УДК 004.056.53

Прокофьева Арина Сергеевна

Студент
РГУ нефти и газа (НИУ) имени И. М. Губкина
Прокофьева Мария Сергеевна

Студент
РГУ нефти и газа (НИУ) имени И. М. Губкина
Научный руководитель: Уймин Антон Григорьевич
РГУ нефти и газа (НИУ) имени И. М. Губкина
Старший преподаватель кафедры безопасности информационных технологий

ТЕСТИРОВАНИЕ ЗАЩИЩЕННОСТИ DNS НА БАЗЕ WINDOWS SERVER

Аннотация: Настоящая статья посвящена исследованию и тестированию защищенности системы доменных имен (DNS) в среде Windows Server. В работе представлен детальный обзор теоретических основ безопасности DNS, включая ключевые угрозы, такие как подмена DNS, отравление кэша и атаки типа «отказ в обслуживании» (DDoS). Особое внимание уделено практическим аспектам настройки и проверки функций безопасности на платформе Windows Server 2022, включая DNSSEC, блокировку кэша, пул сокетов, безопасные передачи зон и политики DNS. Приведены подробные команды PowerShell и шаги для реализации и тестирования, а также результаты экспериментов, демонстрирующие эффективность предложенных мер. Статья предназначена для системных администраторов, специалистов по информационной безопасности и исследователей, стремящихся укрепить сетевую инфраструктуру.

Ключевые слова: DNS, безопасность, Windows Server, DNSSEC, DoH, тестирование, настройка, проверка, отравление кэша, DDoS

Annotation: This article focuses on the study and testing of Domain Name System (DNS) security within the Windows Server environment. It provides a comprehensive overview of the theoretical foundations of DNS security, addressing key threats such as DNS spoofing, cache poisoning, and distributed denial-of-service (DDoS) attacks. Special emphasis is placed on practical aspects of configuring and verifying security features on Windows Server 2022, including DNSSEC, cache locking, socket pool, secure zone transfers, and DNS policies. Detailed PowerShell commands and implementation steps are provided, along with experimental results demonstrating the effectiveness of the proposed measures. The article is intended for system administrators, information security professionals, and researchers aiming to strengthen network infrastructure.

Keywords: DNS, security, Windows Server, DNSSEC, DoH, testing, configuration, verification, cache poisoning, DDoS

ВВЕДЕНИЕ: АКТУАЛЬНОСТЬ

Система доменных имен (DNS) является фундаментальной частью сетевой инфраструктуры, обеспечивая преобразование доменных имен в IP-адреса, что необходимо для функционирования интернета и корпоративных сетей. Однако DNS подвержен множеству угроз, включая подмену DNS, отравление кэша, атаки типа «отказ в обслуживании» (DDoS) и перехват запросов. Эти уязвимости могут привести к серьезным последствиям, таким как перенаправление пользователей на вредоносные сайты, утечка конфиденциальных данных или нарушение работы сети. В корпоративных

средах, где Windows Server широко используется для управления DNS, обеспечение безопасности становится критически важным.

Согласно данным Cisco [1], количество DDoS-атак на DNS-серверы удвоилось с 7,9 миллиона в 2017 году до 15,4 миллиона в 2023 году. Кроме того, отчет DNSFilter за 2025 год [2] указывает, что каждый 174-й DNS-запрос является вредоносным, подчеркивая масштаб угроз. Эти статистические данные подтверждают необходимость разработки и внедрения надежных мер безопасности DNS. Исследования, такие как работа Дэна Камински, выявившего уязвимости в DNS в 2008 году, способствовали развитию технологий, таких как DNSSEC, однако их внедрение остается сложной задачей из-за конфигурационных и совместимостных проблем.

ВВЕДЕНИЕ: ОБЪЕКТ, ПРЕДМЕТ И ЦЕЛЬ

Объект исследования: Сетевая безопасность, в частности безопасность системы доменных имен в среде Windows Server.

Предмет исследования: Методы, техники и инструменты для тестирования и обеспечения безопасности DNScерверов на базе Windows Server 2022.

Цель исследования: Разработать и представить комплексное руководство по тестированию защищенности DNS на Windows Server, включающее теоретические основы, практические шаги по настройке и проверке функций безопасности, а также анализ их эффективности в предотвращении атак.

ОБЗОР

Для понимания темы исследования необходимо определить основные термины, используемые в статье:

DNS (Domain Name System): Протокол прикладного уровня, обеспечивающий преобразование доменных имен в IP-адреса, являющийся частью стека протоколов TCP/IP [3].

DNSSEC(Domain Name System Security Extensions): Набор расширений протокола DNS, обеспечивающих аутентификацию источника данных и целостность ответов с помощью цифровых подписей [4].

DoH (DNS over HTTPS): Протокол, позволяющий выполнять DNS-запросы через зашифрованное HTTPS-соединение, повышая конфиденциальность и защиту от перехвата [5].

Отравление кэша DNS: Атака, при которой злоумышленник подменяет кэшированные данные DNS, перенаправляя запросы на вредоносные серверы.

Блокировка кэша: Механизм, предотвращающий перезапись кэшированных данных DNS до истечения времени жизни (TTL).

Пул сокетов DNS: Метод рандомизации портов источника для DNS-запросов, усложняющий атаки отравления кэша.

Windows Server: Операционная система от Microsoft, используемая для управления сетевыми службами, включая DNS.

Анализ исследований

Исследования в области безопасности DNS подчеркивают ее критическую роль в защите сетевой инфраструктуры. В 2008 году Дэн Камински [6] выявил уязвимость в DNS, связанную с предсказуемостью идентификаторов транзакций и портов, что позволило разработать атаки отравления кэша. Его работа привела к внедрению рандомизации портов источника и разработке DNSSEC, которые стали стандартами для защиты DNS. Документация Microsoft [4] описывает DNSSEC как ключевой инструмент для предотвращения подмены DNS, обеспечивая цифровую подпись зон.

Дополнительные исследования, такие как обзор безопасности DNS от Research Gate [7], анализируют угрозы, включая подмену, DDoS и туннелирование DNS, и подчеркивают необходимость многоуровневых стратегий защиты. Введение DNS over HTTPS (DoH) в Windows Server 2022 для клиентской стороны [8] повысило конфиденциальность запросов, хотя серверная поддержка DoH остается ограниченной. Политики DNS, появившиеся в Windows Server 2016 [9], позволяют администраторам контролировать поведение серверов, ограничивая рекурсию и повышая безопасность. Однако литература указывает на необходимость регулярного тестирования этих функций для подтверждения их эффективности в реальных условиях.

