

# 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  $\text{\LaTeX}$
- Я расскажу страшную сказку про DNS

# 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 шлёт 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 шлёт DNS Update в сеть
- Docker, Kubernetes, etc



# Тайная жизнь привычных программ

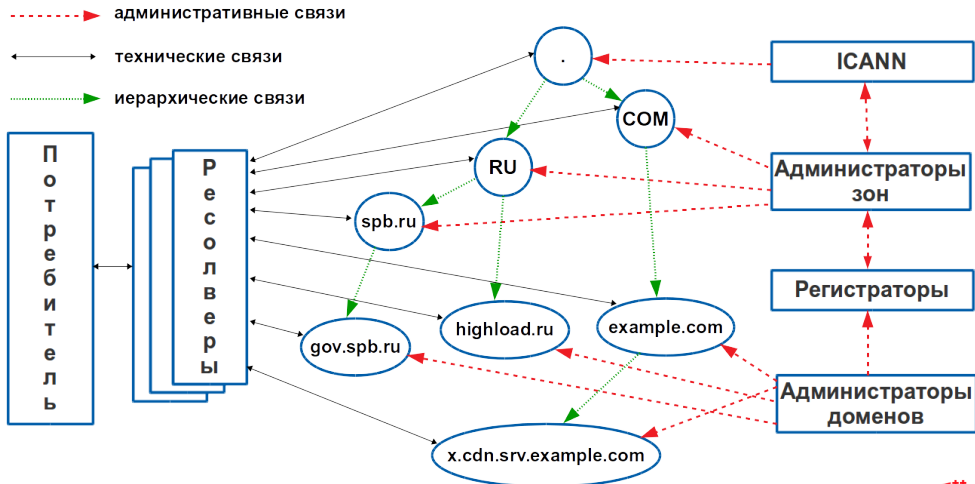
- SSHD определяет домен для подключившегося IP  
и этот факт является одним из источников седых волос у админов
- MySQL определяет домен для подключившегося IP
- Apache определяет домен для подключившегося IP  
даже если `HostnameLookups Off`, но есть `Require`
- Microsoft Windows постоянно шлёт DNS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

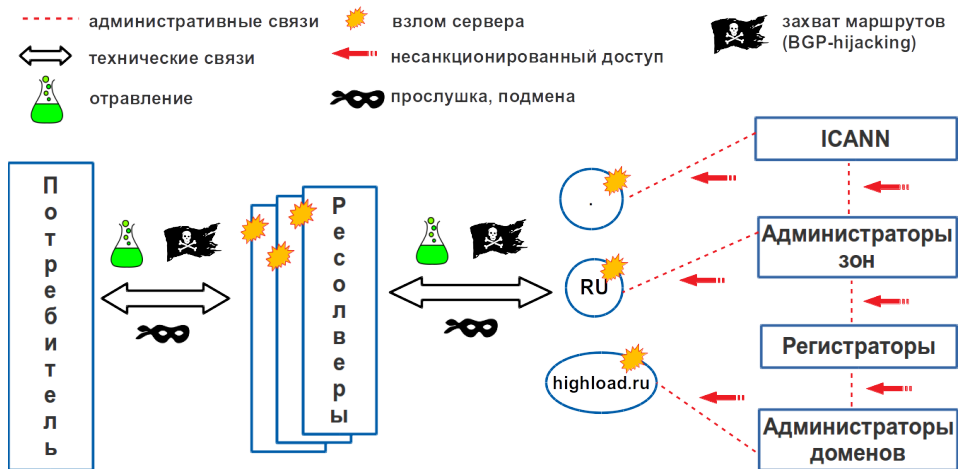
# Как устроен DNS



# 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.”

— Брайан Керниган<sup>26</sup>

# Основные проблемы

- Подделка
- Прослушка



# Основные проблемы. Подделка

- Отравление, подмена
- Взлом серверов и замена записей
- Поддельные серверы, BGP-injection
  - Атака на Route53 в апреле 2018 года<sup>23</sup>  
[www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/](http://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/)
- Госрегулирование
  - Блокировка сайтов в Европе и России

```
dig +short @a.res-nsdi.ru. rutracker.org A
```

