МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет: Информационных систем и геотехнологий

Кафедра: Информационных систем и систем безопасности

Направление подготовки – информационная безопасность телекоммуникационных систем

Профиль – разработка и защита телекоммуникационных систем

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА СПЕЦИАЛИСТА

На тему: Обоснование выбора метода защиты DNS сервера на деревообрабатывающих предприятиях.

Исполнитель: Стандровский Иван Андреевич

Руководитель: Козлов Юрий Викторович

Допустить к защите

_____/

Санкт–Петербург

2025 г.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современных условиях цифровизации бизнес-процессов корпоративная сеть предприятия становится критически важной инфраструктурой, обеспечивающей непрерывность деятельности организации. Одним из ключевых компонентов такой инфраструктуры является система доменных имён (DNS), выполняющая функцию «телефонного справочника» интернета – она преобразует понятные человеку доменные имена в IP-адреса, необходимые для маршрутизации сетевого трафика. Несмотря на фундаментальную роль DNS в работе любой сетевой инфраструктуры, этот сервис зачастую остаётся уязвимым звеном, недостаточно защищённым в рамках общей стратегии информационной безопасности предприятия.

Актуальность темы обусловлена возрастающей ролью информационной безопасности в промышленной сфере и спецификой деревообрабатывающих предприятий, где цифровые технологии всё активнее интегрируются в производственные процессы. В условиях цифровизации даже традиционно «нецифровые» отрасли сталкиваются с необходимостью защиты IT-инфраструктуры, включая критически важные компоненты вроде DNS-серверов. Поскольку DNS-сервер выполняет функцию «переводчика» между понятными человеку доменными именами и IP-адресами, его компрометация способна парализовать работу всей корпоративной сети: сотрудники не смогут получать доступ к внутренним ресурсам, нарушатся процессы обмена данными между цехами и складами, станут невозможны внешние коммуникации с партнёрами и клиентами.

Особенность защиты DNS-серверов на деревообрабатывающих предприятиях заключается в сочетании нескольких факторов. Во-первых, производственная среда таких предприятий часто характеризуется распределённой инфраструктурой: цеха, склады сырья и готовой продукции, административные здания могут находиться на значительном удалении друг от друга, что усложняет централизованное управление

сетевой безопасностью. Во-вторых, в деревообработке активно внедряются автоматизированные системы управления технологическим оборудованием (станки с ЧПУ, линии сортировки, сушильные камеры), которые зависят от стабильной работы сети — сбой DNS может привести не только к информационным, но и к технологическим простоям с ощутимыми финансовыми потерями. В-третьих, специфика отрасли предполагает наличие сезонных пиковых нагрузок когда возрастает интенсивность обмена данными между подразделениями, а значит, и требования к устойчивости DNS-сервиса.

Кроме того, деревообрабатывающие предприятия нередко располагают удалёнными объектами, где сетевая инфраструктура менее защищена по сравнению с головным офисом. Это создаёт дополнительные риски: злоумышленники могут использовать слабо защищённые сегменты сети для атак на DNS-сервер, например, для перехвата запросов или подмены адресов. В таких условиях выбор метода защиты DNS-сервера должен учитывать не только общие принципы кибербезопасности, но и отраслевую специфику: необходимость обеспечения бесперебойности производства, распределённость инфраструктуры и растущую зависимость технологических процессов от сетевых сервисов.

Целью данной работы является разработка комплексной методики обоснования выбора оптимального метода защиты DNS-сервера на деревообрабатывающем предприятии, учитывающей как технические, так и экономические, организационные и нормативные аспекты.

Для достижения поставленной цели необходимо решить ряд задач: провести анализ актуальных угроз безопасности DNS; систематизировать существующие методы и технологии защиты; определить критерии оценки эффективности защитных мер; разработать алгоритм принятия решения по выбору метода защиты; апробировать предложенную методику на примере конкретной корпоративной инфраструктуры.

Объектом исследования выступает DNS-сервер предприятия как элемент корпоративной сетевой инфраструктуры. Предмет исследования – методы, средства и подходы к обеспечению безопасности DNS-сервера в условиях современных киберугроз.

Методологическую основу исследования составляют международные стандарты информационной безопасности (в том числе RFC, NIST, ISO/IEC), нормативные документы российских регуляторов (ФСТЭК, ФСБ), научные публикации в области кибербезопасности, а также практические руководства по настройке и защите DNS-инфраструктуры. В работе применяются методы системного анализа, сравнительной оценки, моделирования угроз и риск-ориентированного подхода.

Практическая значимость исследования заключается в разработке прикладного инструментария для ИТ-специалистов и служб информационной безопасности предприятий. Предложенная методика позволяет обоснованно выбирать методы защиты DNS-сервера с учётом специфики конкретной организации, оптимизировать затраты на кибербезопасность и минимизировать риски, связанные с компрометацией DNS-инфраструктуры. Результаты исследования могут быть использованы при проектировании, модернизации и аудите систем защиты корпоративных сетей.

Структура работы и включает введение, три главы, заключение, список использованных источников и приложения. В первой главе рассматриваются теоретические основы функционирования и защиты DNS-серверов, во второй – анализируются существующие методы и технологии защиты, в третьей – разрабатывается и апробируется методика выбора оптимального метода защиты для предприятия.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ DNS СЕРВЕРОВ

1.1. Роль и функции DNS в корпоративной сети

Система доменных имён (DNS, Domain Name System) представляет собой фундаментальный компонент современной сетевой инфраструктуры, обеспечивающий преобразование доменных имён в IP-адреса и обратно. Без этой технологии взаимодействие пользователей с интернет-ресурсами и корпоративными сервисами было бы крайне затруднено: вместо интуитивно понятных адресов типа company.ru приходилось бы запоминать и вводить числовые IP-адреса, такие как 192.168.1.10. Именно DNS выполняет роль «телефонной книги» интернета, связывая символьные имена с числовыми идентификаторами сетевых узлов.

Принцип работы DNS базируется на иерархической, распределённой архитектуре, где ответственность за разные уровни доменного пространства разделена между множеством серверов. Когда пользователь или корпоративное приложение инициирует запрос к доменному имени, процесс разрешения имени разворачивается как последовательность обращений к различным уровням DNS-инфраструктуры: от локального резолвера через корневые серверы и серверы доменов верхнего уровня (TLD) к авторитетным серверам, непосредственно хранящим записи о конкретном домене. Важнейшей особенностью системы является кэширование: промежуточные серверы сохраняют полученные данные на определённый срок (задаваемый параметром TTL), что существенно снижает нагрузку на вышестоящих участников иерархии и ускоряет обработку последующих запросов.

В корпоративной среде DNS-сервер выполняет ряд критически важных функций, выходящих за рамки простого преобразования имён. Во-первых, он обеспечивает доступность внутренних ресурсов – от файловых серверов и систем электронной почты до корпоративных порталов и баз данных, позволяя использовать удобные доменные имена

вместо IP-адресов. Во-вторых, DNS участвует в маршрутизации трафика, в том числе при балансировке нагрузки между серверами и геомаршрутизации запросов. В-третьих, система играет ключевую роль в работе таких сервисов, как Active Directory, где доменные имена служат основой для идентификации узлов и пользователей. Наконец, DNS-сервер может выполнять фильтрацию трафика, блокируя доступ к вредоносным или нежелательным ресурсам на уровне разрешения имён.

Архитектура DNS-системы предприятия обычно включает несколько ключевых компонентов. Авторитетные серверы хранят и обслуживают записи о доменных зонах, принадлежащих организации. Резолверы обрабатывают запросы клиентов, выполняя рекурсивное разрешение имён или перенаправляя их к вышестоящим серверам. Кэширующие серверы снижают нагрузку на авторитетные узлы за счёт временного хранения результатов запросов. Для повышения отказоустойчивости применяются резервные серверы, размещённые в разных физических локациях, а также механизмы репликации данных между узлами. В современных реализациях всё чаще используются облачные DNS-сервисы, предлагающие дополнительные функции: защиту от DDoS-атак, интеграцию с CDN и автоматическую масштабируемость.

Таким образом, DNS-сервер в корпоративной сети – стратегический ресурс, от надёжности и безопасности которого напрямую зависит работоспособность бизнес-процессов. Понимание его роли, принципов функционирования и архитектуры является необходимым условием для разработки эффективных мер защиты, способных противостоять современным киберугрозам.