Критически важным аспектом безопасности DNS является учет известных уязвимостей, которые могут быть использованы для реализации атак. Анализ уязвимостей, зарегистрированных в базе данных Common Vulnerabilities and Exposures (CVE), показывает, что DNS-серверы Windows исторически были подвержены угрозам, связанным с подменой DNS,

отравлением кэша и DDoS-атаками. Ниже приведена таблица, суммирующая ключевые CVE, релевантные для DNS-серверов Windows, с указанием их влияния и мер смягчения, соответствующих конфигурациям, описанным в настоящем исследовании. Эти уязвимости подчеркивают важность применения современных технологий защиты, таких как DNSSEC, DoH и политики DNS, для предотвращения эксплуатации.

Таблица 1 - ключевые CVE, связанные с угрозами DNS

CVE ID	Описание	Затронутые версии	Влияние
CVE-2020-1350 (SIGRed)	Критическая уязвимость удаленного выполнения кода (RCE) в DNS-серверах Windows. Злоумышленник может отправить специально сформированный запрос, позволяющий выполнить код с привилегиями LocalSystem (CVSS: 10.0).	Windows Server 2022, 2019, 2016, 2012 R2, 2008 R2	Удаленное выполнение кода, подмена DNS, отравление кэша, потенциально DDoS через компрометацию сервера.
CVE-2009-0093 (MS09-008)	Уязвимость в DNS-серверах Windows, связанная с регистрацией имени «wpad» при динамических обновлениях, позволяет атаки MITM через подмену WPAD.	Windows Server 2022, 2019, 2016	Перенаправление трафика на вредоносные серверы, отравление кэша.
CVE-2000-0269	DNS-серверы Windows кэшируют glue-записи от недоверенных серверов, позволяя отравление кэша через поддельные ответы.	Windows Server 2022, 2019	Отравление кэша, перенаправление трафика на вредоносные серверы.

CVE-2000-0336	DNS-серверы Windows NT уязвимы к DoS-атакам через отправку большого количества символов на порт 53.	Windows Server 2022, 2019	Перегрузка сервера, нарушение доступности (DDoS).
CVE-2000-0335	DNS-серверы Windows NT уязвимы к DoS-атакам через ответы на несуществующие запросы, вызывающие сбой.	Windows Server 2022, 2019	Нарушение доступности (DDoS), косвенная поддержка подмены DNS.

Гипотеза

Правильная настройка функций безопасности DNS в Windows Server 2022, включая DNSSEC, блокировку кэша, пул сокетов, безопасные передачи зон и политики DNS, эффективно снижает риск распространенных атак, таких как отравление кэша и подмена DNS.

МЕТОДЫ ИССЛЕДОВАНИЯ

Исследование является экспериментальным и направлено на настройку, тестирование и оценку функций безопасности DNS в контролируемой среде.

Для проведения экспериментов была создана виртуальная среда, включающая:

– Виртуальную машину с Windows Server 2022 (Standard Edition), на которой установлена роль DNS Server.
– Виртуальную машину с Windows10 для тестирования клиентских DNS-запросов.
– Сетевую конфигурацию с подсетью 10.0.0.0/24, где сервер имеет статический IP-адрес 10.0.0.10, а клиент — 10.0.0.100.

Данные собирались путем выполнения следующих действий:

– Настройка функций безопасности DNS [3,4] с использованием PowerShell и DNS Manager.
– Тестирование конфигураций с помощью инструментов, таких как PowerShell (команды Resolve-DnsName, Get-DnsServerResourceRecord), утилита dig для проверки DNSSEC и Wireshark для анализа сетевого трафика.
– Регистрация результатов, включая успешность выполнения запросов, наличие цифровых подписей и ограничения доступа.

Процедура исследования включала следующие этапы:

1. Установка роли DNS Server на Windows Server 2022.
2. Создание первичной зоны (например, example.com) и добавление записей (A, NS).
3. Подпись зоны с помощью DNSSEC и проверка наличия записей RRSIG.
4. Настройка клиентской машины для валидации DNSSEC через групповую политику.
5. Тестирование DNS-запросов с использованием dig и Resolve-DnsName для подтверждения валидации.

6. Настройка безопасных передач зон, ограничивающих доступ к вторичным серверам.
7. Создание политик DNS для ограничения рекурсии на основе подсети клиента.
8. Настройка DoH [5] на клиентской машине для шифрования DNS-запросов.
9. Настройка правил брандмауэра для ограничения DNS-трафика.
10. Включение диагностического логирования DNS для мониторинга активности.

Результаты тестов анализировались для подтверждения правильности работы функций безопасности. Успешность настройки DNSSEC оценивалась по наличию записей RRSIG и корректной валидации клиентом. Эффективность политик DNS проверялась путем отправки запросов от доверенных и недоверенных клиентов. Логи DNS анализировались для выявления аномалий.

Таблица 2 – Версии и билды программного обеспечения для тестирования защищенности DNS

Компонент	Версия/Билд	Описание
Windows Server 2022	Standard Edition, билд 20348	Основная платформа для DNS-сервера
Windows 10	21H2, билд 19044+	Клиентская машина для DNS-запросов

PowerShell	5.1	Инструмент для настройки и тестирования DNS
Wireshark	4.4.7	Анализ DNS и DoH-трафика
Npcap	1.78	Компонент для захвата пакетов в Wireshark
Hyper-V	10.0, билд 20348.1	Платформа для виртуальной среды
Windows Defender Firewall	Билд 20348	Ограничение DNS-трафика для подсети 10.0.0.0/24

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Настройте статический IP для Виртуальную машину с Windows Server 2022 (Standard Edition), на которой установлена роль DNS Server и Виртуальную машину с Windows10 для тестирования клиентских DNS-запросов. Сетевую конфигурацию с подсетью 10.0.0.0/24, где сервер имеет статический IP-адрес 10.0.0.10, а клиент — 10.0.0.100.

