ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.72

Разработка архитектуры межсетевого взаимодействия и системы контроля трафика для корпоративной сети среднего масштаба

А.А. Сидельникова
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
Рассматривается проблема обеспечения информационной безопасности в условиях усложнения корпоративных сетей и роста числа угроз. Обосновывается идея о том, что защита должна быть многоуровневой и строиться на сочетании различных механизмов контроля и фильтрации трафика. Анализируются современные угрозы информационной безопасности, включая внешние атаки и внутренние уязвимости. Проведён обзор современных средств защиты и их функциональных возможностей. На основе полученных результатов разработана архитектура системы безопасности, обеспечивающая многоуровневую защиту сетевых ресурсов. Предложенное решение учитывает необходимость баланса между требованиями безопасности и оптимальностью затрат, а также опирается на отечественные средства защиты.

Ключевые слова: межсетевое взаимодействие, контроль сетевого трафика, корпоративные сети среднего масштаба, угрозы безопасности, многоуровневая защита сети, импортозамещающие средства защиты, архитектура сетевой безопасности

Для цитирования. Сидельникова А.А. Разработка архитектуры межсетевого взаимодействия и системы контроля трафика для корпоративной сети среднего масштаба. *Молодой исследователь Дона.* 2026;11(1):23–30.

Development of an Inter-networking Architecture and Traffic Control System for Medium-Scale Corporate Networks

Anastasia A. Sidelnikova
Don State Technical University, Rostov-on-Don, Russian Federation

Abstract
The article studies the problem of ensuring information security in the context of increasing complexity of corporate networks and a growing number of cyberthreats. The idea of multi-layered protection based on a combination of various traffic control and filtering mechanisms has been substantiated. Existing information security threats including external attacks and internal vulnerabilities have been analysed. An overview of up-to-date cybersecurity tools and their capacities has been made. Based on the results obtained, a security system architecture ensuring multi-layered protection of network resources has been developed. The proposed solution ensures the balance between the security requirements and cost efficiency, and relies on the national cybersecurity tools.

Keywords: inter-networking, network traffic control, medium-scale corporate networks, security threats, multi-layered network protection, import-substituting security tools, network security architecture

For Citation. Sidelnikova AA. Development of an Inter-networking Architecture and Traffic Control System for Medium-Scale Corporate Networks. *Young Researcher of Don.* 2026;11(1):23–30.

Введение. Стремительное развитие цифровых технологий и растущая зависимость бизнеса от сетевых инфраструктур приводят к значительному увеличению объёма сетевого трафика и усложнению архитектуры корпоративных сетей. Одновременно возрастает количество угроз, способных нарушить функционирование организаций, скомпрометировать данные или причинить экономический ущерб. В этих условиях обеспечение безопасного межсетевого взаимодействия и надёжного контроля трафика становится одной из ключевых задач в сфере информационной безопасности.

Усложнение сетевой инфраструктуры сопровождается ростом интенсивности киберугроз, что подтверждается актуальной статистикой. В конце 2024 и начале 2025 года 66 % успешных атак были связаны с использованием вредоносного программного обеспечения, среди которого наиболее распространёнными стали шифровальщики (42 %) и программы удалённого управления (38 %). Также наблюдается увеличение применения шпионского ПО, доля которого достигла 20 %. В 53 % случаев атаки приводили к утечке конфиденциальной информации, а в 32 % — к нарушению бизнес-процессов [1]. Эти угрозы тесно связаны с уязвимостями в системе межсетевого взаимодействия. Проникновение вредоносных программ в корпоративную сеть и их последующая коммуникация с внешними серверами управления возможны только при отсутствии должного контроля, фильтрации и мониторинга сетевых соединений. Дополнительную опасность создают устройства, подключаемые к сети без надлежащей защиты и централизованного управления. Согласно отчёту за 2024 год, количество уязвимых IoT-устройств в корпоративных сетях выросло на 136 % по сравнению с 2023 годом — с 14 % до 33 % от всех выявленных уязвимостей. Через такие устройства злоумышленники могут получить несанкционированный доступ, использовать их как точки входа для распространения вредоносного ПО и других угроз [2]. Кроме того, только в 2024 году было зафиксировано более 500 тысяч DDoS-атак, что почти вдвое превышает показатель предыдущего года [3]. Такая статистика свидетельствует о необходимости пересмотра и усиления существующих подходов к защите сетевого взаимодействия.