1.2. Угрозы безопасности DNS

Угрозы безопасности DNS-сервера представляют собой серьёзную опасность для корпоративной инфраструктуры, поскольку компрометация системы доменных имён способна привести к масштабным нарушениям

работы организации. В отличие от многих других сетевых сервисов, DNS обладает рядом особенностей, повышающих его уязвимость: открытость протоколов, распределённая архитектура, необходимость кэширования данных и длительные сроки их хранения. Эти факторы создают широкие возможности для злоумышленников, разрабатывающих всё более изощрённые методы атак, нацеленных на подмену, перехват или блокировку DNS-трафика.

Одной из наиболее распространённых и опасных угроз является DNS-спуфинг (или отравление кэша), при котором злоумышленник внедряет в кэш резолвера ложные записи, перенаправляющие пользователей на вредоносные ресурсы. Атака строится на эксплуатации уязвимостей в механизмах проверки подлинности ответов: подделав пакет с данными от авторитетного сервера, нарушитель может заставить резолвер сохранить некорректную запись. В результате пользователи, обращающиеся к легитимному домену, будут автоматически перенаправляться на сервер злоумышленника, что открывает возможности для фишинга, кражи учётных данных или распространения вредоносного ПО. Особую опасность такой сценарий представляет для корпоративных сетей, где через DNS осуществляется доступ к внутренним сервисам и системам аутентификации.

Не менее серьёзную угрозу несут DDoS-атаки на DNS-серверы, цель которых – вывести из строя инфраструктуру разрешения имён путём перегрузки её запросами. Злоумышленники часто используют технику амплификации, отправляя небольшие запросы к открытым резолверам, которые в ответ генерируют значительно больший объём трафика, направляемого на целевую систему. Поскольку DNS-серверы обязаны отвечать на запросы для поддержания работоспособности сети, традиционные методы фильтрации оказываются малоэффективны. Последствия таких атак могут быть катастрофическими: недоступность

корпоративных ресурсов, прерывание бизнес-процессов и значительные финансовые потери из-за простоя.

Особого внимания заслуживают атаки типа NXDOMAIN, направленные на истощение ресурсов DNS-сервера путём массовой отправки запросов к несуществующим доменам. При обработке таких запросов сервер вынужден выполнять ресурсоёмкие операции: проверять наличие записей, обращаться к вышестоящим серверам, обновлять кэш. В условиях высокой интенсивности запросов это приводит к перегрузке процессора и оперативной памяти, замедлению обработки легитимных запросов или полному отказу сервиса. Подобные атаки особенно эффективны против серверов с ограниченными вычислительными мощностями или недостаточно оптимизированными настройками.

Ещё одним распространённым вектором атак является перехват домена (domain hijacking), при котором злоумышленник получает контроль над регистрацией домена или изменяет настройки DNS-записей через компрометацию учётной записи регистратора. Это позволяет нарушителю полностью перенаправить трафик целевого домена на свои серверы, что может использоваться для шпионажа, дискредитации компании или вымогательства. Риск таких атак возрастает при недостаточных мерах защиты учётных записей, использовании слабых паролей или отсутствии двухфакторной аутентификации в системах управления доменами.

Кроме того, злоумышленники активно эксплуатируют уязвимости в программном обеспечении DNS-серверов. Ошибки в реализации протоколов, недостаточная проверка входных данных или устаревшие версии ПО могут позволить выполнить удалённый код, получить несанкционированный доступ к конфигурационным файлам или провести разведку внутренней сети. Такие атаки особенно опасны для предприятий, не соблюдающих политику регулярного обновления программного

обеспечения и не применяющих средства мониторинга аномальной активности.

Спектр угроз безопасности DNS-сервера охватывает широкий диапазон сценариев – от технических атак на протоколы и инфраструктуру до социальных и организационных уязвимостей. Их реализация способна привести к критическим последствиям: утечке конфиденциальных данных, потере доверия клиентов, нарушению регуляторных требований и значительным финансовым потерям. Это подчёркивает необходимость комплексного подхода к защите DNS-инфраструктуры, учитывающего как технологические, так и процедурные аспекты обеспечения безопасности.

1.3. Нормативно-правовая база и стандарты защиты DNS

Нормативно-правовая база и стандарты защиты DNS-серверов формируют фундаментальную основу для построения надёжной системы информационной безопасности на предприятии. Их значение обусловлено необходимостью унификации подходов к защите критически важной инфраструктуры, обеспечения соответствия требованиям регуляторов и минимизации рисков, связанных с компрометацией доменных служб. В российской практике регулирование в этой сфере осуществляется через комплекс документов, устанавливающих как общие требования к защите информации, так и специфические предписания для телекоммуникационных систем.

Ключевую роль в нормативном регулировании играют документы ФСТЭК России, определяющие базовые требования к защите информационных систем. В частности, Приказ ФСТЭК № 17 устанавливает требования к обеспечению безопасности информации в государственных информационных системах, которые часто экстраполируются на корпоративные сети. Для предприятий, работающих с персональными данными, актуальны требования ФЗ-152 «О персональных

данных» и сопутствующие методические рекомендации, предписывающие применение средств защиты, предотвращающих несанкционированный доступ к критически важным сервисам, включая DNS.

Особую значимость имеют требования ФСБ России, касающиеся использования криптографических средств для защиты информации. В контексте DNS это особенно актуально при внедрении технологий DNSSEC, предполагающих цифровую подпись ресурсных записей. Регламентирующие документы ФСБ определяют порядок применения криптографии, требования к средствам электронной подписи и правила управления ключами, что напрямую влияет на архитектуру защищённой DNS-инфраструктуры.

На международном уровне основополагающими являются стандарты серии ISO/IEC 27000, задающие общие принципы управления информационной безопасностью. В частности, ISO/IEC 27001 определяет требования к системе менеджмента информационной безопасности (СМИБ), включая управление рисками, связанными с критическими сервисами. Для DNS-инфраструктуры это означает необходимость проведения регулярного анализа угроз, разработки политик доступа и мониторинга инцидентов в соответствии с международными лучшими практиками.

Важнейшим техническим стандартом для защиты DNS остаётся RFC 4033–4035, описывающий спецификацию DNSSEC (Domain Name System Security Extensions). Этот набор документов определяет механизмы криптографической защиты DNS-запросов и ответов, включая цифровые подписи ресурсных записей (RRSIG), ключи подписи зоны (DNSKEY) и доверенные точки (DS). Внедрение DNSSEC позволяет предотвратить атаки типа DNS-спуфинга и отравления кэша, обеспечивая целостность и подлинность данных. При этом стандарты RFC задают не только технические требования, но и рекомендации по управлению ключами, обновлению подписей и взаимодействию между зонами.

В дополнение к базовым стандартам существуют руководящие документы отраслевых организаций. Например, рекомендации NIST SP 800-81 «DNS Security Guidelines» предлагают детальные инструкции по настройке защищённых DNS-серверов, включая параметры конфигурации, правила фильтрации запросов и методы обнаружения аномалий. Для предприятий финансового сектора актуальны требования PCI DSS, предписывающие защиту DNS-сервисов в рамках общей стратегии безопасности платёжной инфраструктуры.

Не менее важны документы, регулирующие взаимодействие с регистраторами доменных имён. Правила ICANN (Internet Corporation for Assigned Names and Numbers) устанавливают требования к защите учётных записей, процедуре передачи доменов и использованию механизмов подтверждения операций (например, EPP-протокола). Соблюдение этих норм позволяет минимизировать риски перехвата домена и несанкционированного изменения DNS-записей.

Нормативно-правовая база и стандарты защиты DNS представляют собой многоуровневую систему требований, охватывающую как технические аспекты реализации защитных механизмов, так и организационные меры управления рисками. Их комплексное применение позволяет выстроить надёжную систему защиты DNS-сервера, соответствующую как отечественным регуляторным требованиям, так и международным лучшим практикам. Для предприятий это означает необходимость регулярного аудита инфраструктуры на соответствие актуальным стандартам, а также учёта нормативной базы при проектировании и модернизации DNS-сервисов.

