

Безопасность DNS

Филипп Кулин



Saint
HighLoad++



Откиньтесь на спинку кресла

Knot 3.0+

```
ppa:cz.nic-labs/knot-dns-latest  
knot-dnsutils
```

```
copr @cznic/knot-dns-latest  
knot-utils
```

```
docker cznic/knot:latest
```

ISC BIND 9.17.11+

```
ppa:isc/bind-dev  
bind9-dnsutils
```

```
copr isc/bind-dev  
isc-bind-bind-utils
```

- Эта презентация сделана с помощью L^AT_EX
- Я расскажу страшную сказку

DNS — всему голова

- Жизнь пользователей в сети
- Запросы к API, работа с CDN
- Облака, микросервисы, автообнаружение и конфигурация
- Невообразимое количество всего

Тайная жизнь привычных программ

- SSHD определяет домен для подключившегося IP
и этот факт является одним из источников седых волос у админов

Тайная жизнь привычных программ

- SSHD определяет домен для подключившегося IP
и этот факт является одним из источников седых волос у админов
- MySQL определяет домен для подключившегося IP

Тайная жизнь привычных программ

- SSHD определяет домен для подключившегося IP
и этот факт является одним из источников седых волос у админов
- MySQL определяет домен для подключившегося IP
- Apache определяет домен для подключившегося IP
даже если `HostnameLookups Off`, но есть `Require`

Тайная жизнь привычных программ

- SSHD определяет домен для подключившегося IP
и этот факт является одним из источников седых волос у админов
- MySQL определяет домен для подключившегося IP
- Apache определяет домен для подключившегося IP
даже если `HostnameLookups Off`, но есть `Require`
- Microsoft Windows постоянно шлет DNS Update в сеть

Тайная жизнь привычных программ

- SSHD определяет домен для подключившегося IP
и этот факт является одним из источников седых волос у админов
- MySQL определяет домен для подключившегося IP
- Apache определяет домен для подключившегося IP
даже если `HostnameLookups Off`, но есть `Require`
- Microsoft Windows постоянно шлет DNS Update в сеть
- Docker, Kubernetes, etc

Тайная жизнь привычных программ

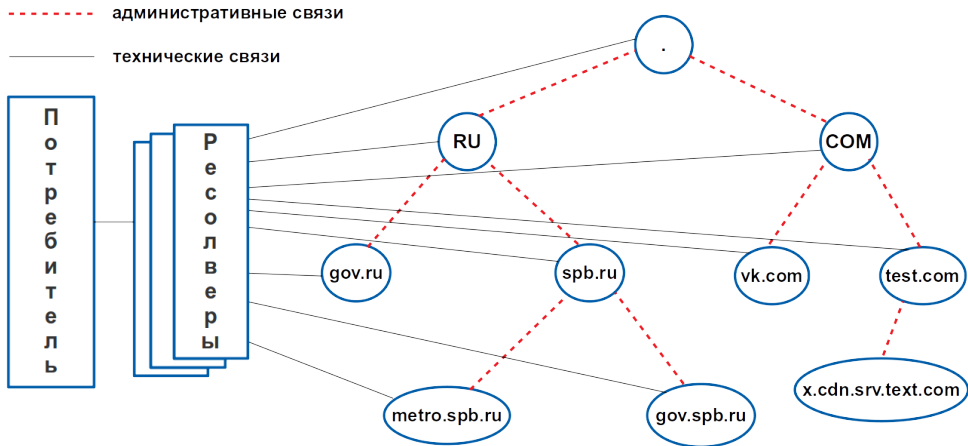
- SSHD определяет домен для подключившегося IP
и этот факт является одним из источников седых волос у админов
- MySQL определяет домен для подключившегося IP
- Apache определяет домен для подключившегося IP
даже если `HostnameLookups Off`, но есть `Require`
- Microsoft Windows постоянно шлет DNS Update в сеть
- Docker, Kubernetes, etc
- **Запустите tcpdump/WireShark**

DNS — это просто?

Три каверзных вопроса:

- Каков максимальный размер доменного имени?
- Точку на конце надо ставить?
- Что именно спрашивает ресолвер и что отвечают DNS-сервера при рекурсивном обходе?

