УДК 004.056.5

Тимошенко Дмитрий Максимович - Студент Кафедры квантовых информационных технологий, практической и прикладной информатики Института информационных технологий МИРЭА – Российского технологического университета.

Лавровская Вера Григорьевна - ассистент кафедры телекоммуникаций ИРИ (Институт Радиоэлектроники и информатики) МИРЭА – Российского технологического университета.

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОТОКОЛА DNS И МЕТОДЫ ЗАЩИТЫ ОТ DNS-SPOOFING В КОРПОРАТИВНЫХ СЕТЯХ

Аннотация

В данной статье рассматриваются фундаментальные принципы работы системы доменных имен (DNS), обеспечивающей базовую маршрутизацию и разрешение имен в современных корпоративных сетях. Проведен глубокий анализ архитектуры протокола и его критических уязвимостей, обусловленных отсутствием криптографической аутентификации в базовой спецификации (RFC 1035) и использованием протокола UDP. Подробно описаны векторы реализации атак, в частности механизм подмены ответов DNS (DNS Cache Poisoning / DNS Spoofing), и их влияние на безопасность корпоративного периметра, включая организацию фишинговых атак и перехват конфиденциального трафика. В статье систематизированы современные методы противодействия данным угрозам, уделено внимание

внедрению расширений безопасности DNSSEC, а также протоколов шифрования DNS over HTTPS (DoH) и DNS over TLS (DoT).

Annotation

This article examines the fundamental principles of the Domain Name System (DNS), which provides basic routing and name resolution in modern corporate networks. A deep analysis of the protocol's architecture and its critical vulnerabilities, caused by the lack of cryptographic authentication in the basic specification (RFC 1035) and the use of the UDP protocol, is carried out. The vectors of implementing attacks are described in detail, in particular the DNS Cache Poisoning / DNS Spoofing mechanism, and their impact on the security of the corporate perimeter, including the organization of phishing attacks and interception of confidential traffic. The article systematizes modern methods of countering these threats, paying attention to the implementation of DNSSEC security extensions, as well as DNS over HTTPS (DoH) and DNS over TLS (DoT) encryption protocols.

Ключевые слова: DNS, DNS-спуфинг, информационная безопасность, корпоративные вычислительные сети, отравление кэша, DNSSEC, кибератаки.

Keywords: DNS, DNS spoofing, information security, corporate computing networks, cache poisoning, DNSSEC, cyberattacks.

1. Введение

В эпоху глобальной цифровизации корпоративных процессов и активной миграции бизнес-инфраструктуры в облачные среды вопросы обеспечения комплексной информационной безопасности (ИБ) приобретают критическое значение. Традиционно основной фокус внимания ИБ-специалистов при

проектировании защищенных сетей сосредоточен на внедрении межсетевых экранов нового поколения (NGFW), систем предотвращения вторжений (IPS) и защите прикладного уровня модели OSI. Однако, как показывает практика проведения аудитов безопасности, инфраструктурные сетевые протоколы зачастую остаются наиболее уязвимым звеном.

Одним из таких критически важных компонентов является система доменных имен (Domain Name System — DNS). Спецификации базового протокола DNS были утверждены в 1987 году документами RFC 1034 и RFC 1035. DNS выполняет роль фундаментальной системы маршрутизации корпоративных сетей, транслируя удобочитаемые доменные имена в IP-адреса.

Архитектура базового протокола DNS разрабатывалась на ранних этапах развития сетей в парадигме абсолютного доверия к участникам информационного обмена. Протокол использует транспортный протокол UDP без проверки состояния соединения (Stateless) и в своей изначальной реализации полностью лишен встроенных механизмов криптографической аутентификации. Этот архитектурный недостаток формирует обширную поверхность для атак, направленных на подмену ответов (DNS Spoofing) и отравление кэша DNS-серверов (Cache Poisoning).

Объектом данного исследования выступает информационная безопасность корпоративных вычислительных сетей, построенных с использованием инфраструктуры DNS.

Предметом исследования являются архитектурные уязвимости протокола DNS и современные программно-аппаратные методы противодействия подмене доменных записей.