# Основные проблемы. Прослушка

- Реклама, сбор статистики, что-то ещё<sup>24</sup>  
[en.wikipedia.org/wiki/DNS\\_hijacking#Manipulation\\_by\\_ISPs](https://en.wikipedia.org/wiki/DNS_hijacking#Manipulation_by_ISPs)
- Шпионаж и промышленный шпионаж
- RFC7626: 73.1% могут быть узнаны по слепку DNS<sup>27</sup>

# Основные проблемы. Прослушка

- Реклама, сбор статистики, что-то ещё<sup>24</sup>  
[en.wikipedia.org/wiki/DNS\\_hijacking#Manipulation\\_by\\_ISPs](https://en.wikipedia.org/wiki/DNS_hijacking#Manipulation_by_ISPs)
- Шпионаж и промышленный шпионаж
  - ... с использованием госрегулирования
- RFC7626: 73.1% могут быть узнаны по слепку DNS<sup>27</sup>
- Госрегулирование
  - Помощь в оперативной блокировке<sup>25</sup>  
[usher2.club/articles/mt-free-pre-block/](https://usher2.club/articles/mt-free-pre-block/)

# 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?
- 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
- Не предусмотрена замена ключа
- **Зависит от источника ответа**
- Внедрение практически отсутствует

# 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

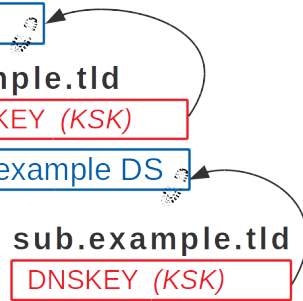
example.tld

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
- Требуется стартовых настроек клиента  
требуется актуальные корневые ключи
- Сложные реализации «отрицательного ответа»
- Большой размер ответа
- Крайне слабая глубина внедрения
- **Это единственный вариант в этой категории**

# DNSSEC. Настройка клиентов

- Прозрачная проверка

Потребитель получает фильтрованные ответы

- Явная проверка

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

- Усиленная проверка

Потребитель проверяет подписи сам

```
delv @8.8.8.8 dxdt.ru A
```

# DNSSEC. Must have

- Подпишите свои домены
  - CoreDNS и Knot DNS - отличные реализации

# DNSSEC. Must have

- Подпишите свои домены
  - CoreDNS и Knot DNS - отличные реализации
- Настройте ваши ресолверы на проверку DNSSEC
  - CoreDNS не умеет проверять DNSSEC
  - ~~systemd-resolved~~, unbound, Knot Resolver — умеют

# DNSSEC. Вкусняшка SSHFP

## 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 — SSH Fingerprint<sup>7</sup>

# Защита от прослушки DNS

Шифрование сообщений

- DNSCrypt

# Защита от прослушки DNS

Шифрование сообщений

- DNSCrypt

Защищенный канал

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

# Защита от прослушки DNS

Шифрование сообщений

- DNSCrypt

Защищенный канал

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

Прочее

- Минимизация QNAME при запросах
- EDNS0 Client subnets



# DNSEncrypt

## Принцип действия

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

```
dig @77.88.8.78 -p 15353 2.dnscrypt-cert.browser.yandex.net. \  
-t TXT +short
```

# DNSCrypt. Особенности

- Не меняет спецификацию DNS
- Нет ни RFC, ни Draft. Только спецификация на сайте
- Не предусмотрена замена мастер-ключа
- Заметное количество программ
- **Нет автообнаружения**
- Не «взлетел»

# 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

```
curl -H 'accept: application/dns-json' \  
      'https://dns.google/resolve?name=example.com' | jq
```

```
curl -H 'accept: application/dns-json' \  
      'https://cloudflare-dns.com/dns-query?name=example.com' | jq
```

# 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

```
kdig +tls @8.8.8.8 highload.ru # попробуйте 195.208.4.1  
dig +tls @1.1.1.1 highload.ru
```