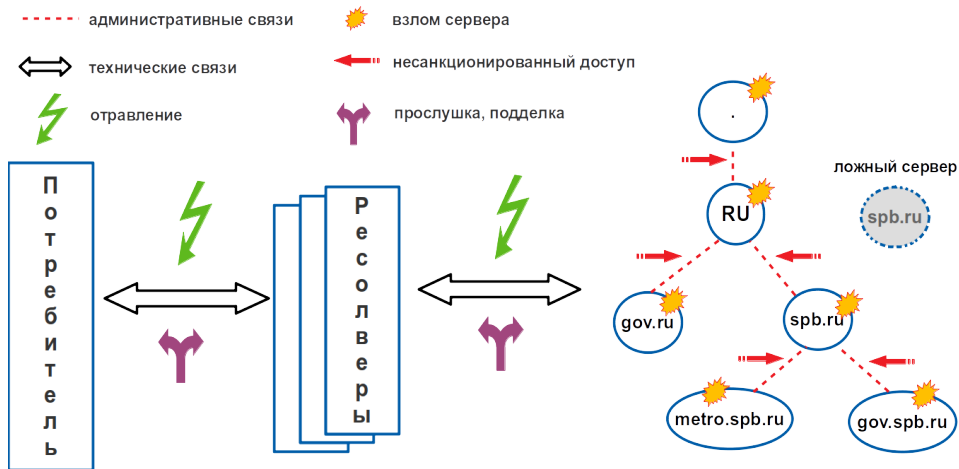
Как устроен DNS



Особенности классического DNS

- UDP транспорт. Нет соединения
- Нет идентификации серверов DNS
- Нет контроля данных
- Нет шифрования

Угрозы в системе DNS



Заложенная в DNS безопасность

Заложенная в DNS безопасность

“... действия, которые с современной точки зрения могут показаться неправильными или ошибочными, часто оказывались естественным следствием господствовавшего в те времена понимания тех или иных вещей, а также ограниченности доступных ресурсов.”

Заложенная в DNS безопасность

“... действия, которые с современной точки зрения могут показаться неправильными или ошибочными, часто оказывались естественным следствием господствовавшего в те времена понимания тех или иных вещей, а также ограниченности доступных ресурсов.”

— Брайан Керниган¹⁵

Основные проблемы

- Подделка
- Прослушка

Основные проблемы. Подделка

- Отравление
- Подмена
- Взлом серверов и замена записей
- Поддельные серверы, BGP-injection

Основные проблемы. Подделка

- Отравление
- Подмена
- Взлом серверов и замена записей
- Поддельные серверы, BGP-injection
 - Атака на Route53 в апреле 2018 года

Основные проблемы. Подделка

- Отравление
- Подмена
- Взлом серверов и замена записей
- Поддельные серверы, BGP-injection
 - Атака на Route53 в апреле 2018 года
- Госрегулирование
 - Блокировка сайтов в Европе и России

Основные проблемы. Прослушка

- Маркетинговые исследования
- Шпионаж и промышленный шпионаж
- RFC7626 — 73.1% могут быть узнаны по слепку DNS

Основные проблемы. Прослушка

- Маркетинговые исследования
- Шпионаж и промышленный шпионаж
 - ... с использованием госрегулирования
- RFC7626 — 73.1% могут быть узнаны по слепку DNS
- Госрегулирование
 - Использование DoH/DoT Telegram

А так ли страшен чёрт?



А так ли страшен чёрт?

- Вы знаете кто, когда и как использует какой DNS?

А так ли страшен чёрт?

- Вы знаете кто, когда и как использует какой DNS?

А так ли страшен чёрт?

- Вы знаете кто, когда и как использует какой DNS?
- Ваш сетевой периметр защищен? Точно?

А так ли страшен чёрт?

- Вы знаете кто, когда и как использует какой DNS?
- Ваш сетевой периметр защищен? Точно?
- Ваша сеть получает подписанные маршруты?

А так ли страшен чёрт?

- Вы знаете кто, когда и как использует какой DNS?
- Ваш сетевой периметр защищен? Точно?
- Ваша сеть получает подписанные маршруты?
 - Вы ведете журнал странных анонсов?

А так ли страшен чёрт?

- Вы знаете кто, когда и как использует какой DNS?
- Ваш сетевой периметр защищен? Точно?
- Ваша сеть получает подписанные маршруты?
 - Вы ведете журнал странных анонсов?
- Ваши сервисы проверяют сертификат соединения?

А так ли страшен чёрт?

