

Колоколов С. А., Белый К. С.

РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия

НАСТРОЙКА DNSSEC И УПРАВЛЕНИЯ КЛЮЧАМИ НА УЧЕБНОМ СТЕНДЕ WINDOWS SERVER

Аннотация. Работа описывает настройку DNSSEC и управление ключами на учебном стенде из двух виртуальных машин Windows Server. Один узел размещает авторитативную зону lab.test, второй обрабатывает запросы с настроенным перенаправлением. Представлены создание зоны, её подписание, параметры ключей и подписей, действия с доверенным ключом и ответы средств PowerShell. После подписания показан ответ с A и RRSIG при запросе с параметром DnssecOk. Этот вывод подтверждает получение DNSSEC-данных, но не удостоверяет успешную криптографическую проверку подписи и всей цепочки доверия. После повторного подписания и очистки кэша получен DNS server failure. Следующий листинг показывает файл экспортированного ключа; импорт trust anchor и успешный запрос после импорта в доступных материалах не представлены. Поэтому причина ошибки и восстановление разрешения имени не считаются установленными результатами. Отдельные кадры Wireshark иллюстрируют размеры ответов подписанной и неподписанной зон, а не среднюю производительность или серию измерений. На основе приведённых источников обсуждаются ротация KSK и ZSK, RFC 5011, NSEC3 и отсутствие конфиденциальности DNS-запросов. Практическая часть ограничена показанными командами, настройками и ответами. Работа может служить учебным разбором настройки DNSSEC и основанием для планирования последующей проверки доверия. Она не оценивает эффективность защиты от атак, доступность производственной системы или успешность всех механизмов валидации. Численные результаты времени разрешения и статистические серии не используются для выводов.

Ключевые слова: DNSSEC; безопасность DNS; trust anchor; Windows Server; цифровые подписи; цепочка доверия; управление ключами.

Введение

Современные информационные системы, корпоративные сети и облачные инфраструктуры в значительной степени зависят от корректной и устойчивой работы системы доменных имён (Domain Name System, DNS). DNS выполняет критически важную функцию сопоставления символьных доменных имён с IP-адресами узлов сети, обеспечивая функционирование веб-ресурсов, почтовых сервисов, распределённых приложений и корпоративных информационных систем. Фактически DNS является одним из базовых элементов сетевой инфраструктуры, без которого невозможна стабильная работа большинства сетевых сервисов.

Однако изначальная архитектура протокола DNS разрабатывалась в условиях доверенной сетевой среды и не предусматривала встроенных механизмов криптографической защиты. Ответы DNS-серверов принимаются клиентами без проверки подлинности источника и целостности передаваемых данных. Такая модель создаёт предпосылки для реализации различных атак, среди которых наибольшую опасность представляют атаки типа cache poisoning (отравление кэша), spoofing (подмена ответов) и man-in-the-middle. В результате злоумышленник может перенаправить пользователя на поддельный ресурс, перехватить конфиденциальные данные либо нарушить работу критически важных сервисов.

В условиях роста киберугроз и увеличения числа распределённых сервисов проблема обеспечения доверия к DNS-инфраструктуре приобрела особую актуальность. Для решения данной задачи был разработан набор расширений DNSSEC (Domain Name System Security Extensions), направленный на обеспечение аутентичности и целостности DNS-ответов. В отличие от классического DNS, DNSSEC использует механизмы асимметричной криптографии, позволяющие подписывать данные зоны цифровой подписью и проверять их корректность на стороне валидирующего резолвера.

Принцип работы DNSSEC основан на публикации открытых ключей зоны (DNSKEY) и цифровых подписей (RRSIG) для наборов ресурсных записей. Валидирующий резолвер при наличии доверенного ключа (trust anchor) и соответствующей цепочки доверия проверяет подписи полученных данных. Ошибка проверки может привести к SERVFAIL; без сведений о

настройках валидатора нельзя считать любую такую ошибку подтверждением нарушения криптографической проверки [1, 2].

Несмотря на очевидные преимущества DNSSEC с точки зрения безопасности, практическое внедрение технологии связано с рядом организационных и технических сложностей. Одной из ключевых проблем является управление жизненным циклом криптографических ключей, включая их генерацию, публикацию, ротацию и обновление trust anchor на валидирующих серверах. Несогласованность ключевой информации может привести к нарушению цепочки доверия и, как следствие, к отказу разрешения доменных имён. Таким образом, DNSSEC повышает уровень защищённости DNS-инфраструктуры, но одновременно предъявляет повышенные требования к администрированию и сопровождению системы.