Цель работы заключается в проведении комплексного анализа механизмов эксплуатации уязвимостей протокола DNS и систематизации эффективных методов защиты сетевой инфраструктуры от атак типа «человек посередине» (MITM) и фишинга, основанных на манипуляции DNS-трафиком.

Для достижения поставленной цели в рамках исследования решаются следующие задачи:

1. Выполнить теоретический анализ принципов функционирования протокола DNS и выявить его ключевые структурные недостатки (использование UDP, отсутствие верификации).
2. Подробно описать механизм реализации атаки DNS-спуфинг и отравления кэша, оценив потенциальный ущерб для предприятия.
3. Проанализировать технологии криптографической защиты зоны — DNSSEC, а также специфику их внедрения.
4. Рассмотреть перспективы защиты клиентского трафика в корпоративной среде в контексте использования протоколов DNS over HTTPS (DoH) и DNS over TLS (DoT).

2. Теоретический анализ протокола DNS и механика реализации атак

2.1. Принципы штатного функционирования системы DNS

Система доменных имен имеет строгую распределенную иерархическую структуру, состоящую из корневых серверов (Root servers), серверов доменов

верхнего уровня (TLD — Top-Level Domain) и авторитативных серверов, отвечающих за конкретные делегированные зоны.

Процесс разрешения доменного имени в IP-адрес для конечного пользователя инициируется через локальный DNS-сервер (рекурсивный резолвер), обычно предоставляемый интернет-провайдером или развернутый внутри корпоративного периметра. Штатный алгоритм включает следующие этапы:

1. Клиентский процесс (stub-resolver) отправляет рекурсивный запрос локальному DNS-серверу с целью узнать IP-адрес целевого узла (например, gw.example.com).
2. При отсутствии актуальной записи в кэше, локальный сервер инициирует итеративный процесс поиска. Сначала он опрашивает один из 13 корневых серверов, который возвращает ссылку на TLD-сервер (в данном случае зоны .com).
3. Затем резолвер обращается к TLD-серверу, получая от него адрес авторитативного сервера, обслуживающего зону example.com.
4. На финальном этапе резолвер запрашивает авторитативный сервер, получает корректную ресурсную запись (A или AAAA), сохраняет связку «Домен – IP-адрес» в свой локальный кэш на время, определяемое параметром TTL (Time to Live), и транслирует ответ клиенту.

Для обеспечения минимальной задержки (latency) и высокой пропускной способности, традиционный DNS-трафик передается в открытом виде с использованием транспортного протокола UDP по порту 53.