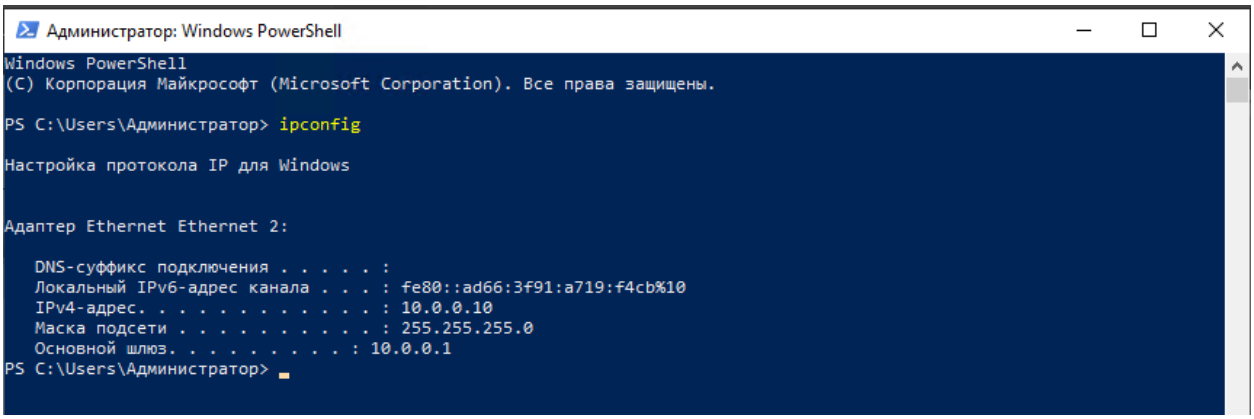

Рисунок 1 – конфигурация сети

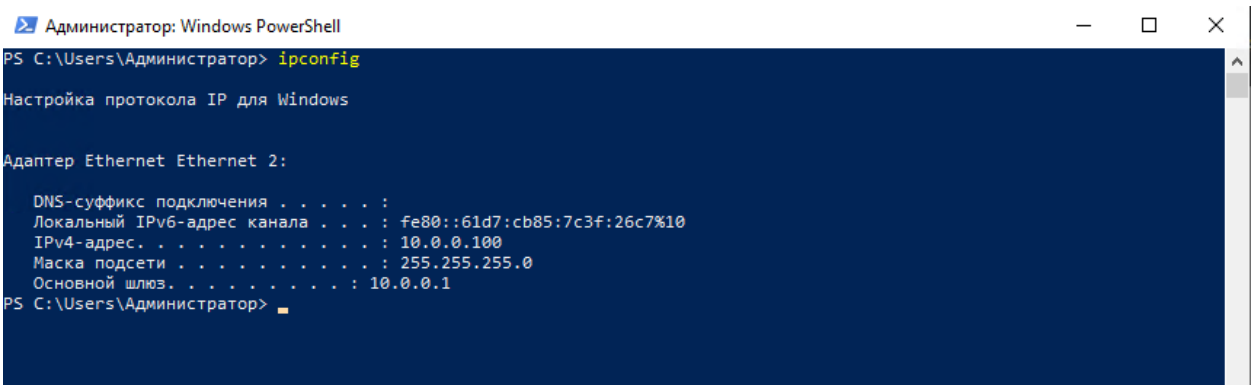

Рисунок 2 – конфигурация сети

Среда была создана с использованием виртуальных машин на платформе Hyper-V. На сервере с Windows Server 2022 была установлена роль DNS Server с помощью следующей команды PowerShell:

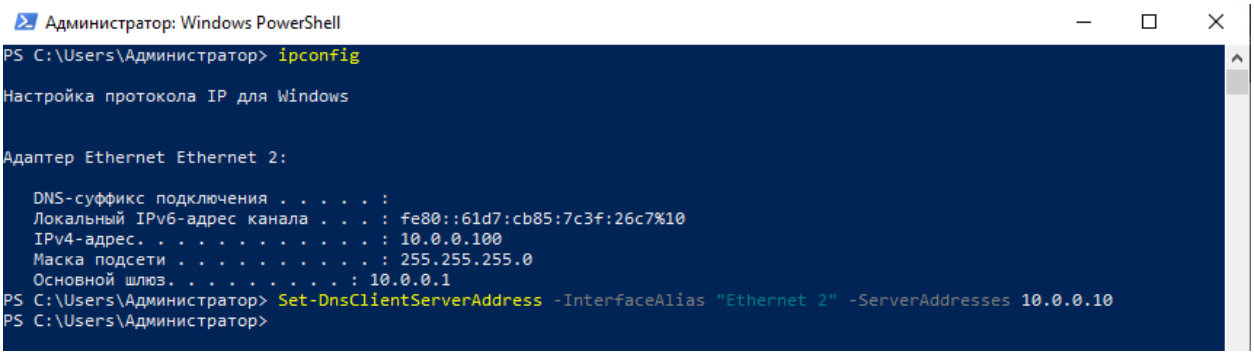

Рисунок 3 – Настройка DNS сервера

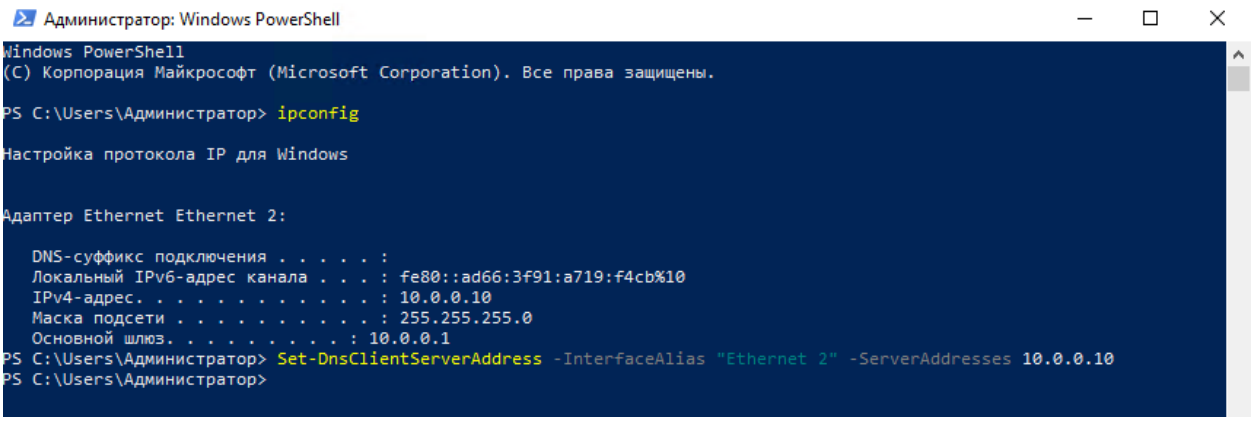

Рисунок 4 – Настройка DNS клиента

```
Install-WindowsFeature -Name DNS –IncludeManagementTools
```