Объектом данного исследования являются механизмы обеспечения безопасности DNSSEC в серверной инфраструктуре на базе Windows Server. Предмет исследования — процессы подписания DNS-зоны, настройки валидирующего резолвера и управления trust anchor в условиях изолированного лабораторного стенда.

Цель работы — описать настройку DNSSEC и управление ключами на изолированном стенде Windows Server, а также проанализировать ответы DNS после повторного подписания зоны. Отдельно рассматривается гипотеза о влиянии несогласованных доверенных ключей, но её подтверждение требует данных о состоянии валидации и сравнения trust anchor.

Для достижения поставленной цели в работе решаются следующие задачи:

- проверить создание и подписание DNS-зоны, получение DNSSEC-данных и поведение службы DNS после переподписания зоны;
- описать параметры управления ключами и ограничения выводов по отдельным захватам DNS-трафика.

Практическая значимость работы состоит в демонстрации конфигурационного сценария на двух виртуальных машинах: создание подписанной зоны, получение A и RRSIG, повторное подписание и регистрация ошибки разрешения имени. Импорт обновлённого trust anchor и успешное восстановление запроса в приведённых результатах не показаны; причина ошибки остаётся гипотезой, требующей отдельной проверки.

Литературный обзор

Классический DNS не предусматривает механизмов криптографической проверки подлинности и целостности ответов, что делает возможными атаки типа spoofing и cache poisoning.

DNSSEC стандартизирован в RFC 4033–4035 [1–3] и обеспечивает криптографическую защиту данных зоны посредством цифровых подписей и цепочки доверия от trust anchor.

При невозможности подтверждения подписи валидирующий резолвер возвращает ошибку (SERVFAIL), реализуя модель fail-secure [1].

Управление ключами KSK и ZSK является критическим элементом внедрения DNSSEC, поскольку нарушение синхронизации ключевой информации приводит к разрыву цепочки доверия [4].

В Windows Server поддержка DNSSEC реализована на уровне службы DNS и включает средства подписания зон, управления ключами и настройки trust anchor. Дополнительным аспектом безопасности DNSSEC является механизм authenticated denial of existence [3, 5], реализуемый с помощью записей NSEC или NSEC3 [5]. Данный механизм позволяет криптографически подтвердить отсутствие запрашиваемого имени в зоне. Однако использование NSEC без дополнительных мер может приводить к возможности перечисления имён зоны (zone walking). Для предотвращения этого эффекта применяется механизм NSEC3, использующий хеширование имён.

DNSSEC обеспечивает целостность и подлинность данных, но не гарантирует конфиденциальность DNS-запросов [6]. Для защиты канала передачи применяются технологии DNS over TLS и DNS over HTTPS [7, 8], которые не заменяют механизм криптографической валидации зоны.

Рассмотренные стандарты описывают проверку подписанных DNS-данных и построение цепочки доверия. В рамках настоящей работы на зоне lab.test представлены результаты переподписания и последующего DNS-ответа с ошибкой; причинная связь с несоответствием trust anchor требует отдельного подтверждения.

Практическая часть представляет учебный пример настройки DNSSEC в изолированной серверной среде и анализа доступных команд, сетевых кадров и сообщений службы DNS.

Материалы и методы

Исследование механизмов безопасности DNSSEC проводилось с использованием теоретического анализа и лабораторного эксперимента. Такой подход позволил сопоставить принципы функционирования технологии DNSSEC, описанные в нормативных документах и технической литературе, с её практической реализацией в серверной среде Windows Server.

На теоретическом этапе был выполнен анализ стандартов DNSSEC (RFC 4033–4035) и документации по службе DNS в Windows Server. Особое внимание уделялось принципам формирования цифровых подписей зоны, публикации записей DNSKEY и RRSIG, построению цепочки доверия (chain of trust), а также роли trust anchor в процессе валидации DNS-ответов.

Практическая часть выполнена на двух узлах Windows Server 2025 в изолированной сети. SRV-A размещает авторитативную зону, а SRV-B обрабатывает запросы с настроенным перенаправлением для lab.test. Команды и ответы иллюстрируют конфигурацию DNSSEC; отдельный статус успешной проверки цепочки доверия в показанном выводе отсутствует.

Использованы средства администрирования DNS и PowerShell. Показаны подписание зоны, настройка trust anchor, повторное подписание и ответы на последующие запросы. Наблюдаемые ответы и ошибки рассматриваются отдельно от предполагаемой причины: наличие RRSIG и параметра -DnssecOk само по себе не является доказательством успешной валидации.

В практической части рассматриваются конфигурация DNSSEC, получение подписанных записей и представленные захваты DNS-ответов на сервере SRV-B. Отдельные кадры Wireshark иллюстрируют содержимое и размеры ответов, но не сравнительную производительность DNS-разрешения.