- Вы знаете кто, когда и как использует какой DNS?
- Ваш сетевой периметр защищен? Точно?
- Ваша сеть получает подписанные маршруты?
 - Вы ведете журнал странных анонсов?
- Ваши сервисы проверяют сертификат соединения?
- **Однако, современные взломы чаще основаны на бардаке**

Защита от подделки

- Не «взлетевший» DNSCurve
- Расширение DNSSEC

DNSCurve

Концепция

- Аутентификация авторитативного DNS-сервера
- Защита обмена между ресолвером и авторитативным сервером

Принцип действия

- Публичный ключ DNS-сервера с магическим префиксом "uz5" в NS-записи домена:

uz5qry75vfy162c239jgx7v2knkwb01g3d04qd4379s6mtcx2f0828.dnscurve.io

- Обмен с DNS-сервером шифруется

DNSCurve. Особенности

- Не меняет саму спецификацию DNS
- Основан на вере в целостность системы
- Зависит от источника ответа
- Внедрение практически отсутствует
- Шифрование на основе ED25519

DNSSEC

- Концепция
 - Источник записи не важен. Используя доверенный корневой ключ, возможно проверить любую подписанную запись
- Принцип действия
 - Записи зоны подписаны ключом зоны
 - Подтверждения подписи выстраиваются в цепочку доверия

DNSSEC. Принцип действия

Подпись зоны

Key-signing key (KSK)

DNSKEY

Zone-signing key (ZSK)

DNSKEY

SOA

NS

AAAA



DNSSEC. Принцип действия

Подпись зоны

Key-signing key (KSK)

DNSKEY

Zone-signing key (ZSK)

DNSKEY

SOA

NS

AAAA

Цепочка доверия

.tld

DNSKEY (KSK)

example DS

example.tld

DNSKEY (KSK)

sub.example DS

sub.example.tld

DNSKEY (KSK)

DNSSEC. Особенности

- **Источник ответа не важен**
- Требуется аккуратности и непрерывного обслуживания даже в статическом состоянии
- Сложные реализации «отрицательного ответа»
- Большой размер ответа
- Возможность использования «устаревших» ответов
- Крайне слабая глубина внедрения

DNSSEC. Варианты использования

- Прозрачная проверка

Потребитель получает фильтрованные ответы

- Явная проверка

Потребитель явно указывает ресолверу, что хочет получить проверенный результат. Проверяет флаги ответа

- Усиленная проверка

Потребитель проверяет подписи сам

DNSSEC. Тренды

- Алгоритм ECDSA
 - скорость
 - небольшой размер ответов по сравнению с RSA
- Подпись «на лету»
 - использование «белой лжи»⁵
 - использование «чёрной лжи»⁶

DNSSEC. Поддержка

СКОРЕЕ ВСЕГО ЗАМЕНЮ ОБЗОРОМ "КАК ПОСМОТРЕТЬ"

- **Клиенты**

`dig/delv, drill, kdig`

- **Ресолверы**

`systemd-resolved, dnsmask, unbound, KNOT Resolver, CoreDNS, PowerDNS recursor, BIND`

- **Авторитативные сервера DNS**

`KNOT, CoreDNS, PowerDNS, NSD, YADIFA, BIND`

- **Сервера DNS с подписью «на лету»**

`KNOT, CoreDNS, PowerDNS (частично)`

DNSSEC. Пример использования

SSH Fingerprint

- Запись SSHFP содержит хэш публичного ключа хоста
- На клиенте `/.ssh/config:VerifyHostKeyDNS yes`
- На сервере `ssh-keygen -R 'hostname'`
 - Не надо все алгоритмы, не тяните за собой легаси
- Работает только с DNSSEC
- [RFC 4255](#)¹⁶

Защита от прослушки DNS

Шифрование сообщений

- DNSCrypt

Защита от прослушки DNS

Шифрование сообщений

- DNSCrypt

Защищенный транспорт

- DNS-over-HTTPS Google API
- DNS-over-TLS
- DNS-over-HTTP/2
- DNS-over-QUIC

Защита от прослушки DNS

Шифрование сообщений

- DNSCrypt

Защищенный транспорт

- DNS-over-HTTPS Google API
- DNS-over-TLS
- DNS-over-HTTP/2
- DNS-over-QUIC

Прочее

- Минимизация QNAME при запросах
- EDNS0 Client subnets

Шифрование канала

Защита канала сводится к двум задачам:

- Аутентификация ресолвера
- Защита обмена между потребителем и ресолвером

DNSEncrypt

Принцип действия

- Настройка мастер-ключа и имени сервера
- Получение «короткого» ключа и сертификата
- Запросы к серверу, идентичные DNSCurve

