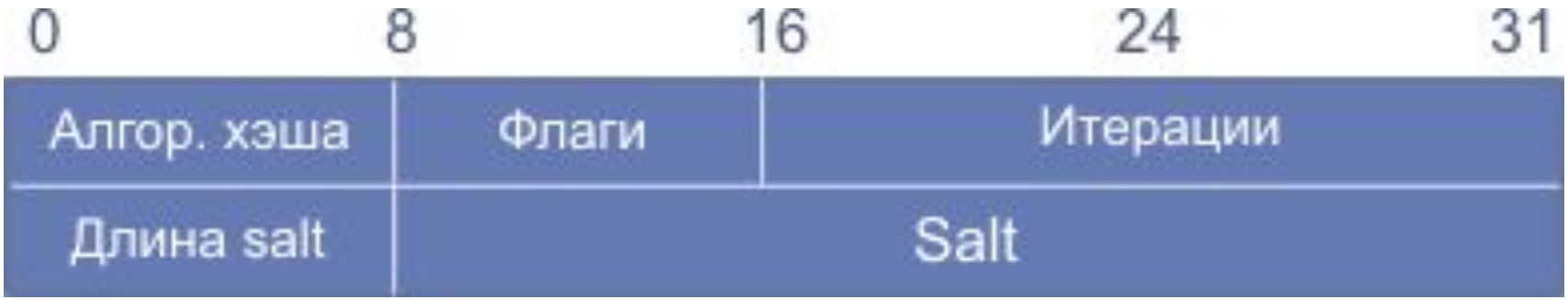
RDATA ресурсной записи NSEC RR

DS RDATA Wire Format

NSEC3 RDATA Wire Format

Значение поля *итерации* представляет собой 16-битовое целое число без знака, первым следует старший бит. Поле *длина Salt* представляет собой октет без знака, характеризующий длину поля *Salt* в октетах.

NSEC3PARAM RDATA Wire Format



Поля *хэш* ***алгоритма*** и ***флаги*** являются однооктетными. Поле ***итерации*** содержит 16-битовое целое число без знака, первым следует старший бит. Длина **Salt** характеризуется одним октетом без знака.\
Поле ***Salt*** добавляется к исходному имени владельца до хэширования и является псевдослучайным кодом.

DoS-атаки DNS

- Если в 2008 году мощность DDoS-атак достигала 40Гбит/с, то в 2014-ом превысила 400 Гбит/с
- Ущерб от этих атак в 2012 году составил 1 млн. долларов в день (США)