В рукописи не представлены итоговые временные ряды, серии из 20 ответов или результаты фильтрации выбросов. Поэтому расчёт среднего времени, среднего размера пакета и статистическая обработка не включены в доказательную часть этой работы.

Настройка статических IP-адресов

На первом этапе эксперимента выполнена ручная настройка сетевого интерфейса обеих виртуальных машин. В свойствах протокола IPv4 на первой машине установлен статический IP-адрес 192.168.56.10, на второй - 192.168.56.11, оба адреса имеют маску подсети 255.255.255.0. В качестве предпочитаемого DNS-сервера указан локальный адрес 127.0.0.1, что соответствует дальнейшей настройке службы DNS на данном узле.

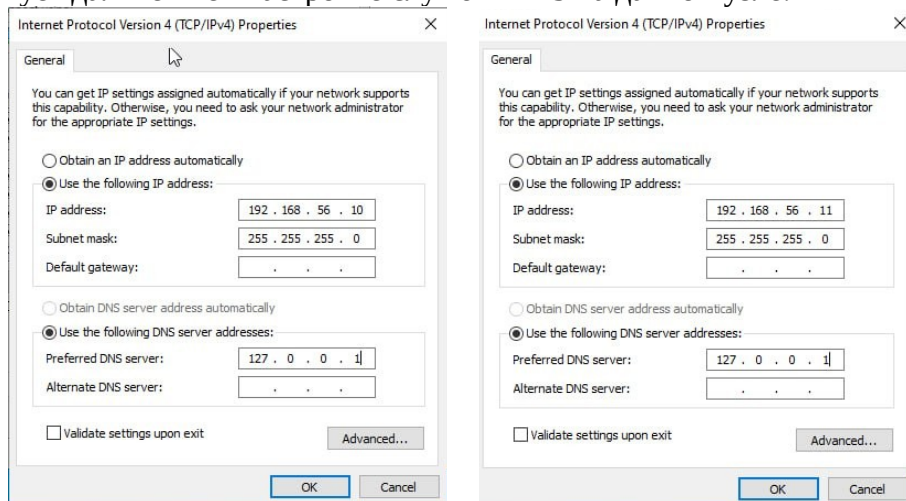


Рис. 1. Настройка статических IP-адресов на SRV-A и SRV-B

Установка роли DNS Server

На обоих серверах показана установка роли DNS Server командой Install-WindowsFeature DNS -IncludeManagementTools. Приведённый вывод подтверждает успешную установку роли и средств администрирования.

Листинг 1 – Установка роли DNS Server

```
PS C:\Users\Administrator> Install-WindowsFeature DNS -IncludeManagementTools
>>
Success Restart Needed Exit Code Feature Result
-----
True      No                Success    {DNS Server, Remote Server Administration ...}

PS C:\Users\Administrator> Get-WindowsFeature DNS
>>
Display Name                                Name      Install State
-----
[X] DNS Server                             DNS       Installed

PS C:\Users\Administrator>
```

Создание зоны lab.test

На сервере выполнено создание первичной зоны lab.test с использованием Add-DnsServerPrimaryZone; полный вывод этой команды в рукописи отсутствует.

Создание А-записи

Для узла www зоны lab.test задана А-запись с адресом 10.10.10.10 с использованием Add-DnsServerResourceRecordA. Текст команды создания записи не приведён; адрес подтверждён последующим DNS-ответом.

Подписание DNSSEC-зоны lab.test

На SRV-A показано подписание зоны lab.test и получение записей DNSKEY и RRSIG. В выводе представлены параметры NSEC3 и признаки использования RSA/SHA256 для подписей. Часть сведений об алгоритмах и жизненном цикле ключей подтверждается выводом переподписания в листинге 5.