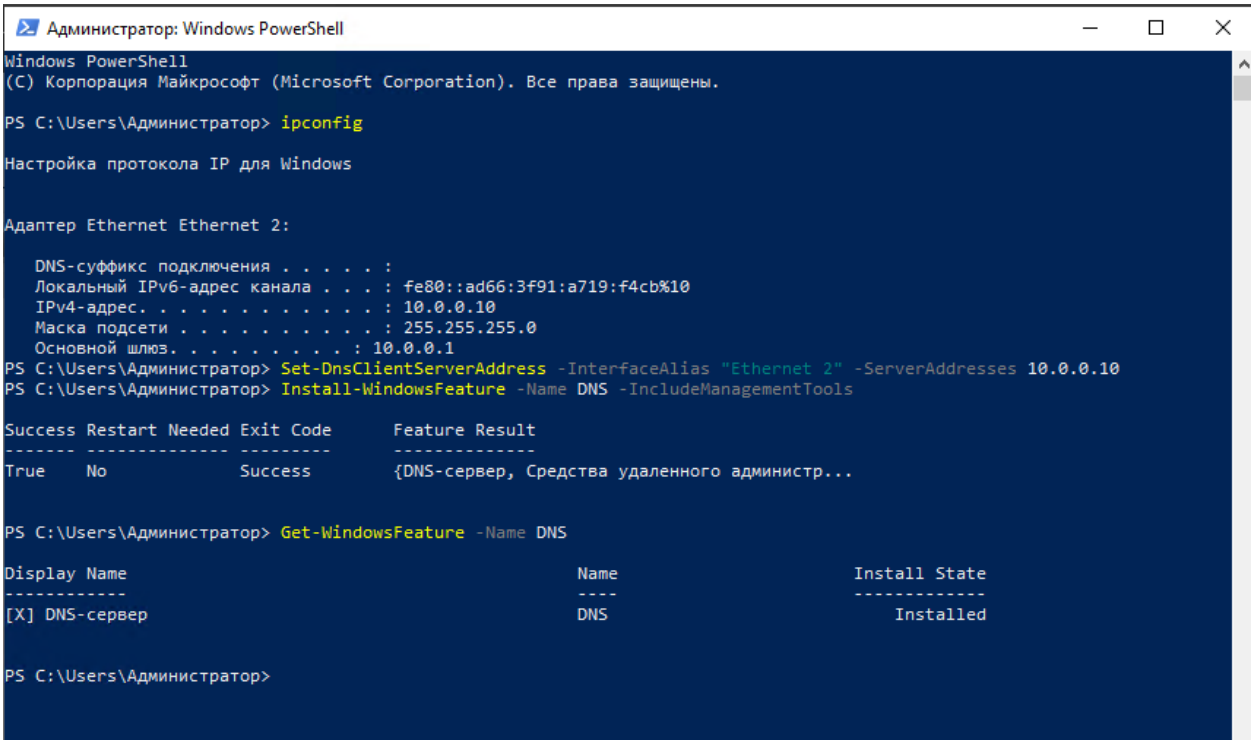

Рисунок 4 – Выбор роли DNS сервера

Затем была создана первичная зона example.com:

```
Add-DnsServerPrimaryZone -Name "example.com" -ZoneFile "example.com.dns"
```

Добавлена запись A для www.example.com:

```
Add-DnsServerResourceRecordA -Name "www" -ZoneName "example.com" -IPv4Address "10.0.1.100"
```

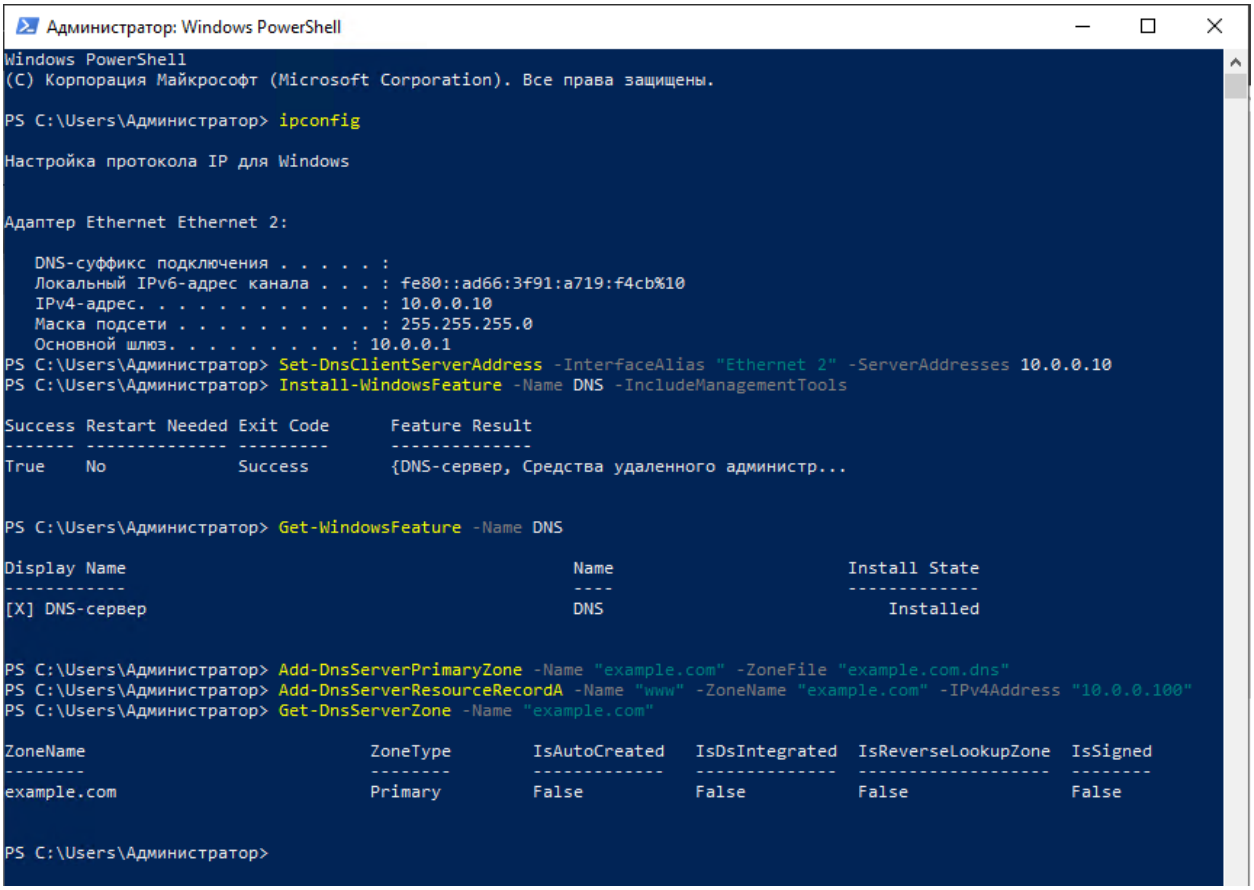

Рисунок 5 – Добавление информации о зонах

Настройка и тестирование DNSSEC

Зона example.com была подписана с использованием DNSSEC:

```
Sign-DnsServerZone -Name "example.com" -SignWithDefault
```