Актуальность разработки системы межсетевого взаимодействия и контроля трафика обусловлена тем, что значительная часть успешных атак происходит на фоне недостатков в архитектуре защиты: неэффективной фильтрации трафика, отсутствия логической сегментации сети и применения устаревших программных или аппаратных решений, не поддерживающих современные протоколы и политики безопасности. Эти факторы значительно упрощают злоумышленникам доступ к внутренним ресурсам организации. В связи с этим особенно важно проектировать решения, которые изначально учитывают риски конфигурационных уязвимостей и обеспечивают гибкость, масштабируемость и адаптацию к угрозам на разных уровнях сети.

В данной статье рассматриваются современные угрозы безопасности корпоративных сетей и анализируются существующие программные и аппаратные решения для их защиты. Целью является разработка оптимальной модели межсетевого взаимодействия и контроля трафика, способной обеспечить многоуровневую защиту корпоративной сети от внешних и внутренних угроз.

Основная часть. Корпоративная сеть среднего масштаба представляет собой инфраструктуру организации, объединяющую примерно от 100 до 1000 пользователей, а также различные устройства и удалённые офисы. Для такой сети характерна распределённая структура и повышенные требования к безопасности. В этом контексте критически важным становится выстраивание эффективного межсетевого взаимодействия — одного из базовых компонентов, обеспечивающих связность и защищённость всей сети. Межсетевое взаимодействие — это организация согласованного обмена данными между разными участками сети внутри организации или между различными сетевыми средами. Оно обеспечивает корректную передачу информации между офисами, филиалами и удалёнными сотрудниками с учётом установленных правил. Для обеспечения безопасного межсетевого взаимодействия необходим постоянный контроль сетевого трафика.

Контроль трафика — это совокупность технических и программных мер, направленных на анализ, фильтрацию и управление потоками данных, проходящих через сеть. Он позволяет выявлять аномалии, ограничивать нежелательные подключения и предотвращать распространение угроз. Контроль трафика осуществляется на разных уровнях модели OSI. Модель OSI (Open Systems Interconnection) — это концептуальная семиуровневая модель, описывающая, как данные передаются в компьютерных сетях от одного устройства к другому. В неё входят следующие уровни: физический, канальный, сетевой, транспортный, сеансовый, представления и прикладной. Уровни модели OSI часто обозначаются сокращённо как L1–L7, где «L» означает «Layer» (уровень). Угрозы, с которыми сталкиваются корпоративные сети, могут проявляться на различных уровнях, и для каждой из них необходимы соответствующие средства защиты.

Обзор угроз. Одной из ключевых угроз корпоративных сетей является несанкционированный сетевой доступ. При отсутствии должной фильтрации входящего и исходящего трафика возможны попытки использования злоумышленниками общедоступных уязвимостей, способных нарушить работу корпоративных сервисов или получить доступ к конфиденциальным данным.

Дополнительную опасность представляет подключение к внутренним ресурсам из внешней среды, особенно при удалённой работе или межфилиальном взаимодействии. Если при этом не используются устойчивые механизмы аутентификации или шифрования, данные могут быть перехвачены, а сеть — скомпрометирована.

Опасность представляют и неконтролируемые DNS-запросы. Система доменных имён (DNS — Domain Name System) используется для преобразования текстовых адресов (например, example.com) в числовые IP-адреса, необходимые для маршрутизации трафика в Интернете. Этот механизм лежит в основе большинства сетевых соединений и работает автоматически при каждом обращении к веб-ресурсам. Однако злоумышленники могут использовать DNS-запросы в обход стандартных средств защиты: через них устанавливается связь с командными серверами, загружаются вредоносные компоненты или создаются скрытые каналы для утечки данных. Подобная активность часто маскируется под легитимный трафик, что затрудняет её своевременное обнаружение.

Распределённые атаки типа DDoS (Distributed Denial of Service) являются одними из наиболее серьёзных угроз сетевой безопасности. Атакующий через множество устройств отправляет огромное количество запросов на серверы компании, перегружая их. Цель заключается не в том, чтобы получить доступ или информацию, а именно ограничить возможность использования ресурса [4]. Атакующие используют ботнеты — сети заражённых устройств, которые одновременно посылают трафик, блокируя работу легитимных пользователей. Современные DDoS-атаки отличаются не только масштабом, но и сложностью: они могут быть многоступенчатыми, сочетать различные протоколы и методы. Последствия подобных атак выражаются в недоступности веб-сервисов, простоях бизнес-процессов и, как следствие — в значительных финансовых и репутационных потерях.