Листинг 2 – Записи DNSKEY и RRSIG зоны lab.test

```
Authenticated Denial of Existence: NSec3
Random Salt Length: 8 octets
NSec3 Hash Algorithm: RsaSha1
NSec3 Iterations: 50
NSec3 OptOut: No.
Do you wish to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

ZoneName      ZoneType      IsAutoCreated  IsDsIntegrated  IsReverseLookupZone
-----
lab.test      Primary       False          False           False
True

PS C:\Users\Administrator> Get-DnsServerResourceRecord -ZoneName "lab.test"
-RRType DNSKEY
>> Get-DnsServerResourceRecord -ZoneName "lab.test" -RRType RRSIG
>>
HostName      RecordType Type Timestamp TimeToLive RecordData
-----
@              DNSKEY      48  0      01:00:00 [ZoneKey]
[RsaSha256][23208]
@              DNSKEY      48  0      01:00:00 [ZoneKey]
[RsaSha256][28641]
@              DNSKEY      48  0      01:00:00 [SEP][ZoneKey]
[RsaSha256][59717]
@              DNSKEY      48  0      01:00:00 [SEP][ZoneKey]
```

```

[RsaSha256][20947]
@                RRSIG      46    0          01:00:00  [NS][RsaSha256]
[23208]
@                RRSIG      46    0          01:00:00  [SOA][RsaSha256]
[23208]
@                RRSIG      46    0          01:00:00  [DNSKEY]
[RsaSha256][23208]
@                RRSIG      46    0          01:00:00  [DNSKEY]
[RsaSha256][59717]
@                RRSIG      46    0          01:00:00  [NSEC3PARAM]
[RsaSha256][23208]
[hostname truncated in screenshot] RRSIG 46 0 01:00:00 [NSEC3][RsaSha256][23208]
[hostname truncated in screenshot] RRSIG 46 0 01:00:00 [NSEC3][RsaSha256][23208]
www              RRSIG      46    0          01:00:00  [A][RsaSha256]
[23208]

```

PS C:\Users\Administrator>

Проверка типа зоны на SRV-B

На втором сервере выполнена проверка списка зон с использованием команды Get-DnsServerZone. В выводе отображается, что зона lab.test имеет тип Forwarder, что подтверждает её настройку в режиме переадресации, а не как первичной (Primary) зоны.

Листинг 3 – Проверка типа зоны на SRV-B

```

PS C:\Users\Administrator> Get-DnsServerZone | Select-Object ZoneName, ZoneType
>>
ZoneName      ZoneType
-----
0.in-addr.arpa Primary
127.in-addr.arpa Primary
255.in-addr.arpa Primary
lab.test      Forwarder

```

Получение DNSSEC-данных на SRV-B

На SRV-B выполнен Resolve-DnsName www.lab.test -Server 127.0.0.1 -DnssecOk. Вывод содержит A и RRSIG: сервер вернул DNSSEC-данные по этому запросу. Параметр -DnssecOk запрашивает такие данные, но показанный вывод не сообщает результат криптографической проверки подписи или всей цепочки доверия.

Листинг 4 – Успешный DNSSEC-ответ на SRV-B

```
Resolve-DnsName www.lab.test -Server 127.0.0.1 -DnssecOk
```

```

Name      Type TTL  Section IPAddress
----
www.lab.test A    3600 Answer  10.10.10.10

```

```

Name      : www.lab.test
QueryType  : RRSIG
TTL        : 3600
Section    : Answer
TypeCovered : A
Algorithm  : 8
LabelCount : 3
OriginalTtl : 3600
Expiration : 2/22/2026 2:28:16 PM
Signed     : 2/12/2026 1:28:16 PM
Signer     : lab.test
Signature  : {49, 82, 246, 205, ...}

```

```

Name      : .
QueryType  : OPT
TTL        : 32768
Section    : Additional
Data       : {}

```

```
PS C:\Users\Administrator>
```

Повторное подписание зоны lab.test

На авторитативном сервере выполнены снятие DNSSEC-подписей и повторное подписание lab.test. Вывод команды содержит параметры новых KSK и ZSK, периоды ротации и параметры NSEC3.

Листинг 5 – Переподписание зоны lab.test на SRV-A

```
PS C:\Users\Administrator> Invoke-DnsServerZoneUnsign -ZoneName "lab.test"
-Force
>> Invoke-DnsServerZoneSign -ZoneName "lab.test" -SignWithDefault -PassThru
-Verbose
>>
VERBOSE: This will reset the DNSSEC settings for the zone to defaults and sign
it.
The following parameters will be configured:
One KeySigningKey with:
  CryptoAlgorithm: RsaSha256
  Key Length: 2048
  Rollover Period: 755.00:00:00
One ZoneSigningKey with:
  CryptoAlgorithm: RsaSha256
  Key Length: 1024
  Rollover Period: 90.00:00:00
Authenticated Denial of Existence: NSec3
Random Salt Length: 8 octets
NSec3 Hash Algorithm: RsaSha1
NSec3 Iterations: 50
NSec3 OptOut: No.

Confirm
This will reset the DNSSEC settings for the zone to defaults and sign it.
The following parameters will be configured:
One KeySigningKey with:
  CryptoAlgorithm: RsaSha256
  Key Length: 2048
  Rollover Period: 755.00:00:00
One ZoneSigningKey with:
  CryptoAlgorithm: RsaSha256
  Key Length: 1024
  Rollover Period: 90.00:00:00
Authenticated Denial of Existence: NSec3
Random Salt Length: 8 octets
NSec3 Hash Algorithm: RsaSha1
NSec3 Iterations: 50
NSec3 OptOut: No.
Do you wish to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

ZoneName ZoneType IsAutoCreated IsDsIntegrated IsReverseLookupZone IsSigned
-----
lab.test Primary False False False True
```

Проверка разрешения имени после смены ключей

После переподписания зоны на авторитативном сервере выполнены очистка кэша и повторный запрос www.lab.test на SRV-B с параметром -DnssecOk. Получена ошибка DNS server failure (SERVFAIL). По одному этому выводу нельзя однозначно установить причину ошибки.