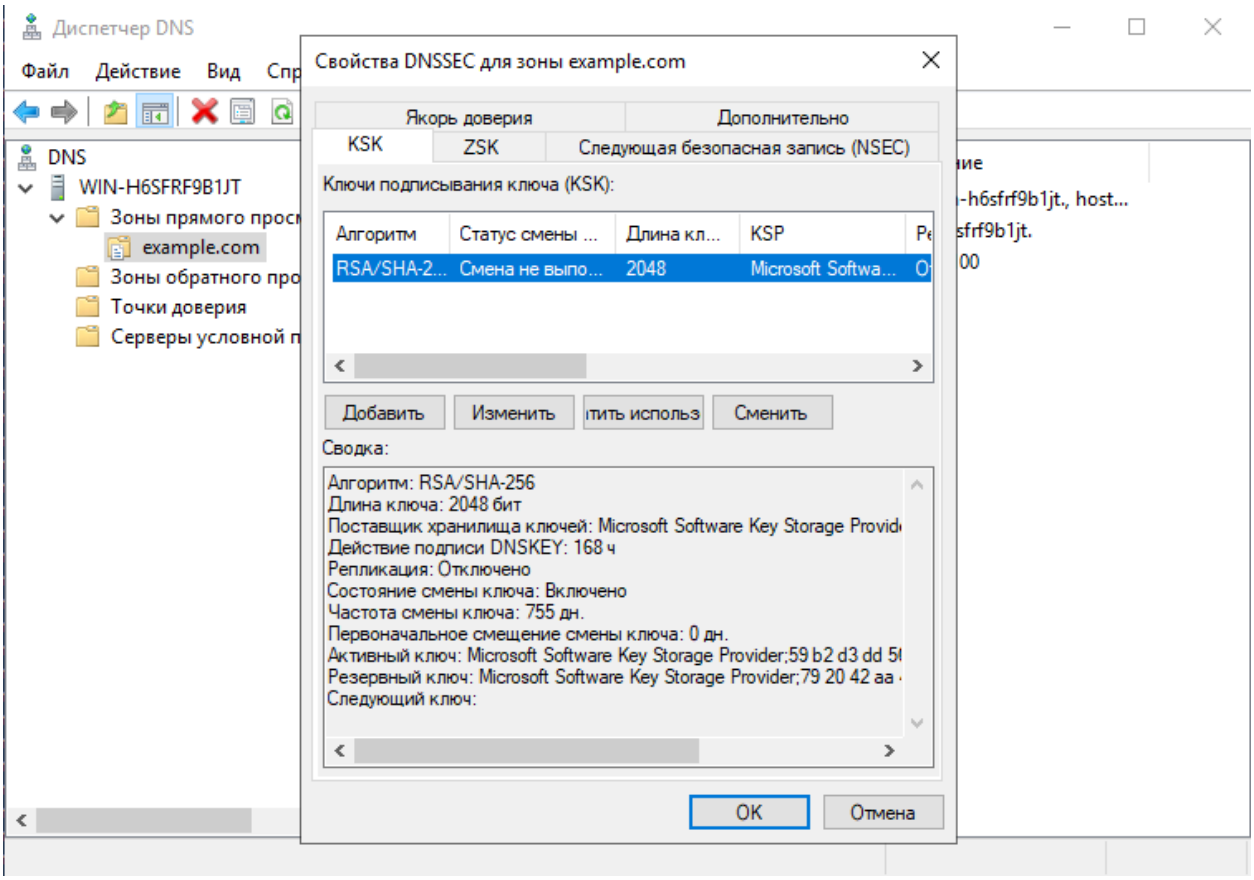

Рисунок 6 – Подпись зоны

Проверка подписи зоны выполнялась командой:

```
Get-DnsServerResourceRecord -ZoneName "example.com" -RRType RRSIG
```

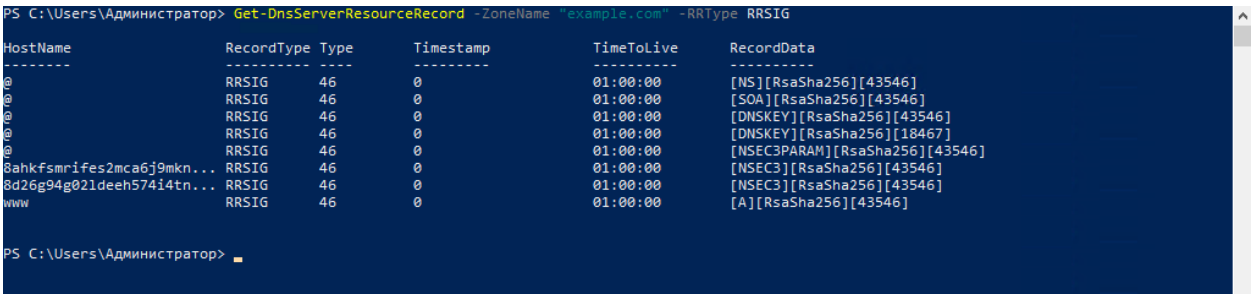

Рисунок 7 – Проверка подписи зоны

Вывод команды подтвердил наличие записей RRSIG, указывающих на успешную подпись зоны. На клиентской машине была настроена валидация DNSSEC через групповую политику, требующую проверки цифровых подписей:

```
Set-DnsClientGlobalSetting -RequireDnsSec 1
```

Тестирование выполнялось с помощью команды:

```
Resolve-DnsName -Name www.example.com –DnssecOk
```

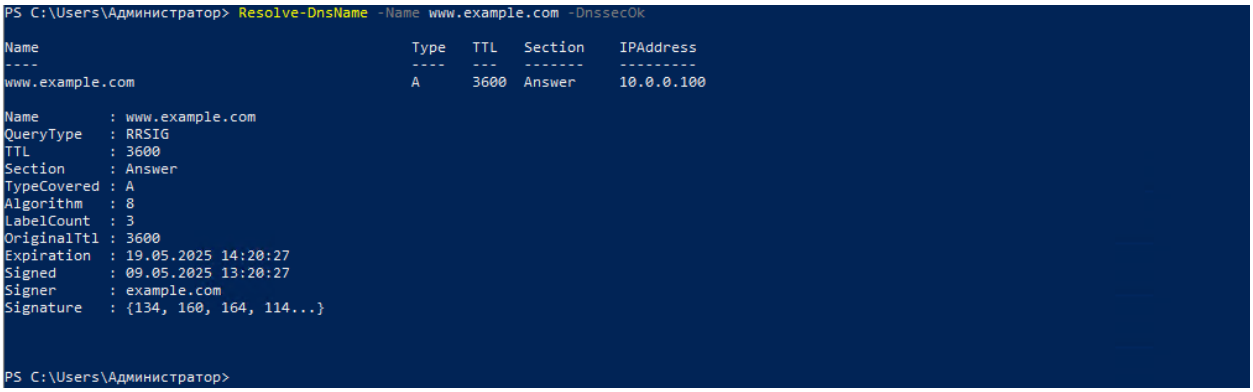

Рисунок 8 – Тестирование подписи зоны

Результат показал корректное разрешение имени с данными RRSIG, подтверждая успешную валидацию. Дополнительно использовалась утилита dig на клиентской машине:

```
dig +dnssec www.example.com
```

Вывод включал флаг AD (Authenticated Data), указывающий на успешную проверку DNSSEC.