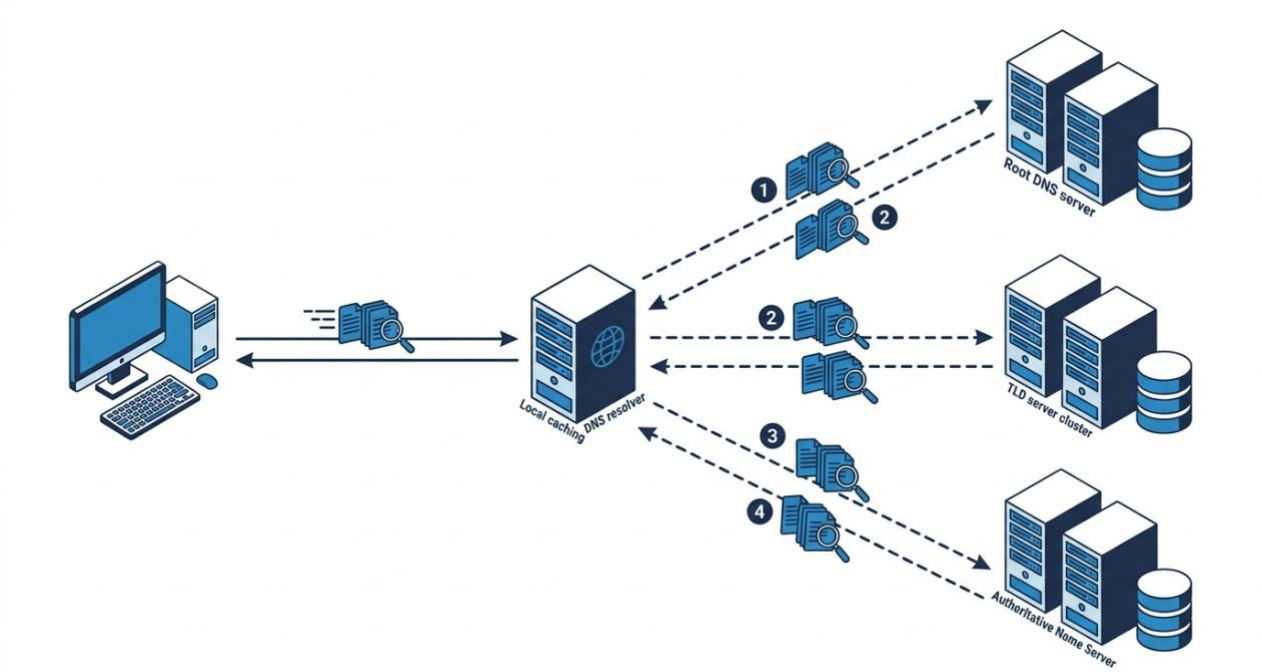

Рисунок 1 – Иерархическая схема итеративного процесса разрешения доменного имени

2.2. Архитектурные уязвимости и структурные недостатки

Критическая уязвимость базового протокола DNS кроется в исторически сложившейся модели доверия. Согласно RFC 1035, рекурсивный резолвер признает входящий DNS-ответ подлинным при совпадении всего трех базовых параметров:

- Идентичность IP-адреса и порта отправителя ответа с параметрами авторитативного сервера, которому был маршрутизирован запрос.
- Совпадение имени запрашиваемого домена и класса ресурсной записи.
- Совпадение 16-битного идентификатора транзакции (Transaction ID / TXID).

Отсутствие криптографической цифровой подписи (в базовой версии без расширения DNSSEC) и использование протокола UDP, не отслеживающего состояние соединения (Stateless), позволяют злоумышленнику осуществлять IP-спуфинг. Атакующему достаточно сгенерировать фальшивый UDP-пакет, подделав IP-адрес источника, и угадать верный TXID. Поскольку размерность поля TXID ограничена 16 битами, существует лишь 65 536 уникальных комбинаций, что делает атаку методом полного перебора (Brute-force) математически реализуемой в рамках узкого временного окна.

2.3. Вектор атаки: механика DNS-спуфинга и уязвимость Каминского

Эксплуатация указанных недостатков приводит к реализации атаки «отравление кэша» (DNS Cache Poisoning). Фундаментальный прорыв в повышении эффективности данного вектора совершил исследователь Дэн Каминский в 2008 году. Его метод позволил обойти ограничения, накладываемые длительным временем жизни записей (TTL), и сделал отравление кэша высокоэффективным инструментом компрометации корпоративных сетей.

Механика атаки Каминского строится на следующих шагах:

1. Злоумышленник направляет целевому рекурсивному серверу корпоративной сети запрос на разрешение заведомо несуществующего, случайно сгенерированного поддомена (например, x8f9q.target-bank.com).
2. Поскольку данной записи гарантированно нет в кэше, резолвер вынужден сформировать новый запрос к легитимному авторитативному серверу зоны target-bank.com.

3. Не дожидаясь ответа, злоумышленник инициирует массированную флуд-атаку (Flood), отправляя резолверу тысячи поддельных UDP-ответов от имени авторитативного сервера, перебирая возможные значения TXID.
4. Вредоносная полезная нагрузка кроется в структуре фальшивого ответа: помимо фиктивного IP-адреса для несуществующего поддомена, ответ содержит секцию дополнительных данных (Authority Section). В этой секции злоумышленник указывает, что новым NS-сервером для всей родительской зоны target-bank.com отныне является подконтрольный ему IP-адрес.
5. Если атакующий успевает угадать TXID до поступления пакета от легитимного сервера (возникает состояние «гонки» — Race Condition), резолвер кэширует вредоносную NS-запись.