Листинг 6 – Ошибка разрешения имени на SRV-B после смены ключей

```
PS C:\Users\Administrator> Clear-DnsServerCache -Force
>> Resolve-DnsName www.lab.test -Server 127.0.0.1 -DnssecOk
>>
Resolve-DnsName : www.lab.test : DNS server failure
```

```
At line:2 char:1
+ Resolve-DnsName www.lab.test -Server 127.0.0.1 -DnssecOk
+ ~~~~~
+ CategoryInfo          : ResourceUnavailable: (www.lab.test:String)
[Resolve-DnsName], Win32Exception
+ FullyQualifiedErrorId :
RCODE_SERVER_FAILURE,Microsoft.DnsClient.Commands.ResolveDnsName

PS C:\Users\Administrator>
```

Просмотр экспортированного ключа

После показанного SERVFAIL представлен файл keyset-lab.test в каталоге C:\DNSSEC. Наличие файла само по себе не подтверждает импорт trust anchor на SRV-B; команда импорта и успешный запрос после неё в доступных листингах отсутствуют.

Листинг 7 – Проверка экспортированного файла ключа

```
PS C:\Users\Administrator> dir C:\DNSSEC
>>
Directory: C:\DNSSEC

Mode                LastWriteTime         Length Name
----                -
-a---- 2/12/2026 1:02 PM          805    keyset-lab.test
```