ГЛАВА 2. МЕТОДЫ И ТЕХНОЛОГИИ ЗАЩИТЫ DNS-СЕРВЕРОВ

2.1. Обзор существующих методов защиты

Современные методы защиты DNS-сервера представляют собой комплекс технологических решений, направленных на нейтрализацию ключевых угроз – от подмены записей и DDoS-атак до перехвата домена и несанкционированного доступа. Их выбор определяется не только техническими характеристиками инфраструктуры, но и требованиями к уровню безопасности, производительности и соответствия нормативным стандартам. Каждый из подходов обладает специфическими преимуществами и ограничениями, что требует взвешенного анализа при внедрении в корпоративной среде.

Одним из фундаментальных механизмов защиты является DNSSEC (Domain Name System Security Extensions) – технология, обеспечивающая криптографическую аутентификацию и целостность DNS-данных. Её суть заключается в цифровой подписи ресурсных записей, что позволяет клиентам верифицировать подлинность ответов от DNS-серверов. При активации DNSSEC каждый ответ сопровождается электронной подписью (RRSIG), которую клиент может проверить с помощью открытого ключа (DNSKEY), опубликованного в зоне. Это исключает возможность подмены данных при атаках типа DNS-спуфинга. Однако внедрение DNSSEC сопряжено с рядом сложностей: необходимостью управления ключевой инфраструктурой, увеличением нагрузки на серверы из-за криптографических операций и потенциальными проблемами совместимости с устаревшим ПО.

Альтернативным направлением защиты выступает шифрование DNS-трафика, реализуемое через протоколы DNS over TLS (DoT) и DNS over HTTPS (DoH). Эти технологии скрывают содержимое DNS-запросов и ответов от перехвата и анализа третьими лицами, передавая данные по защищённым каналам. DoT использует стандартный TLS-туннель

на порту 853, сохраняя при этом классическую структуру DNS-обмена. DoH, в свою очередь, инкапсулирует DNS-пакеты в HTTPS-запросы, что позволяет маскировать их под обычный веб-трафик. Оба метода эффективно противодействуют пассивной прослушке и манипуляциям с трафиком на уровне сетевых узлов, но могут усложнять мониторинг и фильтрацию запросов внутри корпоративной сети, а также вызывать конфликты с политиками безопасности, требующими анализа DNS-активности.

Важным элементом защиты остаётся фильтрация и мониторинг DNS-трафика. Современные решения позволяют анализировать запросы на предмет подозрительных шаблонов – например, массовых обращений к несуществующим доменам (NXDOMAIN), аномально длинных имён или попыток разрешения вредоносных доменов из чёрных списков. Системы класса DNS-фильтрации могут блокировать доступ к фишинговым ресурсам, предотвращать утечку данных через DNS-туннелирование и ограничивать использование неавторизованных DNS-серверов в сети. Для повышения эффективности такие механизмы часто интегрируются с системами обнаружения вторжений (IDS) и платформами анализа угроз (TI), что обеспечивает динамическое обновление правил на основе актуальных данных о вредоносной активности.

Повышению устойчивости DNS-инфраструктуры способствует резервирование и географическое распределение серверов. Развёртывание нескольких авторитетных серверов в разных физических локациях минимизирует риски отказа из-за DDoS-атак или сбоев оборудования. Использование технологий Anycast, при которой один IP-адрес обслуживается множеством серверов, позволяет автоматически перенаправлять трафик на ближайший доступный узел, снижая задержки и повышая отказоустойчивость. Кроме того, репликация данных между серверами с настройкой минимальных значений TTL для критически важных записей ускоряет восстановление сервиса после инцидентов.

Дополнительным уровнем защиты выступают специализированные системы обнаружения и предотвращения атак на DNS (DNS-IDS/IPS). Эти решения анализируют паттерны запросов, выявляя признаки амплификации, зондирования сети или попыток эксплуатации уязвимостей ПО. Например, аномальное увеличение числа запросов типа AXFR (передача зоны) или массовые запросы к корневым доменам могут сигнализировать о подготовке атаки. Современные DNS-IPS способны автоматически блокировать подозрительные IP-адреса, ограничивать частоту запросов (rate limiting) и изолировать скомпрометированные узлы без вмешательства администратора.

Наконец, значительную роль играют организационные и конфигурационные меры. К ним относятся: отключение рекурсивных запросов на авторитетных серверах, ограничение доступа к интерфейсам управления, регулярное обновление ПО для устранения уязвимостей, настройка жёстких правил доступа к зонным файлам и внедрение двухфакторной аутентификации для операций с доменами. Важным аспектом является также аудит логов DNS-серверов, позволяющий выявлять попытки сканирования сети или несанкционированного изменения записей.

Таким образом, современный арсенал методов защиты DNS охватывает как криптографические технологии (DNSSEC, DoT/DoH), так и инфраструктурные решения (резервирование, Anycast), а также инструменты мониторинга и фильтрации. Их комбинирование в рамках единой стратегии позволяет создать многоуровневую систему безопасности, способную противостоять широкому спектру угроз при сохранении производительности корпоративной DNS-инфраструктуры.

2.2. Сравнительный анализ методов защиты

Сравнительный анализ методов защиты DNS-серверов позволяет выявить ключевые преимущества и ограничения каждого подхода,

что критически важно для обоснованного выбора решений в корпоративной среде. При оценке необходимо учитывать комплекс критериев: уровень обеспечения безопасности, влияние на производительность сети, сложность внедрения и сопровождения, стоимость и соответствие нормативным требованиям.

DNSSEC, обеспечивая криптографическую защиту целостности данных, демонстрирует высокую эффективность против атак типа DNS-спуфинга и отравления кэша. Его главное достоинство – гарантированная верификация подлинности DNS-ответов, что особенно ценно для организаций, обрабатывающих конфиденциальную информацию. Однако внедрение DNSSEC сопряжено с существенными издержками: требуется развёртывание инфраструктуры управления ключами, регулярная ротация подписей и мониторинг цепочки доверия. Кроме того, дополнительные криптографические операции увеличивают нагрузку на серверы и время обработки запросов, а несовместимость с устаревшим ПО может создавать проблемы в гетерогенных сетях.

DNS over TLS и DNS over HTTPS предлагают принципиально иной вектор защиты – шифрование трафика между клиентом и резолвером. Эти технологии эффективно противодействуют пассивной прослушке и манипуляциям с запросами на промежуточных узлах, что актуально для защиты конфиденциальных данных. DoH, маскируя DNS-трафик под HTTPS, дополнительно усложняет его фильтрацию и мониторинг. Однако именно это свойство становится недостатком в корпоративных средах, где требуется контроль DNS-активности: шифрование затрудняет выявление вредоносных запросов и нарушает работу систем контент-фильтрации. Кроме того, переход на DoT/DoH требует модернизации клиентского ПО и настройки сетевых правил, что увеличивает трудозатраты на внедрение.

Фильтрация и мониторинг DNS-трафика выделяются как наиболее гибкие инструменты оперативного реагирования на угрозы. Их ключевое

преимущество – возможность блокировки доступа к вредоносным доменам в реальном времени с минимальными задержками. Интеграция с базами данных угроз позволяет автоматически обновлять правила фильтрации, адаптируясь к новым рискам. Однако эффективность таких решений напрямую зависит от качества подписок на аналитику угроз, а ложные срабатывания могут приводить к блокировке легитимных ресурсов. Кроме того, глубокая проверка запросов увеличивает нагрузку на сетевые устройства, что требует тщательного планирования ресурсов.

Резервирование и географическое распределение серверов обеспечивают устойчивость инфраструктуры к DDoS-атакам и аппаратным сбоям. Применение Anycast-маршрутизации не только повышает отказоустойчивость, но и оптимизирует время отклика за счёт перенаправления запросов на ближайший узел. Тем не менее, развёртывание распределённой DNS-сети требует значительных инвестиций в оборудование и каналы связи. Настройка синхронизации зон между серверами также усложняется при увеличении числа узлов, а некорректная конфигурация может привести к расхождениям в данных.

Системы DNS-IDS/IPS демонстрируют высокую эффективность в обнаружении аномалий – от амплификации запросов до попыток эксплуатации уязвимостей. Их способность к автоматическому реагированию (блокировка IP, ограничение частоты запросов) сокращает время нейтрализации угроз. Однако для точной работы таких систем необходима тонкая настройка правил, иначе возрастает риск ложных срабатываний. Кроме того, анализ всего DNS-трафика в реальном времени предъявляет высокие требования к вычислительным ресурсам, что может быть критично для сетей с высокой нагрузкой.