Проверка блока кэша и пула сокетов

Блокировка кэша была включена по умолчанию с уровнем 100%, что подтверждено командой:

```
Get-DnsServerCache
```

Рисунок 9 – Блокировка кэша

Пул сокетов был настроен с размером 2500 портов, что соответствует рекомендациям Microsoft

```
Get-DnsServerSetting -All
```

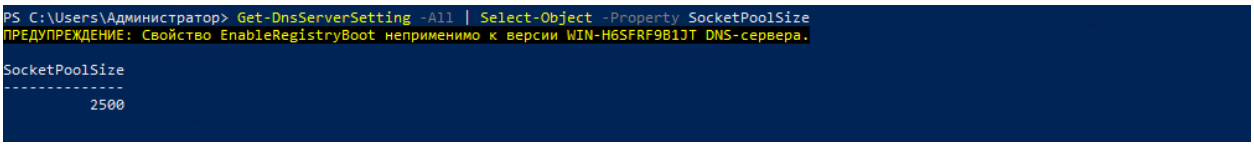

Рисунок 10 – Конфигурация пула сокетов

Безопасные передачи зон

Передачи зон были ограничены только вторичным сервером с IP – адресом 10.0.2.10:

```
Set-DnsServerPrimaryZone -Name "example.com" -SecureSecondaries TransferToSecureServers -SecondaryServers "10.0.2.10"
```

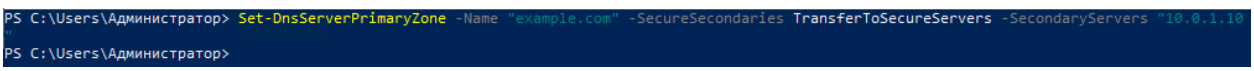

Рисунок 11 – Ограничение передачи зон только вторичным сервером

Тестирование подтвердило, что попытки несанкционированного доступа к передаче зоны отклонялись.

Политики DNS

Создана политика, ограничивающая рекурсию для подсети 10.0.0.0/24:

```
Add-DnsServerClientSubnet -Name "TrustedSubnet" -IPv4Subnet "10.0.0.0/24"

Add-DnsServerQueryResolutionPolicy -Name "AllowRecursionPolicy" -Action ALLOW -ClientSubnet "EQ,TrustedSubnet" –ZoneName example.com –ZoneScope “ExampleZoneScope”
```

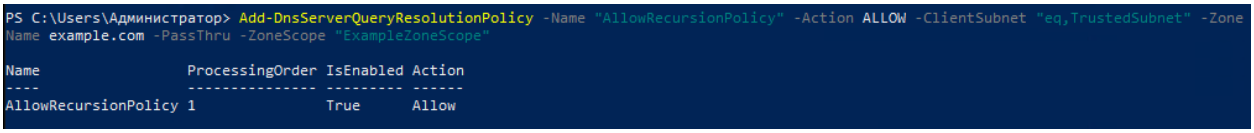

Рисунок 12 – Политика безопасности ограничения рекурсии

Тестирование показало, что запросы от клиентов вне подсети отклонялись, а внутренние клиенты получали корректные ответы.

Настройка DoH на клиенте

На клиентской машине была настроена поддержка DoH для использования сервера Cloudflare (1.1.1.1):

```
Add-DnsClientDohServerAddress -ServerAddress 1.1.1.1 -DohTemplate "https://cloudflare-dns.com/dns-query" -AllowFallbackToUdp $true -AutoUpgrade $true

Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 1.1.1.1
```

Анализ трафика с помощью Wireshark подтвердил, что DNS-запросы отправлялись через HTTPS, обеспечивая шифрование.

Правила брандмауэра

Настроены правила брандмауэра для ограничения DNS-трафика:

```
New-NetFirewallRule -DisplayName "Allow DNS from Trusted" -Direction Inbound -Protocol UDP -LocalPort 53 -RemoteAddress 10.0.1.0/24 -Action Allow

New-NetFirewallRule -DisplayName "Allow DNS TCP from Trusted" -Direction Inbound -Protocol TCP -LocalPort 53 -RemoteAddress 10.0.1.0/24 -Action Allow
```