Атаки на веб-приложения представляют собой одну из распространённых угроз в корпоративных сетях. Злоумышленники могут использовать уязвимости, возникающие в результате недоработок в логике или реализации веб-приложений, чтобы проникнуть в систему, манипулировать данными или украсть конфиденциальную информацию. Результатом таких атак может стать утечка данных, повреждение информации или компрометация работы всего веб-ресурса.

Масштабной проблемой остаются вредоносные программы, способные скрытно распространяться внутри корпоративной инфраструктуры, используя легитимные протоколы и порты. Они могут долгое время оставаться незамеченными, если отсутствуют системы анализа поведения и обнаружения аномалий. В сочетании с возможностью зашифрованного взаимодействия с внешними серверами это делает такие угрозы особенно опасными.

Внутренние угрозы, включая действия сотрудников — как преднамеренные, так и непреднамеренные — играют значительную роль в обеспечении сетевой безопасности. Подключение неавторизованных устройств к корпоративной сети, использование личных USB-накопителей, обход корпоративных политик безопасности — всё это может стать причиной внедрения вредоносного ПО или создания несанкционированных каналов связи. Особенно опасны устройства интернета вещей (IoT), которые, как правило, не обладают встроенными средствами защиты, но при этом получают прямой доступ к внутренним сегментам сети. К числу таких устройств относятся точки беспроводного доступа, IP-камеры, принтеры и т.д. Они имеют открытые порты, слабые или устаревшие настройки безопасности и используются злоумышленниками как средство проникновения и развертывания атак [2].

Наконец, уязвимости в архитектуре самой сети, такие как использование устаревшего оборудования, отсутствие гибких политик доступа и невозможность развертывания сегментированной защиты, делают корпоративную инфраструктуру особенно чувствительной к сложным и многоступенчатым атакам.

Обзор средств защиты. Для защиты корпоративной сети от угроз необходимо применять комплексный подход. Одним из ключевых элементов защиты является использование межсетевых экранов. Межсетевой экран (МЭ), также известный как фаервол (Firewall), — это система безопасности сети, предназначенная для контроля и мониторинга трафика между различными сетями. МЭ может фильтровать входящий и исходящий трафик на основе заранее заданных правил безопасности, блокируя подозрительные соединения и предотвращая несанкционированный доступ к внутренним ресурсам сети. Современные межсетевые экраны нового поколения (NGFW, Next Generation Firewall) могут защищать почти на всех уровнях модели OSI, а также поддерживают расширенные функции, такие как контроль приложений, глубокий анализ трафика (DPI, Deep Packet Inspection), который позволяет проверять содержимое пакетов для выявления скрытых угроз, а также SSL-инспекцию, которая расшифровывает зашифрованный трафик для обнаружения угроз в защищенных соединениях. Они также интегрируются с различными системами, что позволяет обнаруживать попытки атак на ранней стадии, а логирование сетевой активности даёт возможность оперативного реагирования на инциденты.

Для обеспечения безопасности удалённых подключений необходимо использовать VPN. VPN (Virtual Private Network) — это технология, создающая защищённое виртуальное соединение между устройствами или сетями через общедоступные сети, такие как интернет. Целью VPN является обеспечение безопасного и зашифрованного канала связи для передачи данных между удалёнными пользователями или офисами компании, скрывая реальное местоположение и защищая информацию от перехвата. Сам по себе он не гарантирует полной безопасности, так как обеспечивает защиту в основном на сетевом (L3) и транспортном (L4) уровнях. Поэтому критически важно дополнять его системами, способными контролировать трафик внутри туннелей.

Особое внимание должно уделяться системе DNS-фильтрации, которая играет важную роль в защите корпоративных сетей, обеспечивая контроль за обращениями к внешним интернет-ресурсам. Обычно такая система включает в себя такие функции, как белые и чёрные списки, которые управляют доступом к сайтам, блокируя нежелательные ресурсы или разрешая доступ только к проверенным; категоризацию, которая помогает классифицировать сайты по типам контента и упрощает настройку фильтрации; управление ролями, позволяющее гибко контролировать доступ к интернет-ресурсам для разных групп пользователей в организации; а также безопасный поиск, ограничивающий доступ к опасному или неприемлемому контенту в поисковых системах, что минимизирует риски перехода на вредоносные сайты. Все эти функции работают в комплексе, помогая эффективно защищать корпоративную сеть от угроз, связанных с интернет-ресурсами. Наличие данной системы важно, поскольку даже при наличии межсетевого экрана, система DNS-фильтрации служит дополнительным барьером, предотвращая подключение к сайтам, используемым для распространения вредоносного ПО или утечек данных через DNS-каналы.