```
PS C:\Users\Administrator>
```

Создание неподписанной зоны plain.test

Анализ DNS-ответов в Wireshark

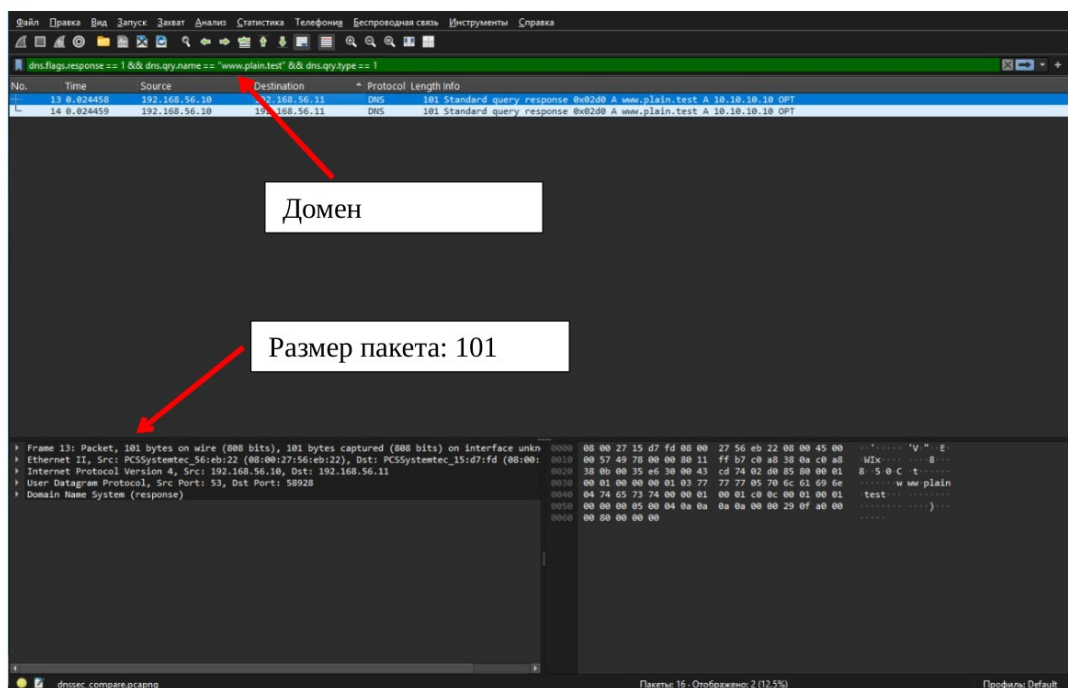


Рис. 2. DNS-ответ для www.plain.test без DNSSEC (101 байт)

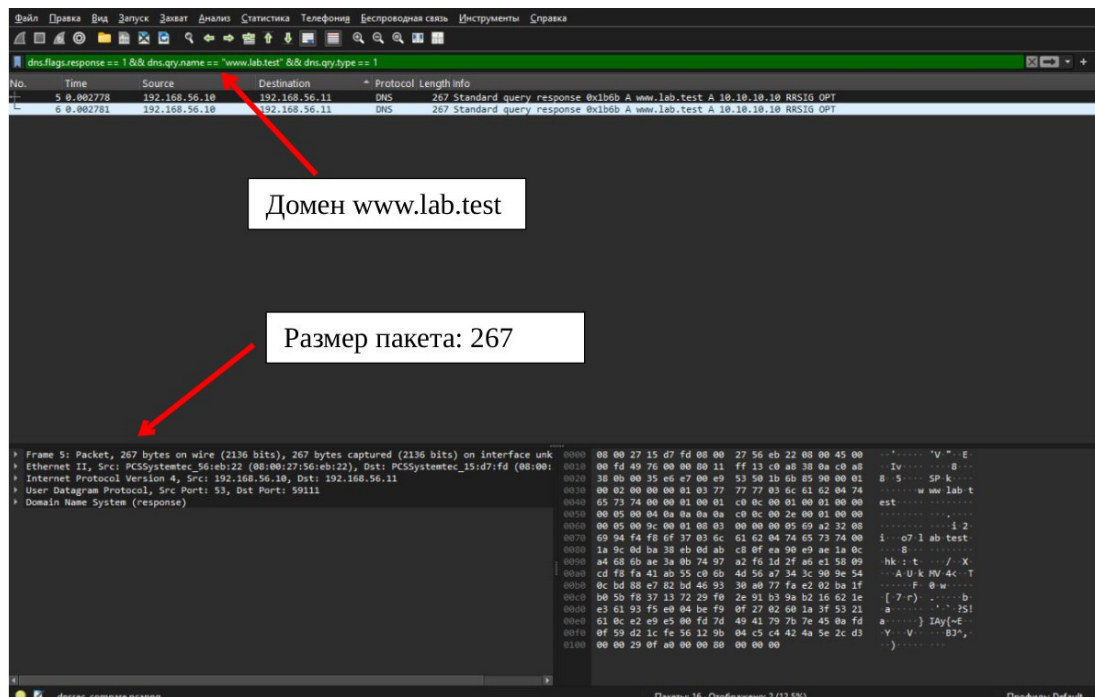


Рис. 3. DNS-ответ для www.lab.test с DNSSEC (267 байт)

Результаты исследования

Представленные команды и ответы иллюстрируют настройку DNSSEC на двух узлах. Они не являются самостоятельной проверкой успешной валидации, эффективности защиты от атак или доступности DNS-сервиса.

В показанной конфигурации создана зона lab.test с A-записью www, разрешаемой в адрес 10.10.10.10. Отдельный вывод запроса до подписания зоны в рукописи не приведён.

После подписания зоны средствами DNSSEC произошло появление записей типов DNSKEY и RRSIG в структуре зоны. Это говорит о генерации криптографических ключей и цифровых подписей.

На SRV-B показан ответ A вместе с RRSIG по запросу с -DnssecOk. Это подтверждает получение DNSSEC-данных, но не сообщает статус проверки подписи и цепочки доверия; наличие forwarder-зоны не является самостоятельным доказательством роли валидатора.

После повторного подписания зоны и очистки кэша показан SERVFAIL. Затем приведено наличие файла экспортированного ключа. По этим листингам нельзя подтвердить импорт обновлённого trust anchor, восстановление разрешения имени или причину ошибки именно в несоответствии доверенного ключа.

В промышленной эксплуатации ключами DNSSEC часто управляют по регламентированным процедурам с поддержкой автоматической ротации при наличии соответствующей функциональности и конфигурации сервера. Успешность такой ротации в данном стенде не проверялась.

Стандарт RFC 5011 описывает механизм автоматического обновления trust anchor при соблюдении предусмотренных условий. В представленных листингах не показано, что механизм был задействован или корректно обновил доверенный ключ на SRV-B.

Показанный SERVFAIL демонстрирует отказ разрешения имени в этой последовательности команд. Без отдельного статуса валидации и сравнения ключей причина отказа не установлена; результат не оценивает снижение риска атак или все реализации DNSSEC.

Стандарты DNSSEC задают механизмы проверки подписанных DNS-данных; перечисленные ниже ограничения и сценарии не проверялись в эксперименте на lab.test и приводятся как свойства технологии по нормативным источникам:

- подмену DNS-ответов (spoofing);
- отравление кэша резолвера (cache poisoning);

- внедрение ложных ресурсных записей при перехвате трафика;
- подмену данных на промежуточных узлах сети.

Защита достигается за счёт криптографической подписи наборов записей и построения цепочки доверия от доверенного ключа верхнего уровня (trust anchor) до авторитативной зоны [1, 2, 3].

В то же время проведённый анализ показывает, что DNSSEC не обеспечивает комплексную защиту DNS-инфраструктуры и имеет ряд принципиальных ограничений.

Для иллюстрации состава DNS-ответов использованы отдельные захваты сетевого обмена в лабораторном стенде.

Анализ сетевого трафика

В отдельных кадрах Wireshark на рисунках 2 и 3 показаны размеры двух ответов для lab.test и plain.test. Это отдельные наблюдения, а не серия измерений; по ним нельзя делать вывод о среднем времени разрешения или сравнительной производительности зон.

Следует отметить, что в реальных сетевых инфраструктурах размер DNSSEC-ответов может быть значительно больше, чем в условиях лабораторного эксперимента. Особенно это касается ответов, содержащих записи DNSKEY и полный набор криптографических подписей зоны.

Классический DNS по UDP ограничивал размер сообщения 512 байтами без EDNS. Расширение EDNS(0) позволяет объявлять больший размер полезных данных UDP; при превышении допустимого размера ответа или невозможности его передачи может использоваться TCP. Автоматический переход зависит от реализации и условий обмена.

При внедрении DNSSEC в производственных сетях необходимо учитывать возможные проблемы, связанные с фрагментацией крупных UDP-пакетов и их фильтрацией сетевыми экранами и NAT-устройствами, что может приводить к задержкам или сбоям в разрешении доменных имён.