DNSCrypt. Особенности

- Не меняет спецификацию DNS
- Нет ни RFC, ни Draft. Только спецификация на сайте
- Имеет заметную программную поддержку
- Не предусмотрена замена мастер-ключа
- Две фазы
- Не «взлетел»

DNSCrypt. Поддержка

СКОРЕЕ ВСЕГО ЗАМЕНЮ ОБЗОРОМ "КАК
ПОСМОТРЕТЬ"

DNS-over-HTTPS (Google API)

Google предоставляет JSON-API к DNS

Страница с описанием:

<https://developers.google.com/speed/public-dns/docs/dns-over-https>

Массово используется для веб-приложений

DNS-over-TLS (DoT)

- Устанавливается защищенное TLS-соединение (порт 853)
- Внутри соединения – стандартный DNS протокол
- Самая простая инсталяция – проксирование `nginx` через `ngx_stream_ssl_module` на обычный DNS

DNS-over-TLS (DoT)

- Устанавливается защищенное TLS-соединение (порт 853)
- Внутри соединения – стандартный DNS протокол
- Самая простая инсталляция – проксирование `nginx` через `ngx_stream_ssl_module` на обычный DNS
- А есть ещё DNS-over-DTLS...

DNS-over-TLS (DoT)

- Устанавливается защищенное TLS-соединение (порт 853)
- Внутри соединения – стандартный DNS протокол
- Самая простая инсталляция – проксирование `nginx` через `ngx_stream_ssl_module` на обычный DNS
- А есть ещё DNS-over-DTLS...
- ... и DNS-over-QUIC...

DNS-over-TLS (DoT). Особенности

- Не меняет спецификацию DNS
- Требуется установка TLS-соединения (дорого)
- Требуется стартовых настроек клиента
 - Нет автоопределения
 - Требуется «бутстрапа» имени сервера
- Специальный 853 порт

DNS-over-TLS (DoT). Поддержка

СКОРЕЕ ВСЕГО ЗАМЕНЮ ОБЗОРОМ "КАК ПОСМОТРЕТЬ"

- **Клиенты**

`kdig, dig 9.17.7+`

- **Ресолверы** (могут принять)

`unbound, CoreDNS, dnsmdist, KNOT Resolver`

- **Ресолверы** (могут спросить)

`unbound, CoreDNS, KNOT Resolver, systemd.resolved, Android 9 Pie`

- **Сервисы**

`Google DNS, Cloudflare DNS, Quad9`

DNS-over-HTTPS (DoH)

- Защищенным транспортом является обычный HTTP/2
- Запросы/ответы — стандартные DNS-пакеты
- Формируется специальный HTTP-запрос
 - GET — DNS-пакет кодируется в параметр
 - POST — DNS-пакет в `application/dns-message`

DNS-over-HTTPS (DoH). Особенности

- Не меняет спецификацию DNS
- Требуется установка HTTP/2-соединения (дорого)
- Требуется стартовых настроек клиента
 - Нет автоопределения
 - Требуется «бутстрапа» имени сервера
- **Не сильно выделяется в HTTP-трафике**

DNS-over-HTTPS (DoH). Поддержка

СКОРЕЕ ВСЕГО ЗАМЕНЮ ОБЗОРОМ "КАК ПОСМОТРЕТЬ"

- **Клиенты**

`kdig 3.0+, dig 9.17.11+`

- **Ресолверы** (могут принять)

`unbound, CoreDNS, dnsmdist, KNOT Resolver`

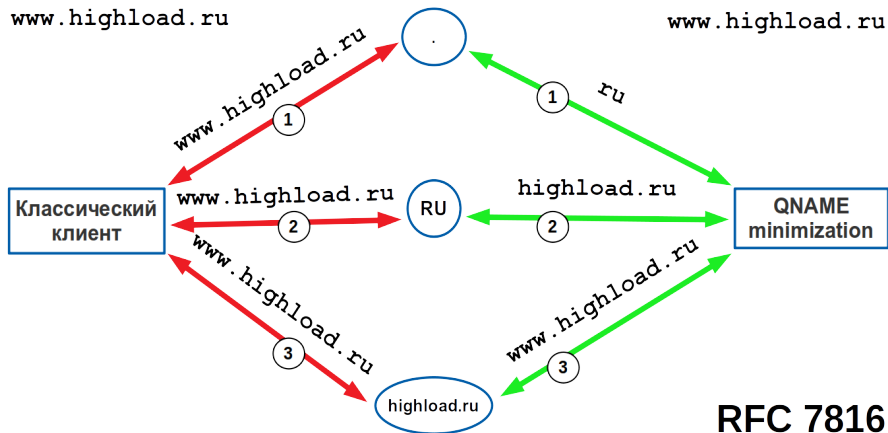
- **Ресолверы** (могут спросить)