Для защиты от DDoS-атак применяются анти-DDoS-системы — специализированные решения, предназначенные для фильтрации и анализа входящего трафика с целью выявления аномалий и блокировки вредоносных запросов. Такие системы часто используют поведенческий анализ, отслеживая отклонения от нормального сетевого поведения, а также статистический мониторинг, фиксируя резкие всплески трафика и другие аномалии. Также широко применяется эшелонированная защита, при которой фильтрация трафика происходит на разных уровнях модели OSI. Анти-DDoS-системы могут размещаться как на периметре корпоративной сети, предотвращая перегрузку внутренних ресурсов, так и за её пределами — в рамках внешних сервисов провайдеров. Важно, чтобы защита была интегрирована с другими средствами безопасности для оперативного выявления угроз и адаптации мер защиты, обеспечивая таким образом многослойную защиту от отказа в обслуживании.

Для защиты веб-приложений от атак, направленных на уязвимости на уровне приложений, используется WAF (Web Application Firewall). Он работает на уровне веб-трафика, фильтруя запросы и блокируя попытки эксплуатации уязвимостей. WAF дополняет другие средства защиты, фокусируясь на специфических угрозах, которые могут возникнуть именно в веб-приложениях, и предотвращая их до того, как они смогут повлиять на работу системы.

На конечных устройствах необходимо использовать антивирусные программы, способные обнаруживать и блокировать вредоносное программное обеспечение, распространяющееся внутри сети. Интеграция антивирусов с централизованной системой управления позволяет отслеживать инциденты безопасности в реальном времени, оперативно реагировать на угрозы и координировать действия по защите всей корпоративной инфраструктуры.

Для более глубокой защиты и раннего выявления вторжений внутри корпоративной сети используются системы IDS (Intrusion Detection System) / IPS (Intrusion Prevention System). Эти системы занимаются анализом и мониторингом трафика в реальном времени, выявляя подозрительное поведение, которое может указывать на активные угрозы, такие как попытки эксплуатации уязвимостей или распространения вредоносного ПО внутри сети. В отличие от других средств защиты, IDS/IPS фокусируются на анализе аномалий и на предотвращении угроз в режиме реального времени, а не на блокировке трафика на уровне приложений или доступа к вредоносным ресурсам. Только 17 % организаций используют IDS/IPS, что ограничивает детекцию внутренних аномалий (например, ботнет-трафик). Эти данные подтверждают актуальность механизмов анализа трафика [5].

Для управления и обработки событий безопасности на уровне всей сети используется система SIEM (Security Information and Event Management). Она собирает и анализирует логи и данные с различных источников (включая IDS/IPS, межсетевые экраны, антивирусы и другие системы), чтобы создать полную картину происходящих инцидентов. SIEM позволяет оперативно реагировать на инциденты, выявлять скрытые угрозы и координировать защиту на уровне всей сети.

Разделение корпоративной инфраструктуры на логические подсети (VLAN, Virtual Local Area Network) с разными уровнями доступа снижает риск распространения вредоносного ПО в случае успешной атаки. Изоляция критически важных элементов позволяет локализовать инциденты и минимизировать потенциальный ущерб. Кроме того, важную роль играет выделение демилитаризованной зоны (DMZ, Demilitarized Zone) — отдельного сегмента сети, куда выносятся публичные сервисы (например, веб-сайты). DMZ изолируется как от внешнего Интернета, так и от внутренней сети, что позволяет снизить риск компрометации основной инфраструктуры в случае атаки на внешние ресурсы. В то время как VLAN обеспечивает сегментацию внутри сети на уровне доступа, DMZ служит буферной зоной между внутренними и внешними соединениями.

Разработка архитектуры защиты. Для создания эффективной и сбалансированной системы межсетевого взаимодействия и контроля трафика в корпоративной сети необходимо учитывать технические аспекты обеспечения безопасности и экономическую целесообразность реализуемых решений. Архитектура должна охватывать ключевые векторы угроз, при этом важно исключать дублирование функционала и избыточность — это позволит сократить расходы на сопровождение без ущерба для защищённости.