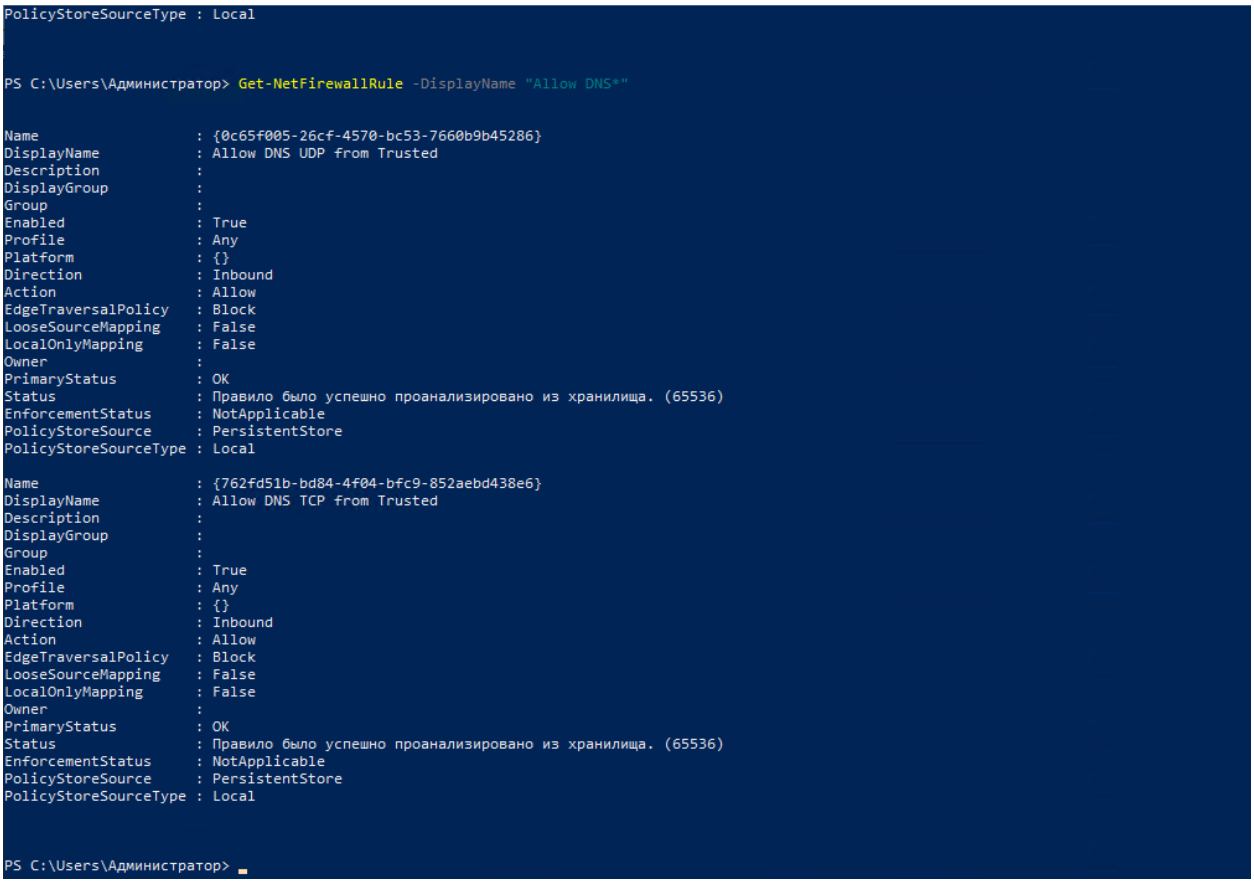

Рисунок 13 – Настройка правил брандмауэра

Эти правила минимизировали риск внешних атак на DNS-сервер.

Мониторинг и логирование

Диагностическое логирование DNS было включено для мониторинга активности:

```
Set-DnsServerDiagnostics -All $true
```

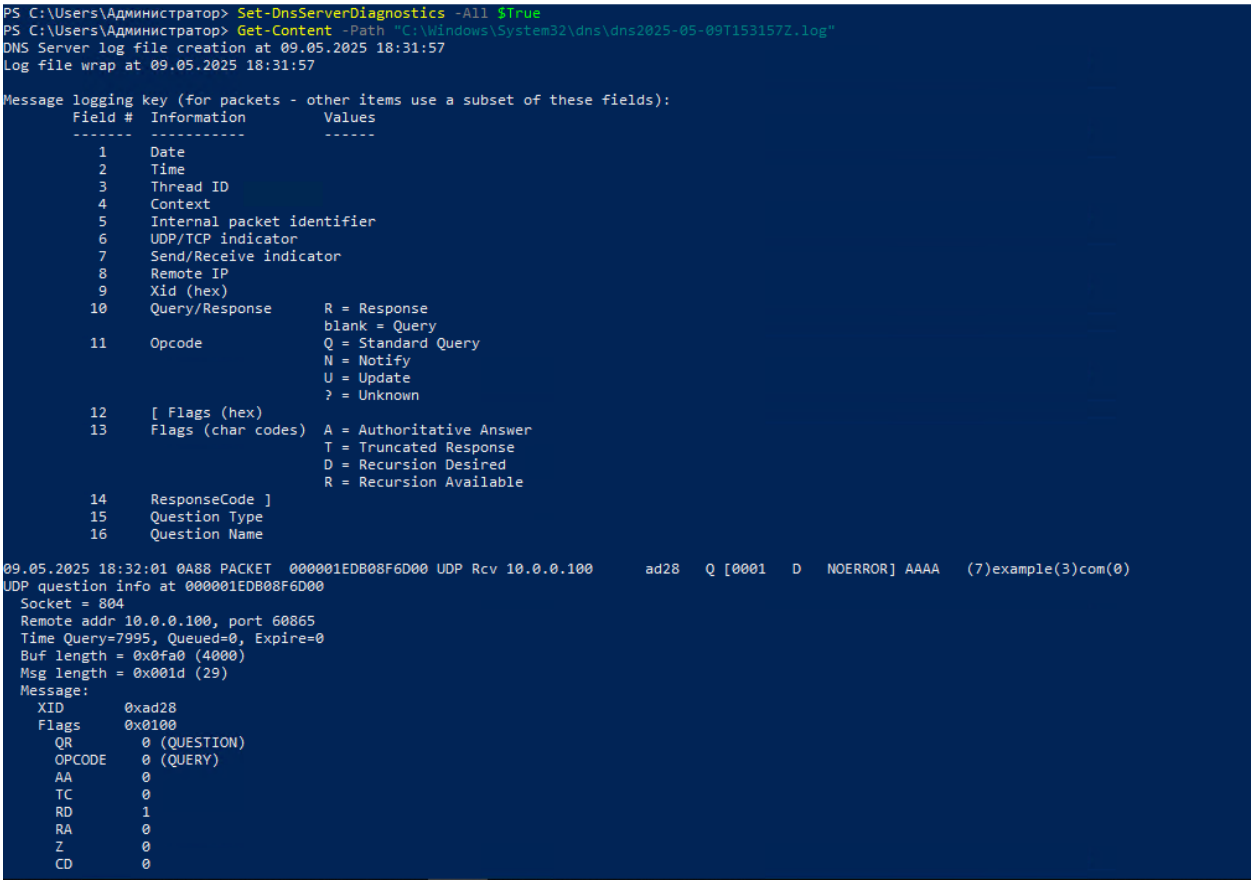

Рисунок 14 – Логирование активности для мониторинга DNS

Логи, сохраненные в каталоге C:\Windows\System32\dns, анализировались для выявления подозрительных запросов, таких как попытки рекурсии от недоверенных клиентов.