`unbound, CoreDNS, KNOT Resolver`

- **Сервисы**

`Google DNS, Cloudflare DNS, Quad9`

Минимизация QNAME



EDNS Client subnet

Это расширение DNS

- Добавляет в запрос подсеть клиента
- Например, для геобалансига

Поддержка

- Google DNS принципиально **да**
- Cloudflare DNS принципиально **нет**

EDNS Client subnet

Это расширение DNS

- Добавляет в запрос подсеть клиента
- Например, для геобалансига

Поддержка

- Google DNS принципиально **да**

```
dig +short @8.8.8.8 -t TXT o-o.myaddr.1.google.com
```

- Cloudflare DNS принципиально **нет**

```
dig +short @1.1.1.1 -t TXT o-o.myaddr.1.google.com
```

Защита DNS и ваш сервер

- systemd-resolved
- unbound или knot-resolver

Защита DNS и docker

- Никакой защиты

Защита DNS и docker

- Никакой защиты
- Docker понимает и `systemd-resolved`, и `resolve.conf`

Защита DNS и docker

- Никакой защиты
- Docker понимает и `systemd-resolved`, и `resolve.conf`
- Каждому контейнеру можно указать свои DNS

Защита DNS и docker

- Никакой защиты
- Docker понимает и `systemd-resolved`, и `resolve.conf`
- Каждому контейнеру можно указать свои DNS
- При неудаче умолчание: **8.8.8.8**

Защита DNS и kubernetes

- CoreDNS — с ним всё хорошо

Защита DNS и kubernetes

- CoreDNS — с ним всё хорошо
- NodeLocal DNSCache настраиваем как хотим

Защита DNS и kubernetes

- CoreDNS — с ним всё хорошо
- NodeLocal DNSCache настраиваем как хотим
- CoreDNS не умеет проверять DNSSEC

Защита DNS и kubernetes

- CoreDNS — с ним всё хорошо
- NodeLocal DNSCache настраиваем как хотим
- CoreDNS не умеет проверять DNSSEC
- Knot Resolver умеет

Как проверить ресолвер

Реакционизм. Подделка

Картинка

Реакционизм. Подделка

- Не позволяет подставлять «свой» ответ

Реакционизм. Подделка

- Не позволяет подставлять «свой» ответ
 - Противоречит копоративным политикам

Реакционизм. Подделка

- Не позволяет подставлять «свой» ответ
 - Противоречит копоративным политикам
 - Мешает спецслужбам проводить спецоперации

Реакционизм. Подделка

- Не позволяет подставлять «свой» ответ
 - Противоречит корпоративным политикам
 - Мешает спецслужбам проводить спецоперации
- Переусложненное обслуживание приводит к ошибкам

Реакционизм. Прослушка



Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы

Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы
 - Нарушает корпоративные стандарты безопасности

Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы
 - Нарушает корпоративные стандарты безопасности
 - Мешает приложениям защиты отслеживать действия браузера

Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы
 - Нарушает корпоративные стандарты безопасности
 - Мешает приложениям защиты отслеживать действия браузера
 - Создаёт видимость безопасности

Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы
 - Нарушает корпоративные стандарты безопасности
 - Мешает приложениям защиты отслеживать действия браузера
 - Создаёт видимость безопасности
- Дополнительная нагрузка

Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы
 - Нарушает корпоративные стандарты безопасности
 - Мешает приложениям защиты отслеживать действия браузера
 - Создаёт видимость безопасности
- Дополнительная нагрузка
- Цикл получения ответа неприемлемо долгий

Реакционизм. Госрегулирование

Картинка с самураем и флажками/нашивками
РКН/FCC/etc

Реакционизм. Госрегулирование

- Давление UK ISPA

Реакционизм. Госрегулирование

- Давление UK ISPA
- Большинство «госблокировок» в мире основано на манипуляциях с DNS