В основе любой современной системы межсетевого взаимодействия должен лежать надёжный экран. На российском рынке представлены различные решения, соответствующие актуальным стандартам безопасности, которые могут быть успешно интегрированы в корпоративные сети. Сравнительные данные о функциональных возможностях таких экранов приведены в таблица 1 [6–9].

Таблица 1

Сравнительные данные о функциональных возможностях межсетевых экранов

Межсетевой экран	Основные функции
Континент 4	NGFW, VPN, режим UTM (комбинированный режим МЭ+IPS+DPI+SSL инспекция)
UserGate D	NGFW, SIEM, IDS/IPS, DPI, VPN, антивирусная защита
Рубикон-К	NGFW, IDS/IPS, VPN
Solar NGFW	NGFW, IPS, SSL-инспекция

Среди представленных решений программно-аппаратный комплекс «Рубикон-К» является наиболее сбалансированным вариантом для построения защищённой корпоративной сети. Устройство реализует ключевые функции межсетевого экрана нового поколения, поддерживает IDS/IPS и VPN, что позволяет эффективно защищать как периметр, так и внутренние сегменты сети. Решение сертифицировано и соответствует требованиям по защите информации в большинстве категорий, включая персональные данные и конфиденциальную корпоративную информацию. Хотя «Рубикон-К» не поддерживает DPI или SSL-инспекцию, это не снижает его эффективности в качестве межсетевого экрана. Такие функции полезны, но не являются обязательными для обеспечения надёжной защиты. Благодаря оптимальному соотношению производительности и функциональности, «Рубикон-К» может быть рекомендован в качестве базового элемента сетевой безопасности для предприятий среднего уровня.

Для обеспечения безопасного доступа сотрудников, работающих удалённо или из филиалов, необходим надёжный VPN-сервис. При использовании «Рубикон-К» дополнительное VPN-решение может не потребоваться, поскольку платформа уже включает модули для создания защищённых каналов связи. Однако для более гибкого разграничения прав доступа рекомендуется внедрение специализированного решения, например, ViPNet VPN. Данный VPN обеспечивает защиту корпоративных данных и эффективное шифрование трафика, что гарантирует безопасность от внешних угроз.

Следующим критически важным элементом является контроль и фильтрация обращений к внешним интернет-ресурсам. Для этого применяется система DNS-фильтрации. Среди подходящих для корпоративного использования можно выделить два решения, представленных на российском рынке. Сравнительные данные об их функциональных возможностях приведены в таблица 2 [10, 11].

Таблица 2

Сравнительные данные о функциональных возможностях систем DNS-фильтрации

Системы DNS-фильтрации	Основные функции
SkyDNS Enterprise	Различные политики фильтрации, белые/чёрные списки, категоризация, управление ролями, безопасный поиск, уведомления по угрозам
BI.ZONE DNS	Категоризация, общая статистика, безопасный поиск

Среди представленных решений оптимальным вариантом для корпоративной сети среднего уровня является SkyDNS Enterprise. Система предоставляет гибкие политики фильтрации, поддерживает белые и чёрные списки, категорийный анализ и уведомления о потенциальных угрозах, что делает её эффективным инструментом контроля доступа к внешним ресурсам. SkyDNS Enterprise гарантирует надёжную защиту на DNS-уровне и может быть рекомендована для интеграции в комплексную систему безопасности.

Для противодействия распределённым DDoS-атакам применяются специализированные решения, способные оперативно обнаруживать и блокировать вредоносный трафик, обеспечивая доступность легитимных сервисов. Сравнительные данные о функциональных возможностях этих Anti-DDoS систем приведены в таблице 3 [12–14].

Таблица 3

Сравнительные данные о функциональных возможностях Anti-DDoS систем

Anti-DDoS системы	Основные функции
Kaspersky DDoS Protection	Защита от атак на уровнях L3, L4, L7, поведенческий анализ и статистический мониторинг, защита от высокообъёмных атак
Гарда Anti-DDoS	Защита от атак на уровнях L3–L7, автоматическое подавление атак, расширенные функции фильтрации
Curator.AntiDDoS	Защита от атак на всех уровнях модели OSI, постоянная фильтрация трафика, защита от высокообъёмных атак

Среди современных решений для защиты от DDoS-атак система «Гарда Anti-DDoS» представляет собой оптимальный выбор для корпоративных сетей, предлагая сбалансированную защиту с автоматизацией процессов и многоуровневым охватом. Она обеспечивает комплексную безопасность на всех этапах передачи данных, применяя интеллектуальные алгоритмы для автоматического блокирования атак без нарушения легитимного трафика. Многоступенчатая фильтрация эффективно отражает как массовые, так и целевые угрозы, минимизируя количество ложных срабатываний. Сочетая высокую производительность с гибкостью настроек, «Гарда Anti-DDoS» гарантирует надёжную защиту критически важных сервисов, поддерживая оптимальный баланс между безопасностью и бесперебойной работой сети.