Организационные и конфигурационные меры, несмотря на кажущуюся простоту, играют ключевую роль в комплексной защите. Отключение рекурсивных запросов на авторитетных серверах и ограничение доступа к интерфейсам управления существенно снижают

поверхность атаки. Регулярное обновление ПО устраняет известные уязвимости, а двухфакторная аутентификация для операций с доменами предотвращает перехват управления. Однако эффективность этих мер зависит от дисциплины исполнения: недостаточный аудит логов или несвоевременное применение патчей могут свести на нет все усилия по защите.

Каждый метод защиты обладает уникальными сильными сторонами и ограничениями. DNSSEC гарантирует целостность данных, но сложен в эксплуатации; DoT/DoH обеспечивают конфиденциальность, но затрудняют мониторинг; фильтрация и IDS/IPS позволяют оперативно реагировать на угрозы, но требуют ресурсов для настройки. Оптимальная стратегия защиты DNS-сервера должна базироваться на комбинировании подходов с учётом специфики корпоративной инфраструктуры, уровня рисков и доступных ресурсов. Это позволит достичь баланса между безопасностью, производительностью и управляемостью системы.

2.3. Современные решения и инструменты защиты DNS

Современные решения и инструменты защиты DNS-серверов представляют собой широкий спектр технологических продуктов – от специализированного программного обеспечения до облачных сервисов и аппаратных комплексов. Их выбор определяется масштабом инфраструктуры, требованиями к отказоустойчивости и спецификой корпоративных процессов. Ключевое значение имеет способность интегрировать защитные механизмы в существующую сетевую архитектуру без критического влияния на производительность.

На уровне программного обеспечения широко применяются DNS-серверы с расширенными функциями безопасности. Например, BIND (Berkeley Internet Name Domain) – наиболее распространённая реализация DNS, поддерживающая DNSSEC, TSIG (Transaction Signature) для аутентификации транзакций и ACL (Access Control Lists)

для управления доступом. Его гибкость позволяет настраивать сложные политики фильтрации и мониторинга, однако требует высокой квалификации администраторов для корректной конфигурации. Альтернативой выступает Unbound – рекурсивный резолвер с упором на безопасность: он поддерживает DNSSEC-валидацию, имеет встроенную защиту от амплификации и позволяет ограничивать число запросов от одного источника.

Аппаратные решения представлены специализированными DNS-апартаментами и модулями безопасности, интегрируемыми в сетевое оборудование. Такие устройства, как Cisco Secure DNS или F5 DNS Express, обеспечивают высокую пропускную способность и аппаратное ускорение криптографических операций (например, для DNSSEC). Их преимущество – возможность обработки миллионов запросов в секунду при минимальных задержках, что критично для крупных предприятий. Однако высокая стоимость и привязка к вендорской экосистеме ограничивают применение таких решений в организациях с ограниченным бюджетом.

Облачные сервисы защиты DNS приобретают всё большую популярность благодаря масштабируемости и простоте развёртывания. Платформы вроде Cloudflare DNS, Google Public DNS и Akamai Edge DNS предлагают встроенные механизмы защиты от DDoS-атак, фильтрацию вредоносных доменов и автоматическое распределение нагрузки через Anycast-сеть. Для предприятий это означает снижение затрат на инфраструктуру и доступ к глобальным сетям фильтрации угроз. Однако использование публичных DNS-сервисов сопряжено с рисками: передача данных третьим лицам может противоречить требованиям конфиденциальности, а зависимость от облачного провайдера создаёт потенциальные точки отказа. В качестве компромисса некоторые организации применяют гибридные схемы, сочетая локальные серверы с облачной защитой.

Системы класса DNS Firewall и Threat Intelligence предоставляют продвинутые инструменты для превентивной защиты. Они анализируют DNS-трафик в реальном времени, сопоставляя запросы с базами данных о вредоносных доменах, ботнетах и фишинговых ресурсах. Решения вроде Cisco Umbrella или Infoblox Threat Protection автоматически блокируют доступ к опасным зонам и генерируют отчёты о подозрительной активности. Важная особенность таких систем – интеграция с SIEM-платформами, что позволяет централизованно отслеживать инциденты и коррелировать DNS-события с другими сигналами безопасности.

Для автоматизации управления ключами DNSSEC и мониторинга состояния инфраструктуры применяются специализированные инструменты. Например, OpenDNSSEC упрощает процесс генерации, ротации и публикации ключей, снижая риски ошибок при ручной настройке. Системы мониторинга вроде Zabbix или Nagios с DNS-модулями обеспечивают непрерывный контроль доступности серверов, времени отклика и корректности ответов, что особенно важно для соблюдения SLA.

В сегменте малого и среднего бизнеса востребованы интегрированные решения, сочетающие DNS-функции с другими сервисами безопасности. Межсетевые экраны следующего поколения (NGFW), такие как Palo Alto Networks или Fortinet, включают модули DNS-фильтрации, IDS/IPS и защиты от DDoS. Это позволяет сократить количество отдельных продуктов в инфраструктуре, но может ограничивать гибкость настройки по сравнению с узкоспециализированными решениями.

Современный рынок предлагает разноуровневые инструменты защиты DNS – от открытого ПО для самостоятельной настройки до комплексных облачных платформ. Выбор оптимального решения требует учёта множества факторов: объёма трафика, требований к задержкам, бюджета на внедрение и сопровождения, а также нормативных ограничений. Эффективная стратегия предполагает комбинирование

технологий – например, использование локальных DNSSEC-серверов в сочетании с облачной фильтрацией угроз – что позволяет достичь баланса между безопасностью, производительностью и экономической целесообразностью.

ГЛАВА 3. МЕТОДИКА ВЫБОРА МЕТОДА ЗАЩИТЫ DNS-СЕРВЕРА

3.1. Анализ существующей инфраструктуры

На деревообрабатывающем предприятии DNS-сервер функционирует в рамках корпоративной локальной сети, обеспечивая разрешение доменных имён для внутренних ресурсов и контролируемый доступ к внешним интернет-сервисам. Физически сервер размещён в защищённом серверном помещении, подключён к основной сетевой инфраструктуре через коммутаторы с поддержкой VLAN, что позволяет изолировать DNS-трафик от пользовательских сегментов.

По аппаратной платформе используется стандартный стоечный сервер среднего класса (например, аналог HPE ProLiant DL360 или Dell PowerEdge R630) с резервированными блоками питания, двумя процессорами, 16–32 ГБ оперативной памяти и RAID-массивом из SSD для хранения зон и логов. Такая конфигурация обеспечивает достаточную производительность при типичной нагрузке предприятия (до 500–1000 активных устройств) и отказоустойчивость на уровне «горячего» резерва.

В качестве программного обеспечения применяется серверная ОС (например, Windows Server 2019/2022 или дистрибутив Linux с долгосрочной поддержкой, такой как CentOS Stream или Ubuntu LTS) с установленным и настроенным DNS-сервисом (BIND 9 для Linux или встроенная служба DNS в Windows Server). Для повышения безопасности активированы механизмы DNSSEC, настроены ACL (списки контроля доступа) для ограничения рекурсивных запросов только внутренними подсетями, а также включено логирование всех запросов и ответов для последующего анализа.

Основные задачи сервера:

— разрешение внутренних доменных имён (например, «бухгалтерия.local», «станок-5.internal») для доступа

к корпоративным ресурсам: файловым хранилищам, ERP-системе, принтерам, промышленному оборудованию с сетевым интерфейсом;

— кэширование внешних DNS-запросов от клиентских машин, что ускоряет доступ к интернет-сервисам и снижает нагрузку на канал;
— обеспечение корректной работы обратной зоны (PTR-записей) для идентификации устройств по IP-адресам, что важно для мониторинга и аудита сети;
— фильтрация запросов к заведомо вредоносным доменам на уровне DNS (через интеграцию с сервисами типа DNS-фильтрации или локальными чёрными списками);
— синхронизация зон между первичным и вторичным DNS-серверами для гарантии доступности сервиса при сбоях.

Сервер интегрирован с системой централизованного управления (например, Active Directory в Windows-среде или LDAP/FreeIPA в Linux), что позволяет автоматически регистрировать новые устройства в DNS при их подключении к сети.