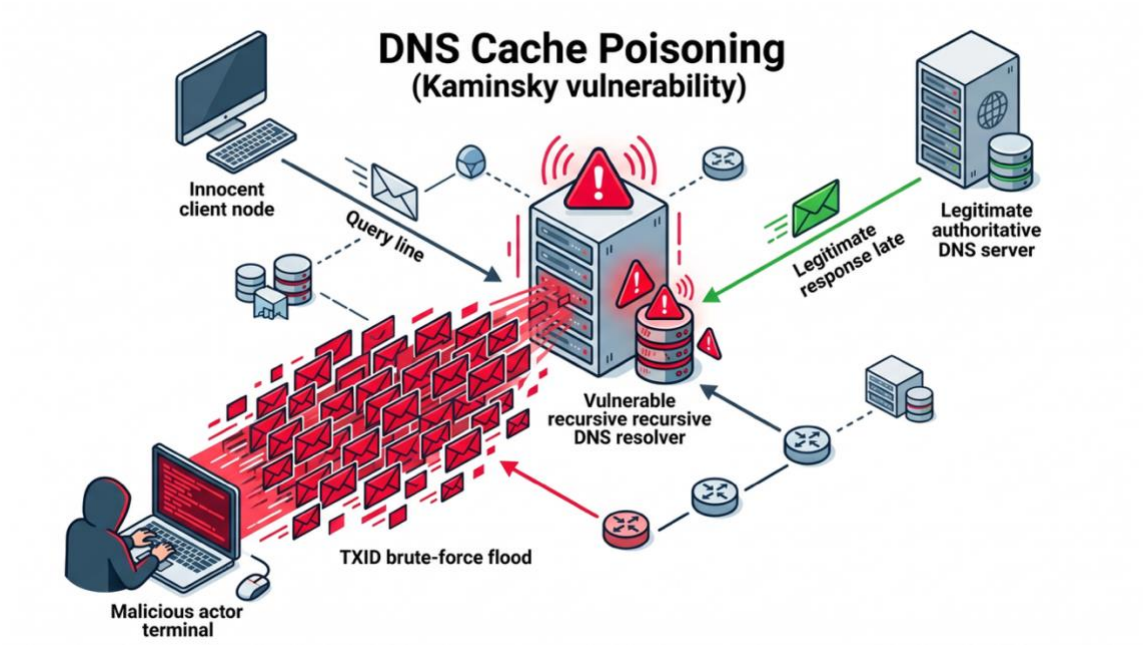

Рисунок 2 – Топология реализации атаки отравления кэша (DNS Cache Poisoning)

В результате успешной эксплуатации уязвимости злоумышленник осуществляет полный перехват управления доменной зоной на уровне кэширующего сервера. Весь последующий легитимный трафик пользователей корпоративной сети, направленный к сервисам скомпрометированного домена, будет маршрутизироваться через теневую инфраструктуру атакующего. Это открывает прямой вектор для реализации масштабных атак типа Man-in-the-Middle (MITM), скрытого корпоративного шпионажа и компрометации учетных записей.

3. Практическая реализация механизмов защиты сетевой инфраструктуры

Обеспечение отказоустойчивости и информационной безопасности корпоративного периметра требует внедрения эшелонированной (многоуровневой) системы защиты инфраструктуры DNS. Поскольку атаки типа DNS-спуфинг эксплуатируют фундаментальные недостатки прикладного уровня модели OSI и Stateless-природу транспортного протокола UDP (порт 53), защитные механизмы должны разворачиваться как на уровне самого DNS-сервера, так и на сетевом периметре с привлечением специализированного коммутационного оборудования и межсетевых экранов. Современный стандарт безопасности предусматривает разделение защиты на два ключевых направления: криптографическая верификация межсерверного взаимодействия и шифрование трафика на участке «последней мили» (от конечного узла до рекурсивного резолвера).