Реакционизм. Госрегулирование

- Давление UK ISPA
- Большинство «госблокировок» в мире основано на манипуляциях с DNS
- НСДИ РФ не совместима с DNSSEC
- НСДИ РФ не поддерживает защиту

Госрегулирование. НСДИ

- Определена в законе 90-ФЗ от 01.05.2019
- Государственный публичный DNS
- Дублирует . (корень)
- Уменьшает ущерб от манипуляций с **.RU**
гипотетических, со стороны США в лице ICANN
- НСДИ обслуживается ЦМУ ССОП
- Предоставляется в том числе AXFR

Безопасность заложенная в НСДИ

Безопасность заложенная в НСДИ



Многое осталось за кадром

- EDNS(0) Padding, Cookies, etc
- Обслуживание DNS, DNSSEC, DoT/DoH
- Применение DNSSEC: DANE, etc
- Обзор серверов, включая stub-решолверы
- Обзор клиентов и инструментов
- DNS Stamps (ссылки `sdna://`)
- `glibc` и `resolv.conf`
- Amplification attack, etc
- ...

Вопросы

Перед докладом я многое освежил в памяти, многое
не вошло в доклад

В любом случае пишите мне

schors@gmail.com

Ссылки. DNSCurve

- [1] *DNSCurve.io - A Community for DNSCurve.* Основной сайт DNSCurve. <https://dnscurve.io/>.
- [2] *M. Dempsy. Link-Level Security for the Domain Name System.* 26 февр. 2010.
<https://datatracker.ietf.org/doc/html/draft-dempsy-dnscurve-01>.
- [3] *Dq is a package with DNS/DNSCurve related software.* <https://mojzis.com/software/dq/>.
- [4] *World's fastest-to-synchronize Secondary DNS service.* Единственный известный DNS-сервис с поддержкой DNSCurve. <https://www.buddyns.com/>.

Ссылки. DNSSEC

- [5] RFC 7129. *Authenticated Denial of Existence in the DNS*. Определение белой лжи. Февр. 2014.
<https://datatracker.ietf.org/doc/html/rfc7129>.
- [6] Dani Grant (Cloudflare). *Economical With The Truth: Making DNSSEC Answers Cheap*. Определение черной лжи. 24 июня 2016. <https://blog.cloudflare.com/black-lies/>.
- [7] *Визуализация DNSSEC*. <http://dnsviz.net/>.
- [8] Филипп Кулин. *DNSSEC. Руководство регистратора доменов*. Дек. 2016.
<https://www.slideshare.net/schors/dnssec-71055077>.
- [9] Филипп Кулин. *DNSSEC. Руководство оператора доменов*. Окт. 2017.
<https://www.slideshare.net/schors/enog14-dnssec>.
- [10] RFC 4033. *Введение в DNSSEC*. Март 2005. <https://tools.ietf.org/html/rfc4033>.
- [11] RFC 4034. *Ресурсные записи для DNSSEC*. Март 2005. <https://tools.ietf.org/html/rfc4034>.
- [12] RFC 4035. *Модификации протокола DNS для DNSSEC*. Март 2005.
<https://tools.ietf.org/html/rfc4035>.
- [13] RFC 6781. *Эксплуатация DNSSEC*. Дек. 2012. <https://tools.ietf.org/html/rfc6781>.
- [14] RFC 7583. *Соображения по ротации ключей DNSSEC*. Окт. 2015.
<https://tools.ietf.org/html/rfc7583>.

Ссылки. DNSCrypt

Ссылки. DoH/Dot

Ссылки. Разное

- [15] Brian Kernighan. *UNIX: A History and a Memoir*. 18 окт. 2019.
- [16] RFC 4255. *Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints*. Янв. 2006.
<https://datatracker.ietf.org/doc/html/rfc4255>.
- [17] RFC 7871. *EDNS(0) Client Subnet*. Май 2016. <https://datatracker.ietf.org/doc/html/rfc7871>.
- [18] RFC 7816. *DNS Query Name Minimisation to Improve Privacy*. Март 2016.
<https://datatracker.ietf.org/doc/html/rfc7816>.

Ссылки. L^AT_EX

- [19] *Beamer - Overleaf, Online LaTeX Editor.* <https://www.overleaf.com/learn/latex/Beamer>.
- [20] *Uri Nativ. How to present code.* 2016. <https://www.slideshare.net/LookAtMySlides/codeware>.
- [21] *Филипп Кулин. Пишем презентации в LaTeX.* 14 окт. 2019. <https://habr.com/ru/post/471352/>.