Для повышения эффективности уже развёрнутой системы защиты целесообразно дополнить её архитектуру решением, функционирующим на уровне веб-приложений. В этом контексте наиболее рациональным выбором становится внедрение веб-аппликационного экрана Garda WAF, который органично дополняет используемую платформу «Гарда Anti-DDoS». Совместное применение этих продуктов позволяет формировать двухэшелонную оборону: система противодействия DDoS-атакам отсеивает массовые сетевые угрозы, в то время как WAF обеспечивает углублённый анализ запросов, включая выявление атак на уровне приложений. Garda WAF задействует внешние репутационные базы и сигнатуры вредоносного поведения, что существенно расширяет возможности обнаружения сложных и целевых угроз [15].

Для защиты от вредоносного программного обеспечения на уровне конечных точек необходимо внедрение антивирусного решения. Среди наиболее надёжных и функциональных продуктов, подходящих для корпоративных сетей среднего масштаба, можно выделить Dr.Web Security Space, Secret Net Studio и Kaspersky Endpoint Security. Все три решения обеспечивают необходимый уровень безопасности, включая контроль целостности, защиту от сетевых угроз и централизованное управление, что критически важно при построении масштабируемой системы информационной безопасности [16–18]. Наиболее оптимальным выбором в условиях формирования сбалансированной корпоративной инфраструктуры представляется Kaspersky Endpoint Security — продукт, сочетающий высокую точность детектирования угроз, устойчивость к сложным атакам и широкие административные возможности, сохраняя при этом совместимость с другими средствами сетевой защиты [18].

Для эффективного контроля трафика важно дополнить систему IDS/IPS интеграцией с SIEM-решением. KOMRAD Enterprise SIEM обеспечивает централизованный сбор и анализ событий безопасности в реальном времени, что позволяет выявлять аномалии в трафике и подозрительные активности. Она интегрируется с различными элементами защиты, предоставляя дополнительный уровень мониторинга [19]. Это улучшает защиту не только периметра сети, но и внутреннего трафика, давая предприятиям более эффективные инструменты для управления угрозами и реагирования на инциденты.

Для построения надёжной системы защиты корпоративной сети, способной эффективно противостоять современным киберугрозам, была разработана многоуровневая архитектура, представленная на рис. 1. В её основе лежит комплексный подход, объединяющий различные средства защиты для обеспечения безопасности на каждом уровне сетевого взаимодействия и контроля трафика.

Когда сотрудник (ПК в VLAN 10) вводит адрес веб-сайта, его компьютер отправляет DNS-запрос на DNS-сервер, расположенный в отдельном VLAN для повышения стабильности и безопасности. DNS-сервер для проверки запрашиваемого доменного имени может обращаться к сервису SkyDNS Enterprise. Тот анализирует домен и, если он признан вредоносным или нежелательным, блокирует его разрешение, предотвращая переход пользователя на опасный ресурс. Если доменное имя безопасно, DNS-сервер возвращает соответствующий IP-адрес.

Далее трафик пользователя направляется к NGFW «Рубикон-К». Тот анализирует его на предмет вредоносной активности и применяет настроенные политики безопасности. Если трафик легитимен и соответствует правилам, он пропускается дальше.

Если пользователь пытается получить доступ к публичному веб-серверу, трафик направляется в демилитаризованную зону. Перед попаданием на веб-сервер он проходит через систему «Гарда Anti-DDoS», которая отфильтровывает потенциальные DDoS-атаки, обеспечивая доступность сервиса. Затем трафик анализируется системой «Гарда WAF», проверяющей запросы на наличие веб-специфичных атак. Только легитимные запросы достигают веб-сервера.

Взаимодействие с удалённым работником происходит через зашифрованный туннель, созданный с помощью ViPNet VPN. Весь трафик между компьютером сотрудника и внутренней сетью (например, при доступе к почтовому или файловому серверу) проходит через этот безопасный канал, обеспечивая конфиденциальность.