3.1. Криптографическая верификация и применение технологии DNSSEC

Технология DNSSEC (Domain Name System Security Extensions — RFC 4033) разработана для обеспечения аутентичности источника данных и контроля целостности DNS-сообщений. Базовая структура стандартного DNS-ответа состоит из заголовка и четырех последовательных секций: секции запросов (Questions), секции ответов (Answers), секции авторитетных серверов (Authority) и секции дополнительной информации (Additional information). Векторы атак типа Cache Poisoning (включая метод Каминского) нацелены на принудительное внедрение ложных NS-записей именно в секции авторитетных серверов и дополнительных данных.

DNSSEC нейтрализует эту угрозу за счет внедрения асимметричного шифрования (криптографии с открытым ключом). В структуру доменной зоны добавляются новые типы ресурсных записей:

- **RRSIG (Resource Record Signature):** электронная цифровая подпись, формируемая закрытым ключом зоны (ZSK — Zone Signing Key) для каждого набора записей (RRset) в секциях ответа.
- **DNSKEY:** открытый ключ, публикуемый в зоне, который рекурсивный резолвер использует для проверки подписей RRSIG.
- **DS (Delegation Signer):** криптографический хэш открытого ключа дочерней зоны, передаваемый на родительский авторитетный сервер для построения непрерывной цепочки доверия (Chain of Trust) от корневых серверов.

При активации DNSSEC корпоративный рекурсивный резолвер выполняет математическую валидацию цифровой подписи полученного ответа. Если злоумышленник направляет сгенерированный UDP-флуд с поддельным идентификатором транзакции (TXID), резолвер обнаружит отсутствие или

невалидность подписи RRSIG для инъецируемых данных в секции Authority. Такой пакет немедленно отбрасывается, предотвращая отравление кэша.

3.2. Настройка и программно-аппаратная защита корпоративного резолвера

Для демонстрации практической реализации эшелонированной защиты ниже приведен фрагмент конфигурационного файла named.conf для корпоративного DNS-сервера BIND9, где активирована автоматическая валидация DNSSEC, ограничены права на выполнение рекурсивных запросов и настроена рандомизация исходных UDP-портов.

```
// Глобальные параметры безопасности DNS-сервера BIND9
options {
    directory "/var/cache/bind";

    // Ограничение круга клиентов на основе ACL (разрешено только внутренней ЛВС)
    allow-query { 192.168.0.0/16; localhost; };
    allow-recursion { 192.168.0.0/16; localhost; };

    // Активация обязательной валидации DNSSEC
    dnssec-validation auto;

    // Рандомизация исходных портов UDP в максимально широком диапазоне
```

```
    use-v4-udp-ports { range 1024 65535; };

    // Защита от разведки (Reconnaissance): скрытие версии ПО
    version "None";
};

// Механизм Response Rate Limiting (RRL) для предотвращения DoS/Amplification атак
rate-limit {
    responses-per-second 10;
    window 5;
};
```

Листинг 1 – Пример конфигурации механизмов защиты на сервере BIND9

Поскольку для реализации успешного спуфинга злоумышленнику необходимо отправить массированный поток UDP-датаграмм (высокоскоростной флуд для эксплуатации Race Condition), критически важно задействовать защитные экраны на граничном сетевом оборудовании корпоративного периметра (например, на маршрутизаторах Eltex ESR). Включение аппаратного контроля аномального трафика позволяет снизить нагрузку на центральный процессор DNS-сервера.

```
! Активация механизмов фильтрации подозрительных пакетов на маршрутизаторе Eltex ESR
esr(config)# ip firewall screen suspicious-packets unknown-protocols
esr(config)# logging firewall screen suspicious-packets unknown-protocols
esr(config)# ip firewall screen suspicious-packets icmp-fragment
```

esr(config)# esr(config)# commit

Листинг 2 – Конфигурация экранирования пакетов на периметре сети

3.3. Обеспечение конфиденциальности на «последней миле»: протоколы DoT и DoH

Внедрение DNSSEC гарантирует подлинность данных между иерархическими серверами в глобальной сети, но оставляет незащищенным локальный сегмент (от рабочей станции пользователя до корпоративного резолвера). Внутри локальной вычислительной сети (ЛВС) злоумышленник может осуществить перехват или подмену DNS-запросов с помощью смежных атак (например, через ARP-спуфинг или компрометацию протокола DHCP).