# 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

```
kdig +tls @8.8.8.8 highload.ru # попробуйте 195.208.4.1  
dig +tls @1.1.1.1 highload.ru
```

- 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

```
kdig +tls @8.8.8.8 highload.ru # попробуйте 195.208.4.1  
dig +tls @1.1.1.1 highload.ru
```

- 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  
требуется «бутстрапа» имени сервера
- **Нет автообнаружения**
- Специальный 853 порт

# 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`

```
kdig +https @8.8.8.8 highload.ru # попробуйте 195.208.4.1  
dig +https @1.1.1.1 highload.ru
```



# DNS-over-HTTPS (DoH). Особенности

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

# Защита. Must have

- Ресолверы в зонах доверия  
или даже DoH/DoT до публичных серверов
- Локальные кэши в каждом периметре
  - NodeLocal DNSCache в Kubernetes
  - ~~systemd-resolved~~, unbound, Knot Resolver
- DoT/DoH через недоверенные сети  
особенно локальные домены

# Защита канала. Вот незадача



технические связи



прослушка, подмена



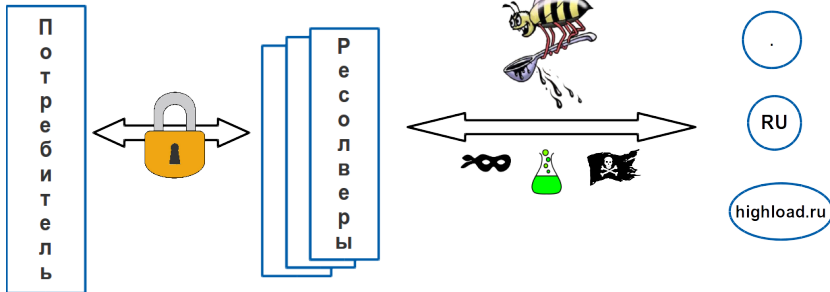
отравление



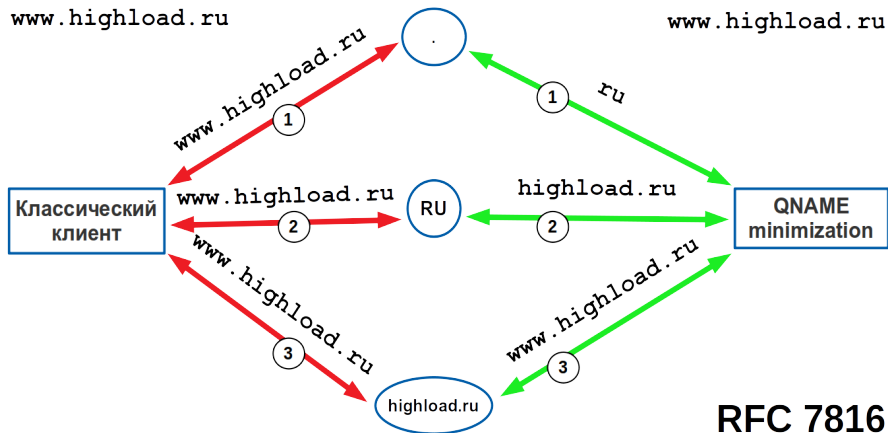
захват маршрутов  
(BGP-hijacking)



DoT/DoH/DoQ



# Минимизация QNAME



RFC 7816

# EDNS Client subnet

Это расширение DNS

- Добавляет в запрос подсеть клиента
- Например, для геобалансинга

Поддержка

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

# EDNS Client subnet

Это расширение DNS

- Добавляет в запрос подсеть клиента
- Например, для геобалансинга

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
```

# Известные сервисы отладки

- `whoami.akamai.net A`
- `whoami.akamai.net AAAA`
- `o-o.myaddr.l.google.com TXT`
- `whoami.cloudflare.com TXT`
- `whoami.ipv6.akahelp.net TXT`
- `whoami.ipv4.akahelp.net TXT`
- `whoami.ds.akahelp.net TXT`

# Как проверить ресолвер

Google Public DNS. DNS blocking and hijacking<sup>28</sup>