Взаимодействие с удалёнными филиалами осуществляется через Site-to-Site VPN. Данная технология создаёт зашифрованный туннель между двумя или более локальными сетями через ненадёжную среду (например, интернет). Для организации такого подключения каждый филиал использует маршрутизатор (или NGFW с функциями маршрутизации) — сетевое устройство, которое не только устанавливает VPN-соединение, но и определяет оптимальные пути передачи данных между сетями. Это позволяет удалённым филиалам безопасно обмениваться данными, как если бы они находились в одной физической сети, и получать доступ к ресурсам центральной сети (например, почтовому или файловому серверу), и наоборот. Весь трафик между филиалами и центральным офисом проходит через этот защищённый туннель.

Все события безопасности, происходящие в сети (логи с NGFW, WAF, серверов, рабочих станций и других устройств), собираются и анализируются системой KOMRAD Enterprise SIEM. Она выявляет аномалии и потенциальные инциденты, предоставляя информацию для оперативного реагирования.

В данной архитектуре коммутаторы представляют собой устройства, которые физически объединяют узлы сети (ПК, серверы) и логически разделяют их на VLAN, обеспечивая изоляцию различных групп устройств и повышая безопасность. Взаимодействие между VLAN контролируется NGFW, который осуществляет маршрутизацию и применяет политики безопасности для межсетевого трафика.

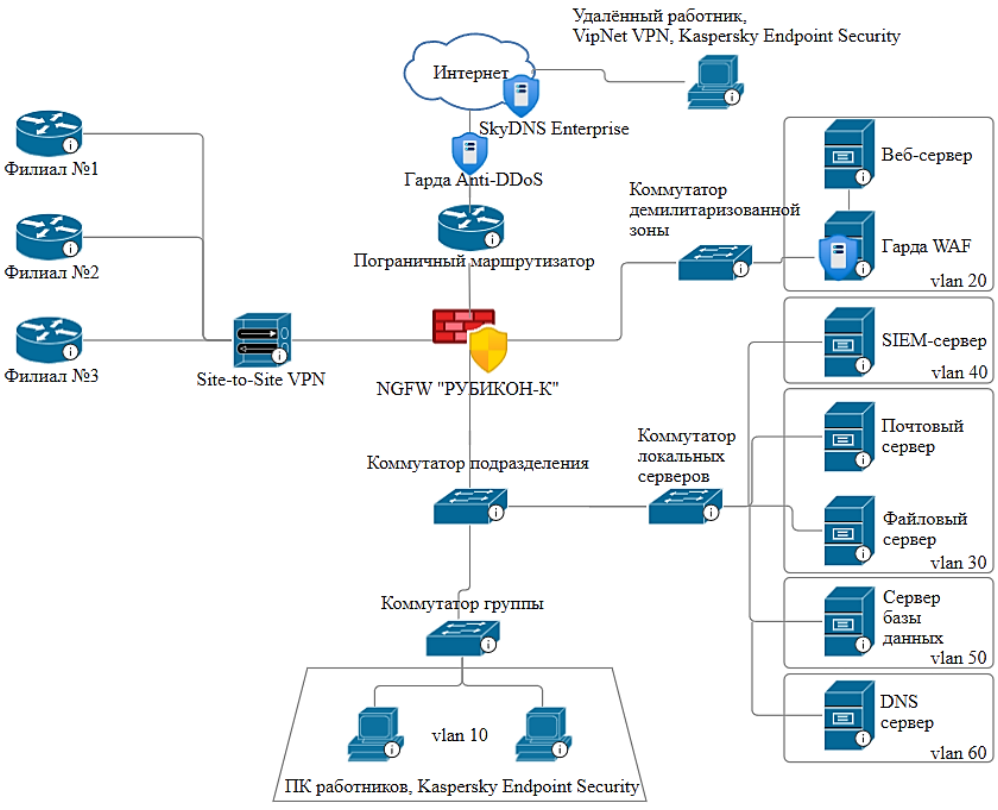

Рис. 1. Архитектура межсетевого взаимодействия и системы контроля трафика

Представленная архитектура формирует эшелонированную систему безопасности, в рамках которой каждый защитный механизм выполняет строго определённую функцию. Применение российских разработок позволяет соответствовать как политике импортозамещения, так и отечественным стандартам в области информационной безопасности. Все выбранные решения отличаются актуальными техническими характеристиками, обеспечивают гибкость настройки политик доступа и отвечают современным требованиям защиты. Они адаптированы для корпоративных сетей, поддерживают необходимые функции и не являются устаревшими, что формирует надёжную основу для построения безопасной инфраструктуры.