Для защиты «последней мили» прикладной протокол DNS инкапсулируется в защищенные криптографические туннели транспортного уровня, полностью переводя обработку запросов со stateless-протокола UDP на надежный сессионный протокол TCP с TLS-шифрованием:

1. **DNS over TLS (DoT — RFC 7858):** направляет DNS-запросы через выделенный TCP-порт 853. Весь поток данных изолируется внутри TLS-сессии, что делает невозможным как пассивный анализ (сниффинг трафика), так и его активную модификацию промежуточными узлами.
2. **DNS over HTTPS (DoH — RFC 8484):** инкапсулирует запросы в стандартные сессии HTTP/2 или HTTP/3, использующие криптографический порт 443 TCP. Основным преимуществом DoH является его визуальное смешивание с общим веб-трафиком

организации, что исключает возможность селективной блокировки со стороны внешних провайдеров, но накладывает на ИБ-специалистов обязанность осуществлять инспекцию внутренних конечных точек.

3.4. Анализ эффективности комплексной защиты

Систематизация рассмотренных аппаратно-программных методов противодействия подмене доменных имен приведена в таблице 1.

Таблица 1 – Сравнительный анализ методов противодействия DNS-спуфингу

Метод защиты	**Преимущества**	**Недостатки / Ограничения**
Рандомизация исходных портов (Source Port Randomization)	Существенно снижает вероятность успешного перебора (Brute-force) идентификаторов TXID; минимальные накладные расходы.	Не защищает от атакующего, находящегося на пути трафика (On-Path attacker); является

Метод защиты	Преимущества	Недостатки / Ограничения
		лишь временным барьером.
Технология DNSSEC	Гарантирует криптографическую подлинность данных; полностью исключает риски отравления кэша (Cache Poisoning).	Повышенная административная нагрузка (ротация ключей); возрастает размер пакетов, вызывая риски фрагментации на сетевом уровне.
Шифрование трафика (DoT / DoH)	Полная защита клиентских запросов внутри ЛВС от перехвата и модификации; обеспечение строгой конфиденциальности.	Требует поддержки со стороны клиентских ОС и приложений; создает вычислительную нагрузку на серверы при TLS-хэндшейках.

4. Обсуждение результатов и анализ перспектив

Проведенный анализ показывает, что проблема уязвимости системы DNS носит комплексный характер. Как следует из базовых принципов сетевого взаимодействия, уязвимости прикладного уровня зачастую

обусловлены архитектурным выбором на нижележащих уровнях эталонной модели OSI.

4.1. Влияние транспортного уровня на безопасность DNS

Фундаментальная уязвимость традиционных DNS-запросов напрямую связана со спецификой их инкапсуляции. Для обеспечения максимальной скорости обмена данными система DNS по умолчанию использует транспортный протокол UDP и порт 53. В отличие от полнофункционального протокола TCP, который устанавливает сеанс связи с помощью трехстороннего согласования и гарантирует надежную доставку, протокол UDP является протоколом без отслеживания состояния (Stateless). Отсутствие контроля состояния сеанса связи позволяет злоумышленникам относительно легко подделывать IP-адреса источника и осуществлять успешные атаки типа «отравление кэша», обрушивая на резолвер поток фальшивых датаграмм.

4.2. Трудности внедрения механизмов защиты

Несмотря на то что технология DNSSEC обеспечивает надежную криптографическую защиту, её развертывание сталкивается с существенными инфраструктурными препятствиями. Внедрение DNSSEC многократно увеличивает размер передаваемых DNS-ответов из-за включения цифровых подписей (RRSIG).

Если размер ответа превышает стандартное ограничение UDP-пакета, сервер вынужден устанавливать флаг TC (Truncation) и требовать от клиента повторного запроса по протоколу TCP, что увеличивает задержки в сети. Кроме того, чрезмерно увеличенные UDP-пакеты могут приводить к IP-фрагментации на сетевом уровне. В результате жестко настроенные

межсетевые экраны могут классифицировать такие фрагментированные пакеты как потенциальную сетевую аномалию и блокировать их.