```
dig -t TXT test.dns.google.com. '@dns.google.'
```

```
dig -t TXT +tcp locations.dns.google.com. '@dns.google.'
```

Have problems with 1.1.1.1? \*Read Me First\*<sup>29</sup>

```
dig +short CHAOS TXT id.server @1.1.1.1
```

```
dig @1.1.1.1 whoami.Cloudflare.com txt +short
```



# Версия сервера

```
dig +short -c CHAOS -t TXT version.bind @8.8.8.8  
dig +short -c CHAOS -t TXT id.server @1.1.1.1
```

- RFC4892 — идентификация сервера<sup>30</sup>
- HOSTNAME.BIND, VERSION.BIND, ID.SERVER

# Настройка локальных кэшей

- Включение/выключение QNAME
- Манипуляции с Client subnet

# Реакционизм. Подделка

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

# Реакционизм. Прослушка

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

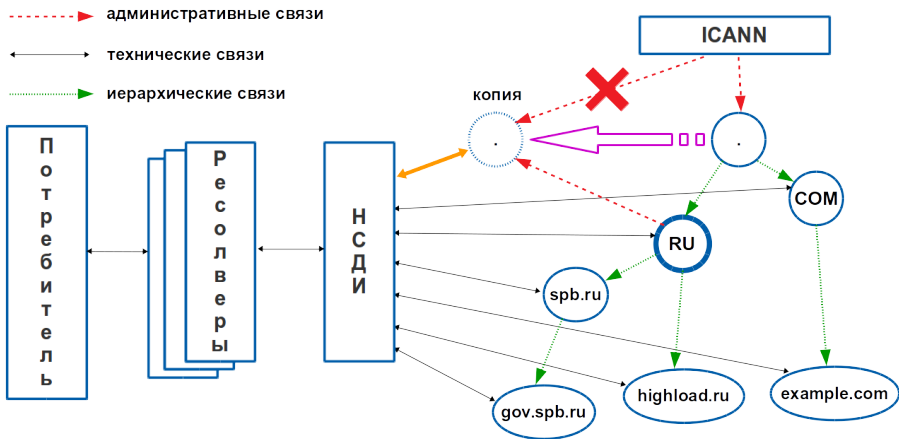
# Реакционизм. Прослушка

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

# Реакционизм. Госрегулирование

- Давление UK ISPA и IWF  
[www.opennet.ru/opennews/art.shtml?num=51046](http://www.opennet.ru/opennews/art.shtml?num=51046)
- Большинство «госблокировок» в мире основано на манипуляциях с DNS

# Национальная система доменных имен



# Госрегулирование РФ. НСДИ

Национальная система доменных имен

- Определена в законе 90-ФЗ от 01.05.2019  
Приказ Роскомнадзора от 31.07.2019 № 229
- Государственный публичный DNS
- Дублирует . (корень)
- Уменьшает ущерб от манипуляций с **.RU**  
гипотетических, со стороны США в лице ICANN
- Обслуживается ЦМУ ССОП
- Предоставляется в том числе AXFR



# Заложенная в НСДИ безопасность

# Заложенная в НСДИ безопасность



# 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](mailto:schors@gmail.com)

# Ссылки. DNSCurve и DNSCrypt

- [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/>.
- [5] DNSCrypt version 2 protocol specification. <https://dnscrypt.info/protocol/>.
- [6] dnscrypt-proxy. <https://github.com/DNSCrypt/dnscrypt-proxy>.

# Ссылки. DNSSEC

- [7] RFC 4255. Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints. Янв. 2006.  
<https://datatracker.ietf.org/doc/html/rfc4255>.
- [8] Визуализация DNSSEC. <http://dnsviz.net/>.
- [9] Филипп Кулин. DNSSEC. Руководство регистратора доменов. Дек. 2016.  
<https://www.slideshare.net/schors/dnssec-71055077>.
- [10] Филипп Кулин. DNSSEC. Руководство оператора доменов. Окт. 2017.  
<https://www.slideshare.net/schors/enog14-dnssec>.
- [11] RFC 4033. Введение в DNSSEC. Март 2005. <https://tools.ietf.org/html/rfc4033>.
- [12] RFC 4034. Ресурсные записи для DNSSEC. Март 2005. <https://tools.ietf.org/html/rfc4034>.
- [13] RFC 4035. Модификации протокола DNS для DNSSEC. Март 2005.  
<https://tools.ietf.org/html/rfc4035>.
- [14] RFC 6781. Эксплуатация DNSSEC. Дек. 2012. <https://tools.ietf.org/html/rfc6781>.