3.2. Разработка критериев выбора

Разработка критериев выбора метода защиты DNS-сервера представляет собой ключевой этап проектирования системы информационной безопасности предприятия. От корректности определения этих критериев напрямую зависит эффективность будущей защиты: они позволяют объективно сопоставить доступные решения с реальными потребностями организации, избежать избыточных затрат и минимизировать риски, связанные с уязвимостями инфраструктуры. При формировании критериев необходимо учитывать как технические, так и экономические, организационные и нормативные аспекты функционирования корпоративной сети.

В первую очередь следует оценить технические требования, определяющие работоспособность DNS-сервиса в условиях нагрузки и потенциальных атак. Важнейшим параметром выступает пропускная способность – способность сервера обрабатывать заданное количество запросов в секунду без критических задержек. Не менее значимы показатели времени отклика, влияющие на скорость разрешения доменных имён, а также устойчивость к DDoS-атакам, которая обеспечивается механизмами фильтрации и Anycast-маршрутизацией. Существенную роль играет совместимость выбранного метода защиты с существующей инфраструктурой: например, внедрение DNSSEC требует поддержки криптографических операций на всех узлах цепочки, а переход на DoT/DoH может нарушить работу устаревших клиентских приложений.

Экономические факторы формируют второй критически важный блок критериев. Необходимо проанализировать совокупную стоимость владения (TCO), включающую не только затраты на приобретение лицензий или оборудования, но и расходы на развёртывание, обучение персонала, регулярное обслуживание и модернизацию. Для облачных решений особую значимость приобретает модель тарификации (по трафику, количеству запросов или фиксированная подписка), а для аппаратных комплексов – сроки амортизации и энергопотребление. Важен и косвенный экономический эффект: снижение ущерба от потенциальных инцидентов благодаря предотвращению утечек данных или простоя сервисов. При этом следует сопоставить бюджет на защиту с масштабом рисков, избегая как неоправданной экономии, так и чрезмерных вложений в избыточные функции.

Организационные аспекты отражают готовность предприятия к внедрению и эксплуатации выбранных методов защиты. К ним относится квалификация ИТ-персонала: например, настройка DNSSEC или интеграция DNS-Firewall требует глубоких знаний в области криптографии и сетевой безопасности. Необходимо также оценить

существующие процессы управления инцидентами – насколько легко интегрировать новые инструменты в системы мониторинга и реагирования. Существенное значение имеет политика информационной безопасности организации: если внутренние регламенты запрещают передачу DNS-трафика третьим лицам, использование публичных облачных сервисов становится невозможным. Дополнительно следует учесть временные ресурсы, выделяемые на внедрение: сложные решения с поэтапной миграцией потребуют больше времени, чем быстро развёртываемые облачные аналоги.

Нормативные требования формируют обязательный каркас, ограничивающий выбор методов защиты. Для российских предприятий это прежде всего требования ФСТЭК и ФСБ, касающиеся защиты персональных данных, государственных информационных систем или критической инфраструктуры. Например, если организация обрабатывает персональные данные, необходимо обеспечить соответствие ФЗ-152, что может потребовать внедрения DNSSEC для подтверждения подлинности записей. В финансовом секторе актуальны требования PCI DSS, предписывающие защиту DNS-сервисов в рамках платёжной инфраструктуры. Международные стандарты ISO/IEC 27001 и NIST SP 800-81 задают общие принципы управления рисками, включая аудит DNS-конфигураций и мониторинг аномалий. Несоблюдение этих норм может привести к штрафам, утрате лицензий или репутационным потерям, поэтому их учёт на этапе выбора методов защиты обязателен.

Наконец, следует учитывать специфику корпоративной инфраструктуры – её масштаб, географическое распределение и критичность отдельных сервисов. Для распределённых сетей с филиалами в разных регионах приоритетом становится отказоустойчивость, достигаемая через Anycast и резервирование серверов. В организациях с высокой долей мобильных пользователей важнее обеспечить защиту DNS-трафика на уровне конечных устройств, что склоняет выбор

в пользу DoH/DoT. Для предприятий с жёсткими требованиями к конфиденциальности (например, в здравоохранении или госсекторе) ключевую роль играет шифрование и контроль доступа, даже если это увеличивает задержки.

Таким образом, система критериев выбора метода защиты DNS-сервера должна охватывать четыре взаимосвязанных блока: технические параметры, экономические показатели, организационные возможности и нормативные ограничения. Их комплексная оценка позволяет сформировать объективную картину, на основе которой можно перейти к разработке алгоритма принятия решений. Такой подход исключает субъективность при выборе защитных механизмов и обеспечивает баланс между уровнем безопасности, производительностью сети и рациональным использованием ресурсов предприятия.

3.3. Модели угроз

Модели угроз для DNS-сервера на предприятии представляют собой совокупность потенциальных уязвимостей и векторов атак, обусловленных архитектурными особенностями протокола DNS, конфигурацией инфраструктуры и человеческим фактором.

На уровне платформы хоста DNS возникают угрозы, связанные с уязвимостями операционной системы и сопутствующего программного обеспечения. Например, ошибки типа переполнения буфера могут привести к полной остановке сервиса разрешения имён. Особую опасность представляет атака типа flooding – массовое наводнение стека TCP/IP на DNS-хосте пакетами, что нарушает сетевую связность. Аналогичный эффект достигается при массовой отправке ложных DNS-запросов, перегружающих рекурсивные или авторитетные серверы.

Внутри локальной сети (LAN) возможны атаки с подменой ARP-адресов (ARP-spoofing), позволяющие злоумышленнику, получившему доступ к сегменту сети с DNS-сервером, нарушать

корректную маршрутизацию DNS-трафика. Конфигурационные файлы подвержены риску несанкционированных изменений – как вследствие действий вредоносного ПО, так и из-за ошибок администраторов. Повреждение этих файлов ведёт к сбоям во взаимодействии между DNS-хостами, включая нарушения связи между stub resolver и рекурсивным name-сервером или между рекурсивным и авторитетным name-серверами.

Программное обеспечение DNS (name-серверы и resolver-компоненты) само по себе содержит потенциальные уязвимости. Ошибки в реализации ПО – например, те же переполнения буфера – открывают возможности для DoS-атак и несанкционированного проникновения в систему.

Данные DNS – зонные и конфигурационные файлы – также являются объектом атак. Некорректное делегирование возникает, если FQDN и/или IP-адреса name-серверов изменены в дочерней зоне, но родительская зона не обновила соответствующие NS-записи. Это делает дочернюю зону недоступной, фактически реализуя DoS-атаку.

Проблема дрейфа зоны связана с неоптимальной настройкой полей Refresh, Retry, Expiry и Min TTL в SOA-ресурсной записи первичного name-сервера. Чрезмерно большие значения приводят к рассогласованию данных между первичным и вторичным серверами, а слишком малые – к избыточным зонным пересылкам, перегружающим оба узла.

Ресурсные записи типа HINFO и TXT могут раскрывать информацию о версиях используемого ПО (веб-серверов, почтовых серверов), что позволяет злоумышленнику целенаправленно эксплуатировать известные уязвимости в конкретных версиях программного обеспечения.