4.3. Перспективы развития: шифрование транспортного уровня

Поскольку протокол DNSSEC не решает проблему конфиденциальности (данные по-прежнему передаются в открытом виде), современным трендом корпоративной безопасности становится глубокое шифрование трафика. Протоколы DNS over HTTPS (DoH) и DNS over TLS (DoT) полностью переносят процесс разрешения имен с ненадежного протокола UDP на защищенные сессии TCP/TLS. В ближайшей перспективе именно гибридная модель — использование DoH/DoT внутри корпоративного периметра и DNSSEC для связи между рекурсивными и авторитативными серверами в глобальной сети — станет эталонным стандартом проектирования безопасных вычислительных систем.

5. Заключение

В ходе проведенного исследования был выполнен комплексный анализ уязвимостей системы доменных имен (DNS) и механизмов реализации атак, направленных на подмену маршрутной информации в корпоративных сетях. Теоретический анализ подтвердил, что исторически заложенные в спецификацию протокола недостатки — отсутствие встроенной криптографической аутентификации и использование транспортного протокола UDP — делают инфраструктуру DNS фундаментально уязвимой к подмене исходных адресов.

Доказано, что эксплуатация уязвимостей кэширующих серверов (в частности, использование вектора атаки Каминского) является одним из

наиболее опасных инструментов злоумышленников для перехвата управления доменной зоной. Компрометация локального DNS-резолвера фактически означает потерю контроля над маршрутизацией всего прикладного трафика предприятия.

Показано, что обязательным условием обеспечения безопасности современной ИТ-инфраструктуры является внедрение технологии DNSSEC для строгой верификации цифровых подписей доменных зон. В качестве дополнительного эшелона защиты, гарантирующего конфиденциальность и целостность клиентских запросов в недоверенных сегментах сетей, критически важно применение инкапсулирующих протоколов DoH и DoT, а также грамотная настройка списков контроля доступа и межсетевых экранов для фильтрации аномального трафика.

Таким образом, надежная информационная безопасность предприятия невозможна без обеспечения криптографической защиты инфраструктурных протоколов. Комплексная конфигурация серверов доменных имен выступает первичным и наиболее действенным барьером на пути реализации масштабных сетевых кибератак.

Литература

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 6-е изд. – Санкт-Петербург: Питер, 2020. – 1008 с.
2. Танненбаум, Э. Компьютерные сети [Текст] / Э. Танненбаум, Д. Уэзерролл; пер. с англ. В. Водолазского. – 5-е изд. – Санкт-Петербург: Питер, 2012. – 960 с.

3. Основы сетевых технологий. Часть 1. Лекция 10. Транспортный уровень [Текст]: учебные материалы / Кафедра телекоммуникаций. – 2024.
4. Основы сетевых технологий. Часть 1. Лекция 12. Принципы обеспечения безопасности сети [Текст]: учебные материалы / Кафедра телекоммуникаций. – 2024.
5. Основы сетевых технологий. Часть 1. Лекция 14. Протокол DNS [Текст]: учебные материалы / Кафедра телекоммуникаций. – 2024.
6. Mockapetris, P. Domain Names - Implementation and Specification: RFC 1035 [Electronic resource] / P. Mockapetris. // Internet Engineering Task Force (IETF). – URL: https://datatracker.ietf.org/doc/html/rfc1035 (дата обращения: 27.05.2026).
7. Arends, R. DNS Security Introduction and Requirements: RFC 4033 [Electronic resource] / R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. // Internet Engineering Task Force (IETF). – URL: https://datatracker.ietf.org/doc/html/rfc4033 (дата обращения: 27.05.2026).
8. Hoffman, P. DNS Queries over HTTPS (DoH): RFC 8484 [Electronic resource] / P. Hoffman, P. McManus. // Internet Engineering Task Force (IETF). – URL: https://datatracker.ietf.org/doc/html/rfc8484 (дата обращения: 27.05.2026).