- [15] RFC 7583. Соображения по ротации ключей DNSSEC. Окт. 2015.  
<https://tools.ietf.org/html/rfc7583>.
- [16] RFC 7129. Authenticated Denial of Existence in the DNS. Определение белой лжи. Февр. 2014.  
<https://datatracker.ietf.org/doc/html/rfc7129>.
- [17] Dani Grant (Cloudflare). Economical With The Truth: Making DNSSEC Answers Cheap. Определение черной лжи. 24 июня 2016. <https://blog.cloudflare.com/black-lies/>.

# Ссылки. DoH/DoT

- [18] RFC 7858. Specification for DNS over Transport Layer Security (TLS). Май 2016.  
<https://datatracker.ietf.org/doc/html/rfc7858>.
- [19] RFC 8310. Usage Profiles for DNS over TLS and DNS over DTLS. Март 2018.  
<https://datatracker.ietf.org/doc/html/rfc8310>.
- [20] RFC 8484. DNS Queries over HTTPS (DoH). Окт. 2018.  
<https://datatracker.ietf.org/doc/html/rfc8484>.
- [21] Specification of DNS over Dedicated QUIC Connections. draft-huitema-dprive-dnsquic-00. Май 2020.  
<https://datatracker.ietf.org/doc/html/draft-huitema-dprive-dnsquic>.
- [22] Experimental DNS-over-TLS Auto-discovery. [https://github.com/CZ-NIC/knot-resolver/tree/c8cb9740f8ebd34219c7d860106969fcb6c7bf6/modules/experimental\\_dot\\_auth](https://github.com/CZ-NIC/knot-resolver/tree/c8cb9740f8ebd34219c7d860106969fcb6c7bf6/modules/experimental_dot_auth).

# Ссылки. Инциденты

- [23] Aftab Siddiqui. What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets. 27 апр. 2018.  
<https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/>.
- [24] Wikipedia. DNS hijacking. Manipulation by ISPs.  
[https://en.wikipedia.org/wiki/DNS\\_hijacking#Manipulation\\_by\\_ISPs](https://en.wikipedia.org/wiki/DNS_hijacking#Manipulation_by_ISPs).
- [25] Леонид Евдокимов. Тайный список запрещённых ресурсов. 25 сент. 2018.  
<https://usher2.club/articles/mt-free-pre-block/>.



# Ссылки. Разное

- [26] Brian Kernighan. UNIX: A History and a Memoir. 18 окт. 2019.
- [27] RFC 7816. DNS Query Name Minimisation to Improve Privacy. Март 2016.  
<https://datatracker.ietf.org/doc/html/rfc7816>.
- [28] Google Public DNS. Troubleshooting.  
<https://developers.google.com/speed/public-dns/docs/troubleshooting>.
- [29] Have problems with 1.1.1.1? \*Read Me First\*. <https://community.cloudflare.com/t/have-problems-with-1-1-1-1-read-me-first/15902>.
- [30] RFC 4892. Requirements for a Mechanism Identifying a Name Server Instance. Июнь 2007.  
<https://datatracker.ietf.org/doc/html/rfc4892>.
- [31] RFC 7871. EDNS(0) Client Subnet. Май 2016. <https://datatracker.ietf.org/doc/html/rfc7871>.
- [32] Introducing a New whoami Tool for DNS Resolver Information.  
<https://developer.akamai.com/blog/2018/05/10/introducing-new-whoami-tool-dns-resolver-information>.

# Ссылки. L<sup>A</sup>T<sub>E</sub>X

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