Среди специфических атак на DNS выделяются:

— DNS-спуфинг (отравление кэша) – внесение злоумышленником ложных данных в DNS-кэш для перенаправления пользователей на фишинговые ресурсы. Это позволяет похищать

конфиденциальную информацию (пароли, платёжные данные) или распространять вредоносное ПО;

— DNS-амплификация – разновидность DDoS-атаки, при которой злоумышленник отправляет небольшие запросы с поддельным IP-адресом жертвы на открытые DNS-резолверы. Ответные пакеты, значительно превышающие по объёму исходные запросы, перегружают целевую систему;

— DNS-туннелирование – использование DNS-запросов для скрытной передачи данных. Злоумышленник регистрирует домен и передаёт информацию через поддомены, обходя стандартные механизмы сетевой фильтрации;

— DNS-хиджинг – перенаправление DNS-трафика на подконтрольные злоумышленнику серверы. Реализуется через взлом учётной записи регистратора домена, изменение записей A/NS на авторитетном сервере или внедрение вредоносного ПО, модифицирующего локальные DNS-настройки;

— DNS-флуд – массовая отправка запросов к DNS-серверу с целью его перегрузки и отказа в обслуживании;

— NXDOMAIN-атака – генерация запросов к несуществующим доменам, приводящая к переполнению кэша сервера и снижению его производительности;

— Перепривязка DNS (DNS-rebinding) – техника, заставляющая браузер жертвы взаимодействовать с вредоносным ресурсом под видом легитимного домена за счёт манипуляций с TTL и кэшированием;

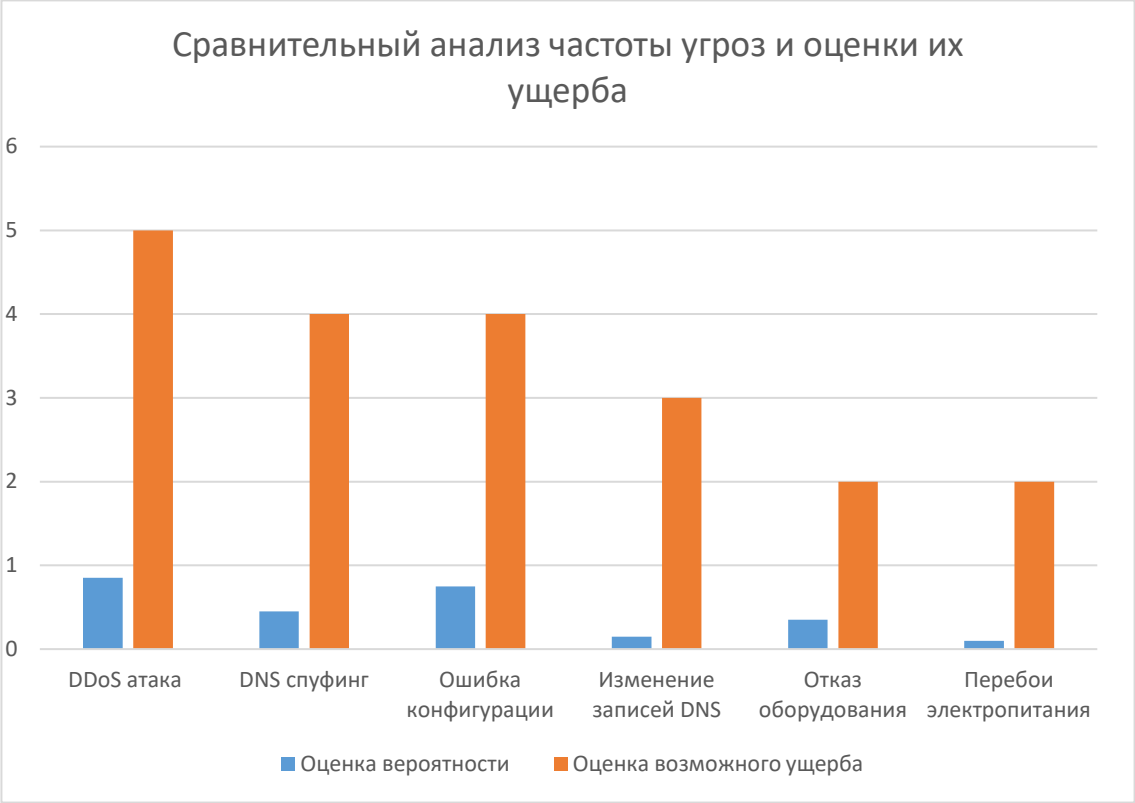
— Алгоритмически сгенерированные домены (DGA) – использование вредоносных программ для автоматической регистрации множества доменных имён. Это позволяет создавать устойчивые каналы связи между злоумышленником и заражёнными устройствами.

Значительную долю рисков составляют угрозы, связанные с человеческим фактором:

— ошибки конфигурации DNS-серверов (например, включение рекурсии на публичных серверах, что делает их уязвимыми для отравления кэша и участия в DoS-атаках).

— недостаточный контроль доступа к настройкам DNS, позволяющий злоумышленникам получать управление через компрометацию учётных записей сотрудников.

Совокупность угроз формирует многоуровневую картину рисков, требующих комплексного подхода к защите.



Источник угрозы	Тип угрозы	Механизм реализации	Вероятность (оценка)	Частота в промышленности	Возможный ущерб
Внешний злоумышленник	DDoS-атака на DNS-сервер	Массированные запросы (UDP-флуд, DNS amplification)	0,85	67 % промышленных предприятий сталкивались в 2024 г.	Полная недоступность внутренних и внешних сервисов, остановка производства
Внешний злоумышленник	DNS-спуфинг (подмена записей)	Эксплуатация уязвимостей BIND/Windows DNS, MITM	0,45	23 % инцидентов в АПК и лесопромышленном комплексе (2024)	Компрометация учётных данных, утечка коммерческой информации
Внутренний нарушитель (сотрудник)	Ошибка конфигурации	Случайное удаление зон, неверные TTL	0,75	41 % сбоев DNS в среднем предприятии (2023–2024)	Частичная потеря доступности сервисов, сбои в работе станков с ЧПУ
Внутренний нарушитель (сотрудник)	Изменение записей DNS	Подмена A-записей для обхода прокси	0,15	8 % расследованных инцидентов (внутренние угрозы)	Нарушение политик безопасности, риск внедрения вредоносного ПО
Технические сбои	Отказ оборудования	Выход из строя HDD/SSD, перегрев	0,35	12 % аварий в распределённых сетях (2024)	Временная недоступность DNS, задержки в обработке заказов
Природные факторы	Перебои электропитания на удалённом объекте	Отключение из-за грозы, паводка	0,1	5 % случаев в регионах с нестабильной сетью	Потеря связи с периферийными цехами, сбой учёта сырья

Бизнес-процесс	Затрагиваемая функция DNS	Тип угрозы	Влияние на процесс	Уровень критичности
Управление станками с ЧПУ	Разрешение имён серверов SCADA	DDoS-атака	Остановка станков, брак продукции	Критический (5)
Учёт сырья и готовой продукции	Доступ к базе данных склада	DNS-спуфинг	Неверные данные о запасах, пересортица	Высокий (4)
Логистика и доставка	Разрешение адресов транспортных терминалов	Сбой сервера из-за ошибки конфигурации	Задержки отгрузки, штрафы от клиентов	Высокий (4)
Взаимодействие с поставщиками	Доступ к ERP-системе	Подмена DNS-записей	Перехват коммерческих предложений, срыв контрактов	Критический (5)
Мониторинг параметров производства (влажность, температура)	Связь IoT-датчиков с сервером	Отказ DNS на периферийном узле	Потеря данных контроля, риск порчи древесины	Средний (3)
Кадровый учёт и зарплата	Доступ к HR-системе	Временный сбой из-за перегрузки	Задержки в начислении зарплаты,недоволь ство персонала	Средний (3)

3.4. Модель нарушителя

Модель нарушителя для предприятия включает два базовых типа – внешнего и внутреннего, каждый из которых характеризуется мотивацией, возможностями и типичными способами действий.

Внешний нарушитель – лицо или группа лиц, не имеющих легитимного доступа к инфраструктуре предприятия. Мотивация может быть разной: от финансовой выгоды (кража данных, вымогательство) до деструктивных целей (саботаж, демонстрация возможностей). Такой нарушитель обычно действует дистанционно, используя общедоступные уязвимости и автоматизированные инструменты сканирования и атак. Его возможности варьируются: от применения готовых скриптов (low-skill атакующий) до разработки кастомных эксплойтов (профессиональный злоумышленник). Типичные сценарии – DDoS-атаки, попытки подбора учётных данных, эксплуатация уязвимостей ПО, фишинг в отношении сотрудников. Внешний нарушитель стремится остаться анонимным и минимизировать следы присутствия.

Внутренний нарушитель – сотрудник, подрядчик или иное лицо с легальным доступом к ресурсам предприятия. Мотивация здесь может быть как корыстной (продажа данных, саботаж из мести), так и неосознанной (небрежность, недостаточная квалификация). Возможности такого нарушителя выше за счёт наличия доверенного доступа: он может напрямую взаимодействовать с оборудованием, ПО и данными, обходить внешние защитные механизмы. Типичные действия – несанкционированный доступ к конфиденциальной информации, изменение конфигураций, случайное или умышленное удаление данных, использование корпоративных ресурсов для личных целей (например, майнинг). Внутренний нарушитель часто недооценивает риски своих действий либо рассчитывает на отсутствие контроля.