Приведённые захваты иллюстрируют отдельные DNS-ответы в данном стенде. Оценка сравнительной производительности требует воспроизводимых повторных измерений с согласованными условиями и сохранёнными исходными данными.

Во-первых, DNSSEC не обеспечивает конфиденциальность DNS-запросов: их содержимое может быть доступно наблюдателю сетевого трафика. Это ограничение рассматривается в RFC 7626 [6]; оно не является результатом специального эксперимента на данном стенде.

Во-вторых, использование механизма authenticated denial of existence на основе записей NSEC может приводить к возможности перечисления имён зоны (zone walking), поскольку NSEC раскрывает информацию о соседних записях [3]. Для снижения данного риска применяется механизм NSEC3, основанный на хешировании имён [5], однако он не исключает полностью возможность перебора при слабых параметрах хеширования.

Authenticated denial of existence с NSEC3 рассматривается в источнике [5]. В данной рукописи не приведён вывод запроса fake.lab.test с NXDOMAIN и NSEC3, поэтому такая проверка не включена в перечень подтверждённых практических результатов.

В-третьих, DNSSEC не защищает от компрометации криптографических ключей. В случае утечки закрытого ключа KSK злоумышленник получает возможность формировать корректно подписанные, но недостоверные данные. Практики безопасного управления ключами и процедуры их ротации регламентируются отдельными рекомендациями [4], что подчёркивает необходимость организационных и технических мер защиты инфраструктуры управления ключами.

DNSSEC предназначен для проверки подлинности и целостности DNS-данных и не обеспечивает конфиденциальность запросов [2, 6]. Практическая часть этой статьи иллюстрирует конфигурацию и ответы; успешность криптографической проверки и причинная связь SERVFAIL с trust anchor отдельно не установлены.

Заключение

На учебном стенде показаны создание и подписание зоны lab.test, настройка перенаправления DNS-запросов, повторное подписание и последующие запросы. Показанные команды и иллюстрации описывают конфигурационный сценарий, но не подтверждают полный цикл обновления trust anchor.

Криптографическая проверка DNSSEC основывается на подписях и цепочке доверия, описанных в стандартах [1–3]. Возвращённая RRSIG показывает наличие подписанных данных, но не заменяет подтверждение успешной валидации.

После повторного подписания зоны и очистки кэша показан ответ DNS server failure. Последующий листинг показывает файл экспортированного ключа, но не его импорт и не успешное разрешение имени после импорта. Поэтому восстановление DNS-разрешения и причинная атрибуция ошибки именно нарушению цепочки доверия не считаются подтверждёнными результатами.

Выводы ограничены показанными командами, конфигурацией и ответами двух виртуальных машин. Производительность, устойчивость к атакам и успешность всех криптографических проверок не оценивались. Материал может использоваться для учебного разбора настройки DNSSEC и планирования дальнейших проверок.

Библиографический список

45. Arends R., Austein R., Larson M., Massey D., Rose S. Protocol Modifications for the DNS Security Extensions // RFC 4035. – IETF, 2005. – 52 с. – URL: <https://datatracker.ietf.org/doc/html/rfc4035>.
46. Arends R., Austein R., Larson M., Massey D., Rose S. DNS Security Introduction and Requirements // RFC 4033. – Internet Engineering Task Force (IETF), 2005. – 21 с. – URL: <https://datatracker.ietf.org/doc/html/rfc4033>.
47. Arends R., Austein R., Larson M., Massey D., Rose S. Resource Records for the DNS Security Extensions // RFC 4034. – IETF, 2005. – 37 с. – URL: <https://datatracker.ietf.org/doc/html/rfc4034>.
48. Kolkman O., Mekking W. DNSSEC Operational Practices, Version 2 // RFC 6781. – IETF, 2012. – 53 с. – URL: <https://datatracker.ietf.org/doc/html/rfc6781>.
49. Laurie B., Sisson G., Arends R., Blacka D. DNSSEC Hashed Authenticated Denial of Existence (NSEC3) // RFC 5155. – IETF, 2008. – 32 с. – URL: <https://datatracker.ietf.org/doc/html/rfc5155>.
50. Bortzmeyer S. DNS Privacy Considerations // RFC 7626. – IETF, 2015. – 17 с. – URL: <https://datatracker.ietf.org/doc/html/rfc7626>.