Заключение. В рамках исследования проанализированы ключевые угрозы безопасности корпоративных сетей и методы их нейтрализации, включая современные средства защиты, применяемые на различных уровнях инфраструктуры. На основе полученных данных разработана система межсетевого взаимодействия и контроля трафика, обеспечивающая многоуровневую защиту для сетей среднего масштаба. Предложенная архитектура сочетает эффективность и экономическую целесообразность, что позволяет внедрять её в организациях с ограниченными ресурсами без потери надёжности, а также обеспечивает возможность последующего масштабирования в соответствии с потребностями бизнеса.

Список литературы

1. *Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года.* Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (дата обращения 06.12.2025).

2. *What are the Riskiest Connected Devices Right Now?* FORESCOUT. URL: https://www.forescout.com/blog/what-are-the-riskiest-connected-devices-right-now/ (дата обращения: 06.12.2025).

3. *Отчет о DDoS-атаках на онлайн-ресурсы российских компаний в 2024 году.* SOLAR. URL: https://rt-solar.ru/analytics/reports/5364/ (дата обращения: 06.12.2025).

4. Келдыш Н.В. *Системная защита информации компьютерных сетей.* Москва: Издательство «Мир науки»; 2022. 100 с. URL: https://izd-mn.com/PDF/43MNNPU22.pdf (дата обращения: 06.12.2025).

5. Глухов Н.И., Наседкин П.Н. Аналитика внутренних угроз информационной безопасности предприятий. *Доклады Томского государственного университета систем управления и радиоэлектроники.* 2024;24(1):33–41.

6. *Сертифицированный межсетевой экран Континент 4.* Kod-Security. URL: https://kod-security.ru/kontinent-4 (дата обращения: 12.12.2025).

7. *Межсетевой экран следующего поколения.* UserGate. URL: https://www.usergate.com/ru/products/next-generation-firewall (дата обращения: 12.12.2025).

8. *Рубикон-К. Эшелон Технологии*. URL: https://etecs.ru/rubikon-k/ (дата обращения: 12.12.2025).

9. *SOLAR. SOLAR NGFW.* URL: https://rt-solar.ru/products/solar_ngfw/ (дата обращения: 12.12.2025).

10. *SkyDNS. Сокращайте поверхность атаки на первом рубеже*. URL: https://www.skydns.ru/ (дата обращения: 12.12.2025).

11. *BI.ZONE. BI.ZONE. Secure DNS*. URL: https://bi.zone/catalog/products/secure-dns/ (дата обращения: 12.12.2025).

12. *ИТ Энигма. Kaspersky DDoS Protection. Защита от DDoS-атак от «Лаборатории Касперского»*. URL: https://it-enigma.ru/produktyi/zashhita-web-portalov-i-prilozhenij/zashhita-ot-ddos/kaspersky-ddos-protection (дата обращения: 29.12.2025).

13. *Гарда. Гарда Anti-DDoS.* URL: https://garda.ai/products/network-security/ddos-protection (дата обращения: 12.12.2025).

14. *Curator. Curator.AntiDDoS.* URL: https://curator.pro/solutions/ddos#2 (дата обращения: 12.12.2025).

15. *Гарда. Гарда WAF*. URL: https://garda.ai/products/network-security/waf (дата обращения: 12.12.2025).

16. *Dr.WEB. Dr.Web Desktop Security Suite*. URL: https://products.drweb.ru/workstations/ (дата обращения: 12.122025).

17. *Код безопасности. Secret Net Studio*. URL: https://www.securitycode.ru/products/secret-net-studio/ (дата обращения: 12.12.2025).

18. *Selectel Документация. Kaspersky Endpoint Security*. URL: https://docs.selectel.ru/security/server-protection/kaspersky-endpoint-security/ (дата обращения: 29.11.2025).

19. *Эшелон. Технологии. KOMRAD Enterprise SIEM.* URL: https://etecs.ru/komrad_siem/#integration (дата обращения: 12.12.2025).

Об авторе:

Анастасия Алексеевна Сидельникова, студентка кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), sidelnickova.anastasiya2018@gmail.com

Конфликт интересов: **автор заявляет об отсутствии конфликта интересов.**

Автор прочитал и одобрил окончательный вариант рукописи.

About the Author:

Anastasia A. Sidelnikova, Student of the Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), sidelnickova.anastasiya2018@gmail.com

Conflict of Interest Statement: **the author declares no conflict of interest.**

The author has read and approved the final manuscript.