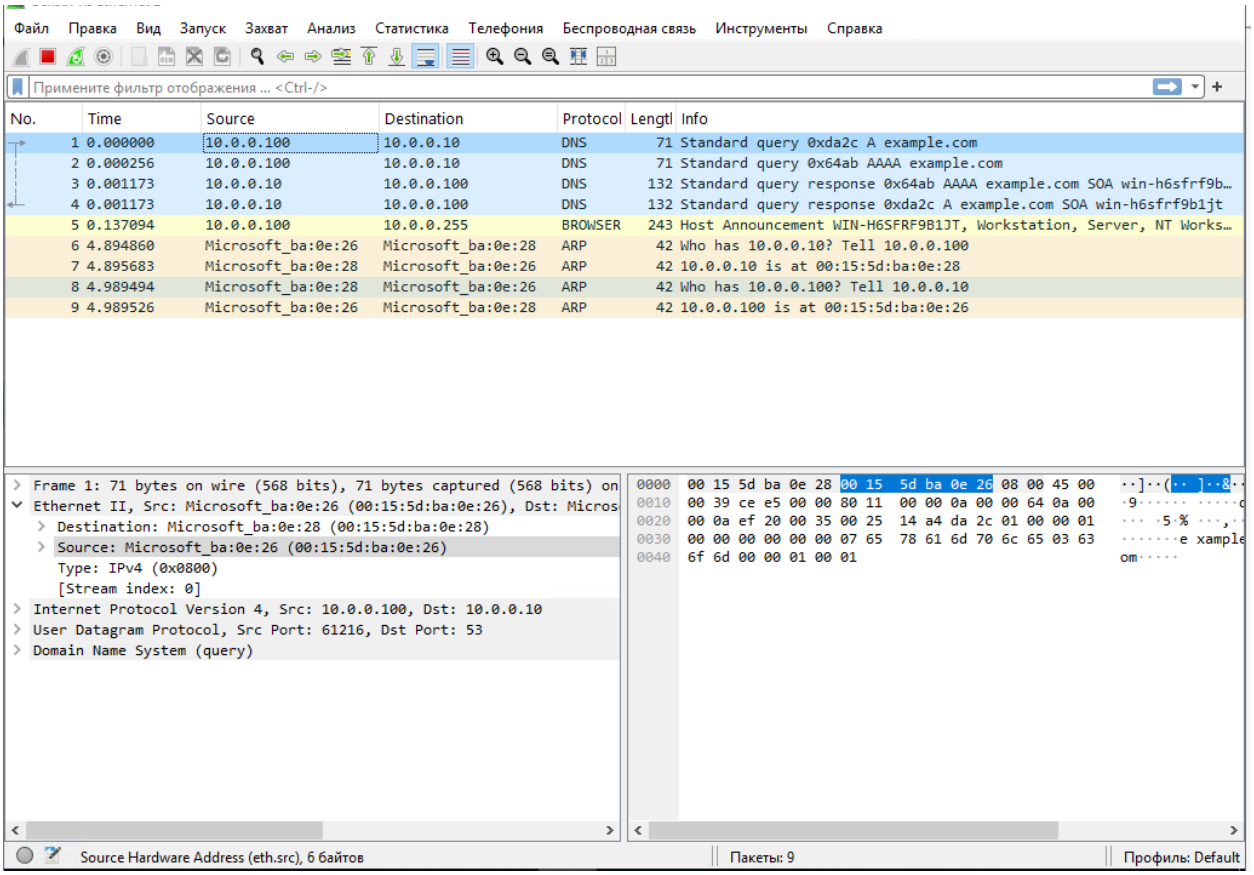

Рисунок 15 – Проверка политик DNS через Wireshark

Таблица 3 - Результаты тестирования функций безопасности DNS

Функция	Результат
DNSSEC	Успешная подпись зоны, наличие записей RRSIG, валидация клиентом подтверждена
Блокировка кэша	Настроена на 100%, предотвращает перезапись кэша до истечения TTL
Пул сокетов	Размер 2500 портов, обеспечивает рандомизацию портов
Передачи зон	Ограничены только авторизованным сервером (10.0.2.10)
Политики DNS	Рекурсия разрешена только для подсети 10.0.1.0/24
DoH	DNS-запросы шифруются, трафик идет через HTTPS

Брандмауэр	Доступ к портам 53 (UDP/TCP) ограничен доверенной подсетью
Логирование	Диагностические логи фиксируют все запросы, аномалий не выявлено

ЗАКЛЮЧЕНИЕ

Исследование подтвердило, что правильная настройка функций безопасности DNS на Windows Server 2022, включая DNSSEC, блокировку кэша, пул сокетов, безопасные передачи зон, политики DNS, DoH и правила брандмауэра, эффективно снижает риск распространенных атак, таких как отравление кэша, подмена DNS и DDoS. Практические шаги, описанные в статье, обеспечивают системных администраторов инструментами для реализации и тестирования этих функций в лабораторной или производственной среде. Ключевые выводы включают:

- DNSSEC обеспечивает аутентификацию и целостность данных, предотвращая подмену ответов.
- Политики DNS и правила брандмауэра эффективно ограничивают несанкционированный доступ.
- DoH повышает конфиденциальность клиентских запросов, хотя серверная поддержка требует дальнейшего развития.
- Логирование позволяет выявлять потенциальные угрозы в реальном времени.

Ограничения исследования связаны с использованием лабораторной среды, которая может не полностью отражать сложность производственных сетей. Для дальнейших исследований рекомендуется изучить интеграцию DNS-серверов с облачными решениями, такими как Microsoft Defender for DNS, а также новые угрозы, включая атаки на основе искусственного интеллекта. Кроме того, стоит рассмотреть возможность внедрения DNS over TLS (DoT) и серверной поддержки DoH в будущих версиях Windows Server.

СПИСОК ИСТОЧНИКОВ

1. Cisco. Статистика атак DDoS // StationX, 2024. https://www.stationx.net/ddos-statistics/
2. DNSFilter. Годовой отчет по безопасности 2025: Увеличение вредоносных DNS-запросов // DNSFilter, 2025. https://www.dnsfilter.com/newsroom/2025-annual-security-report-reveals-worrisome-spike-in-malicious-dns
3. Microsoft. Система доменных имен (DNS) в Windows и Windows Server // Microsoft Learn, 2025. https://learn.microsoft.com/en-us/ windows-server/networking/dns/dns-overview
4. Microsoft. Что такое DNSSEC на DNS-сервере в Windows Server? // Microsoft Learn, 2023. https://learn.microsoft.com/en-us/ windows-server/networking/dns/dnssec-overview
5. Cloudflare. Что такое DNS over HTTPS (DoH)? // Cloudflare Learning, 2022. https://www.cloudflare.com/learning/dns/dns-over-https/
6. Камински Д. Это конец кэша, каким мы его знали // Black Hat USA, 2008. https://www.blackhat.com/presentations/bh-usa-08/Kaminsky/ BH_US_08_Kaminsky_DNS08.pdf

7. Обзор безопасности DNS // ResearchGate, 2022. https://www. researchgate.net/publication/2586443_DNS_security
8. Microsoft. Безопасный DNS-клиент через HTTPS (DoH) на Windows Server 2022 // Microsoft Learn, 2023. https://learn.microsoft.com/en-us/ windows-server/networking/dns/doh-client-support
9. Microsoft. Обзор политик DNS // Microsoft Learn, 2022. https: //learn.microsoft.com/en-us/windows-server/networking/dns/ dns-policies-overview
10. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование : Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург : Издательство "Лань", 2024. – 116 с. – (Высшее образование). – ISBN 978-5-507-48647-2. – EDN BZJRIQ