51. Hu Z. и др. Specification for DNS over Transport Layer Security (TLS) // RFC 7858. – IETF, 2016. – URL: <https://datatracker.ietf.org/doc/html/rfc7858> (дата обращения: 17.02.2026).
52. Hoffman P., McManus P. DNS Queries over HTTPS (DoH) // RFC 8484. – IETF, 2018. – URL: <https://datatracker.ietf.org/doc/html/rfc8484> (дата обращения: 17.02.2026).

References

53. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). Protocol modifications for the DNS Security Extensions (RFC 4035). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc4035>
54. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). DNS security introduction and requirements (RFC 4033). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc4033>
55. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). Resource records for the DNS Security Extensions (RFC 4034). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc4034>
56. Kolkman, O., & Mekking, W. (2012). DNSSEC operational practices, version 2 (RFC 6781). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc6781>

57. Laurie, B., Sisson, G., Arends, R., & Blacka, D. (2008). DNSSEC hashed authenticated denial of existence (NSEC3) (RFC 5155). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc5155>
58. Bortzmeyer, S. (2015). DNS privacy considerations (RFC 7626). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc7626>
59. Hu, Z., et al. (2016). Specification for DNS over Transport Layer Security (TLS) (RFC 7858). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc7858>
60. Hoffman, P., & McManus, P. (2018). DNS queries over HTTPS (DoH) (RFC 8484). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc8484>

Информация об авторах

Колоколов С. А. — РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; e-mail: kolokolovstepa@gmail.com.

Белый К. С. — РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; для корреспонденции через соавтора С. А. Колоколова: kolokolovstepa@gmail.com.

DNSSEC CONFIGURATION AND KEY MANAGEMENT ON A WINDOWS SERVER TEACHING TESTBED

Kolokolov S. A., Bely K. S.

Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia

Abstract. *This paper describes DNSSEC configuration and key management on a teaching testbed with two Windows Server virtual machines. One node hosts the authoritative lab.test zone, while the other processes queries using configured forwarding. The article presents zone creation, signing parameters, keys and signatures, trust-anchor configuration steps, and PowerShell responses. A query using DnssecOk returns A and RRSIG data after signing. This output demonstrates receipt of DNSSEC records but does not establish successful cryptographic verification of the signature or complete trust chain. A DNS server failure is displayed after re-signing and clearing the cache. The next listing shows an exported key file; importing that trust anchor and obtaining a successful query after import are not documented in the available material. Accordingly, neither the precise cause of the failure nor restored name resolution is treated as a verified result. Individual Wireshark frames illustrate response sizes for signed and unsigned zones, rather than average performance or a measurement series. Cited sources support discussion of KSK and ZSK rollover, RFC 5011, NSEC3, and the lack of DNS-query confidentiality. The practical scope is limited to the displayed commands, configurations, and responses. The material supports teaching and planning further trust-validation checks. It does not assess attack resistance, production availability, or successful operation of all validation mechanisms.*

Keywords: *DNSSEC; DNS security; trust anchor; Windows Server; digital signatures; chain of trust; key management.*

Information about the authors

Stepan A. Kolokolov — Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: kolokolovstepa@gmail.com.

Kirill S. Bely — Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; correspondence through co-author Stepan A. Kolokolov: kolokolovstepa@gmail.com.