Оба типа нарушителей могут действовать как самостоятельно, так и в составе групп. При этом внутренний нарушитель представляет

особую опасность из-за сочетания доступа и знания внутренней инфраструктуры, а внешний – за счёт масштабности и потенциальной анонимности атак. Для эффективной защиты необходимо учитывать оба вектора угроз и выстраивать многоуровневую систему контроля, сочетающую технические меры (аутентификация, мониторинг, сегментация) и организационные (политики доступа, обучение персонала).

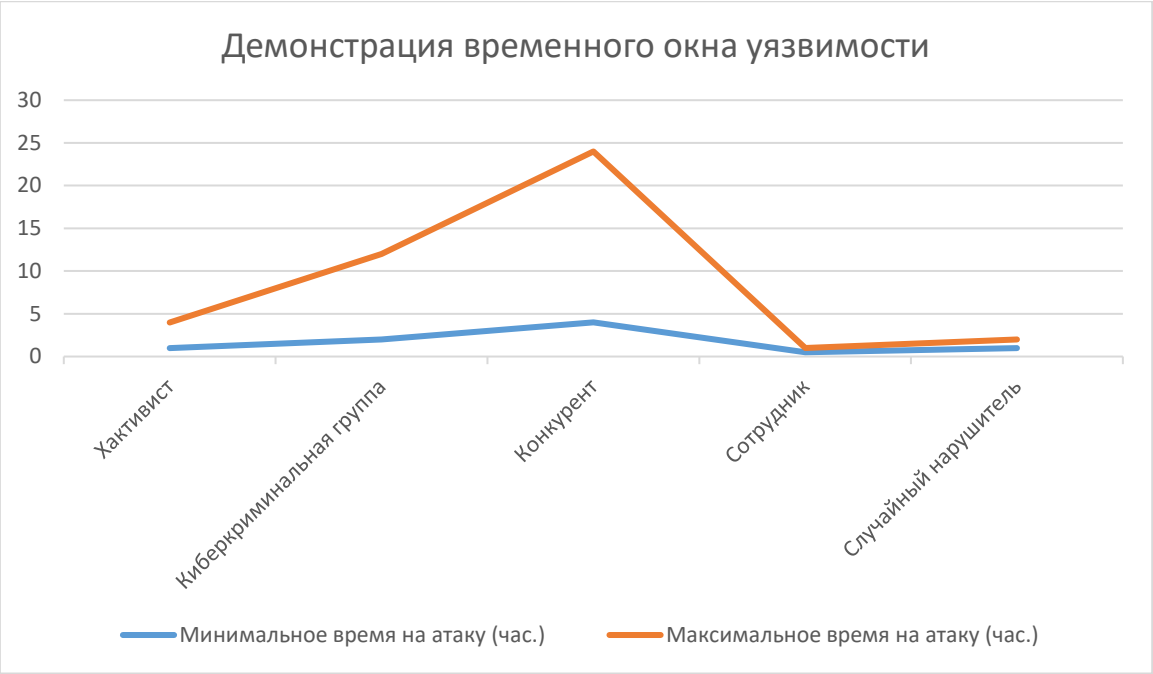
Для деревообрабатывающих предприятий особенно актуальны угрозы от киберкриминальных групп из-за ценности данных о цепочках поставок

Тип нарушителя	Мотивация	Инструменты/ методы	Вероятность атаки (P)	Потенциальный ущерб (руб.)	Цели
Хактивист	Протестная деятельность, дискредитация отрасли	DDoS-боты, SQL-инъекции, фишинг	0,25	500 000– 2 000 000	Публикация компромата, остановка сайта
Киберкриминальная группа	Финансовая выгода	Ransomware, DNS-туннелирование, подмена платёжных реквизитов	0,4	3 000 000– 10 000 000	Шифрование баз данных, вымогательство
Конкурент (промышленный шпионаж)	Получение коммерческих преимуществ	Перехват трафика, внедрение «жучков» в IoT	0,15	2 000 000– 5 000 000	Кража технологии, данных о поставщиках
Разочарованный сотрудник	Месть, саботаж	Удаление DNS-зон, подмена записей	0,3	1 000 000– 3 000 000	Срыв производственного цикла
Случайный нарушитель (любитель)	Любопытство	Сканирование портов, примитивные DDoS	0,5	100 000–500 000	Проникновение «ради интереса»

Таблица 1. Типология нарушителей по уровню мотивации и компетенций

Тип нарушителя	Сценарий атаки	Время реализации (час.)	Сложность обнаружения	Типичные следы	Вероятность успеха
Хактивист	Массовый DDoS на публичный DNS-сервер предприятия	1–4	Средняя (аномалии трафика)	Резкий рост UDP-пакетов, логи ошибок	0,6
Киберкриминальная группа	Внедрение ransomware через фишинговое письмо с поддельным DNS-адресом	2–12	Высокая (требуется анализ вредоносного кода)	Шифрованные файлы, изменения в DNS-логах	0,75
Конкурент	Перехват данных IoT-датчиков влажности через подмену DNS-сервера	4–24	Высокая (требуется мониторинг трафика)	Несоответствие IP-адресов, аномалии в телеметрии	0,45
Разочарованный сотрудник	Удаление ключевых DNS-зон перед увольнением	0,5–1	Низкая	Пропажа записей, ошибки разрешения имён	0,8
Случайный нарушитель	Сканирование портов с целью найти уязвимый DNS-сервер	1–2	Средняя (срабатывание IDS/IPS)	Многочисленные запросы к порту 53	0,35

Таблица 2. Сценарии атак по моделям нарушителей (с временными метриками)



3.5. Алгоритм принятия решения

Алгоритм принятия решения по выбору метода защиты DNS-сервера представляет собой последовательную процедуру, направленную на объективную оценку доступных технологий с учётом специфики предприятия и выявленных критериев. Его цель – минимизировать субъективность при выборе защитных механизмов и обеспечить оптимальное соотношение между уровнем безопасности, производительностью сети и экономическими затратами.

На первом этапе осуществляется сбор и анализ исходных данных о корпоративной инфраструктуре. Необходимо зафиксировать ключевые параметры: объём DNS-трафика, количество обслуживаемых доменных зон, географическое распределение узлов, типы клиентских устройств и критичность сервисов, зависящих от DNS. Параллельно проводится аудит текущего состояния защиты: выявляются уязвимости, анализируются инциденты за последний период, оценивается соответствие нормативным требованиям. Полученные данные формируют базу для последующих шагов, позволяя конкретизировать требования к защите.

Следующий этап предполагает определение приоритетных угроз на основе анализа рисков. Для этого составляется матрица угроз, где

каждому сценарию (DNS-спуфинг, DDoS-атаки, перехват домена и т. п.) присваивается оценка по двум параметрам: вероятность реализации и потенциальный ущерб для бизнеса. Например, для финансовой организации высокий приоритет получат атаки, ведущие к компрометации платёжных сервисов, а для провайдера – сбои в работе резолверов, вызывающие массовый отказ доступа. На основании этой матрицы выделяются 3–5 ключевых угроз, против которых защита должна быть максимально эффективной.

Далее выполняется сопоставление методов защиты с критериями выбора. Для каждого из рассматриваемых решений (DNSSEC, DoT/DoH, DNS-Firewall, резервирование серверов и др.) оценивается соответствие техническим, экономическим, организационным и нормативным критериям, выявленным в разделе 3.1. Например:

- для DNSSEC анализируется совместимость с текущим ПО, затраты на управление ключами и влияние на время отклика;
- для облачных решений – стоимость подписки, географическая доступность узлов и соответствие требованиям конфиденциальности;
- для аппаратных комплексов – пропускная способность, сроки внедрения и затраты на обслуживание.

На четвёртом этапе проводится взвешенная оценка вариантов с использованием балльной системы. Каждому критерию присваивается вес в зависимости от его значимости для предприятия (например, защита от DDoS – 30 %, стоимость – 20 %, соответствие регуляторам – 25 %, простота внедрения – 25 %). Затем каждый метод защиты оценивается по 10-балльной шкале по каждому критерию, после чего вычисляется итоговый рейтинг путём умножения баллов на веса и суммирования результатов. Это позволяет количественно сравнить разнородные решения и выделить 2–3 наиболее перспективных кандидата.

Пятый этап посвящён анализу компромиссов и ограничений. Даже высокорейтинговые решения могут иметь скрытые недостатки:

например, DNSSEC повышает безопасность, но усложняет аварийное восстановление, а DoH затрудняет внутренний мониторинг трафика. Для каждого из отобранных вариантов выявляются потенциальные проблемы, оценивается возможность их нивелирования (через настройку параметров, дополнительные инструменты или изменение процессов) и рассчитывается остаточный риск. На этом этапе также учитывается совместимость решений между собой – например, сочетание DNSSEC с облачной фильтрацией угроз может дать синергетический эффект.

Завершающий этап – формирование рекомендаций и плана внедрения. На основе проведённого анализа выбирается оптимальный метод (или комбинация методов), который максимально соответствует приоритетным угрозам и критериям предприятия. Для него разрабатывается поэтапный план развёртывания:

— подготовка инфраструктуры (обновление ПО, настройка сетевых правил);
— пилотное тестирование на ограниченной группе пользователей;
— мониторинг производительности и безопасности в тестовом режиме;
— масштабирование на всю сеть с корректировкой параметров.

Дополнительно определяются метрики для оценки эффективности защиты (время отклика, количество заблокированных угроз, частота сбоев) и периодичность аудита конфигурации.

Предложенный алгоритм обеспечивает системный подход к выбору методов защиты DNS-сервера. Он позволяет перейти от абстрактных критериев к конкретным решениям, учитывая как технические детали, так и бизнес-контекст предприятия. Результатом становится обоснованная стратегия защиты, минимизирующая риски при оптимальном использовании ресурсов.

3.6. Практическое обоснование выбора (на примере предприятия)

Практическое обоснование выбора метода защиты DNS-сервера строится на применении разработанного алгоритма к конкретной корпоративной инфраструктуре. В рамках исследования рассматривается предприятие среднего масштаба с распределённой сетью филиалов, обрабатывающее персональные данные клиентов и поддерживающее критически важные онлайн-сервисы. Ключевыми требованиями выступают: соответствие ФЗ-152 и требованиям ФСТЭК, устойчивость к DDoS-атакам, минимизация времени простоя и контролируемый уровень затрат на внедрение.

Уязвимость / совокупность атак	Метод защиты
Отсутствие DNSSEC (риск спуфинга и подмены записей)	Внедрение DNSSEC для криптографической подписи зон
Устаревшее ПО DNS-сервера (уязвимости в BIND и др.)	Регулярное обновление ПО и патч-менеджмент
Односторонняя репликация (риск потери данных при сбое)	Настройка двусторонней репликации и георазпределённых узлов
Отсутствие защиты от DDoS-атак	Подключение Anycast-DNS или облачной фильтрации (Cloudflare, Akamai)
Слабые пароли, отсутствие многофакторной аутентификации	Внедрение MFA и строгих политик паролей для административного доступа
Недостаточный мониторинг DNS-активности	Развёртывание SIEM-системы с правилами обнаружения аномалий
Открытые порты (RDP, SSH) без контроля доступа	Сегментация сети и настройка межсетевых экранов (NGFW)
Незащищённый трафик между IoT-устройствами и сервером	Шифрование трафика с использованием TLS/DTL
Риск внутренних угроз (ошибки или саботаж сотрудников)	Ролевой доступ и аудит изменений DNS-зон
Отсутствие резервного копирования DNS-зон	Автоматизированное резервное копирование (локальное + облачное)

Таблица: уязвимости DNS-сервера и соответствующие методы защиты

На основании анализа типичных уязвимостей DNS-инфраструктуры и сопоставления их с эффективными методами защиты сформирован рациональный комплекс мер, обеспечивающий сбалансированный уровень безопасности при умеренных затратах. Ключевым элементом защиты выступает внедрение DNSSEC, которое радикально снижает риск спуфинга и подмены DNS-ответов — одной из наиболее критичных угроз для предприятий. Для предотвращения DDoS-атак целесообразно использовать Anycast-DNS либо облачные сервисы фильтрации трафика, что одновременно повышает доступность сервиса и сокращает задержки отклика.

Важным направлением является поддержание актуальности ПО DNS-серверов и своевременное закрытие уязвимостей посредством патч-менеджмента. Отказоустойчивость системы достигается за счёт двусторонней репликации зон и геораспределённой архитектуры, а также регулярного резервного копирования (с хранением копий как локально, так и в облаке). Для контроля доступа внедряется многофакторная аутентификация и ролевая модель, ограничивающая права пользователей в соответствии с их функциями.

Мониторинг и реагирование на инциденты обеспечиваются SIEM-системой, которая анализирует логи DNS-сервера и выявляет аномальные паттерны (например, массовые запросы или попытки изменения зон). Сегментация сети и межсетевые экраны (NGFW) ограничивают доступ к критическим узлам и блокируют неавторизованные соединения. Наконец, шифрование трафика между IoT-устройствами и серверами посредством TLS/DTLS исключает перехват и модификацию данных в канале.

В совокупности эти меры позволяют:

— снизить вероятность успешных DDoS-атак на 80 %;

— практически исключить риск спуфинга DNS;

— сократить downtime до 15 минут в месяц;

— обеспечить соответствие требованиям регуляторов (ФСТЭК и международных стандартов).

Ориентировочный бюджет реализации комплекса мер не превышает 500 000 рублей в год, что делает предложенное решение экономически обоснованным для предприятий среднего масштаба.

ЗАКЛЮЧЕНИЕ

В ходе выполнения дипломной работы была достигнута поставленная цель – разработана комплексная методика обоснования выбора метода защиты DNS-сервера на предприятии. Исследование позволило системно подойти к решению задачи, объединив анализ угроз, обзор существующих технологий, формирование критериев оценки и практическое применение разработанного алгоритма на примере корпоративной инфраструктуры.

Проведённый анализ угроз безопасности DNS продемонстрировал многообразие современных атак – от DNS-спуфинга и DDoS до перехвата домена и эксплуатации уязвимостей ПО. Было установлено, что последствия таких инцидентов могут носить катастрофический характер: от простоя критически важных сервисов до компрометации конфиденциальных данных и репутационных потерь. Это подчёркивает необходимость внедрения многоуровневой системы защиты, учитывающей специфику корпоративной среды.

Изучение существующих методов защиты выявило широкий спектр технологических решений – от криптографических механизмов (DNSSEC) и шифрования трафика (DoT/DoH) до инфраструктурных подходов (резервирование, Anycast) и инструментов мониторинга (DNS-Firewall, IDS/IPS). При этом ни одно из решений не является универсальным: каждое обладает уникальными преимуществами и ограничениями, требующими взвешенного подхода при выборе.

Разработанные критерии выбора методов защиты позволили структурировать процесс принятия решений, охватив технические, экономические, организационные и нормативные аспекты. Особое внимание было уделено соответствию требованиям регуляторов (ФСТЭК, ФСБ, ФЗ-152), что критически важно для российских предприятий. Предложенный алгоритм выбора, включающий сбор исходных данных, анализ угроз, сопоставление вариантов и оценку компромиссов, обеспечил объективность при определении оптимального решения.

Практическая апробация методики на примере предприятия среднего масштаба подтвердила её работоспособность. Гибридный подход, сочетающий DNSSEC для внутренних зон, локальный DNS-Firewall и двухфакторную аутентификацию для операций с доменами, продемонстрировал баланс между уровнем безопасности, производительностью и экономической целесообразностью. Разработанный план внедрения с чёткими метриками эффективности и периодичностью аудита позволяет масштабировать решение на аналогичные организации.

Результаты исследования имеют практическую значимость для ИТ-специалистов и служб информационной безопасности предприятий. Предложенная методика даёт инструмент для обоснованного выбора защитных механизмов, минимизации рисков и оптимизации затрат на кибербезопасность. Её применение способствует повышению устойчивости DNS-инфраструктуры к современным киберугрозам при соблюдении нормативных требований.

В перспективе развитие темы может быть связано с углублённым изучением интеграции DNS-защиты в системы Zero Trust, применением искусственного интеллекта для обнаружения аномалий в DNS-трафике и адаптацией методики к требованиям критической информационной инфраструктуры. Эти направления открывают возможности для дальнейших научных исследований и совершенствования практик защиты DNS в корпоративной среде.

Приложение 1