Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.53

КОВАЛЬКО
Ольга Александровна

ИССЛЕДОВАНИЕ СПОСОБОВ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАБОТЫ СЕТИ VPN

Автореферат
на соискание степени магистра
по специальности 7-06-0611-06 Системы и сети инфокоммуникаций

_____

Научный руководитель
Кандидат технических наук, доцент
ХАЦКЕВИЧ Олег Александрович

_____

Минск 2026

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема диссертационной работы соответствует пункту 1 приоритетных направлений научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 гг., утвержденных Указом Президента Республики Беларусь № 156 от 7 мая 2020 г. «Цифровые информационно-коммуникационные и междисциплинарные технологии, основанные на их производстве».

Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Целью диссертационной работы является исследование способов повышения эффективности работы сети VPN путем внедрения технологии виртуальных частных сетей при построении корпоративной сети ООО «НИСИД».

Для достижения поставленной цели необходимо решить следующие задачи:

1 Проанализировать отечественные и зарубежные литературные источники по способам повышения эффективности работы сети VPN.

2 Провести исследование и анализ современных технологий реализации сетей VPN.

3 Выполнить проектирование виртуальной частной сети.

4 Выбрать оборудование для модернизированной сети.

5 Разработать сценарии работы сети VPN с помощью программного средства.

6 Осуществить расчет и исследования показателей виртуальной частной сети.

7 Провести анализ результатов моделирования.

Личный вклад соискателя ученой степени

Содержание диссертации отображает личный вклад автора. Он заключается в научном обосновании методов и алгоритмов повышения эффективности работы сети VPN, постановке и проведении экспериментов по исследованию характеристик, оценке эффективности разработанных алгоритмов, обработке и анализе полученных результатов, формулировке выводов.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем

кандидатом технических наук, доцентом Хацкевичем Олегом Александровичем.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы докладывались и обсуждались на 60-ой и 61-й научных конференциях аспирантов, магистрантов и студентов БГУИР, г. Минск.

Опубликование результатов диссертации

По результатам исследований, представленных в диссертации, опубликованы 2 статьи в сборниках материалов 60-й и 61-й научной конференции аспирантов, магистрантов и студентов 2024 г. и 2025 г.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав с выводами по каждой главе, заключения, библиографического списка, одного приложения.

Общий объем диссертационной работы составляет 131 страницу, из них 93 страницы текста, 28 рисунков на 12 страницах, 21 таблица на 5 страницах, список использованных библиографических источников (53 наименования на 4 страницах), 1 приложение на 7 страницах, графический материал на 10 страницах.

Проверка на уникальность

Проведена экспертиза диссертации Ковалько Ольги Александровны «Исследование способов повышения эффективности работы сети VPN» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) в on-line режиме 13.01.2026 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 71,3 %).

ВВЕДЕНИЕ

В условиях цифровизации современного общества информация выступает одним из ключевых ресурсов, обладающих высокой ценностью, что объективно обусловливает необходимость её защиты от несанкционированного доступа, искажения и утраты. Развитие

вычислительной техники и информационно-коммуникационных технологий привело к существенному усложнению процессов обработки и передачи данных, вследствие чего задачи обеспечения информационной безопасности приобрели особую значимость и актуальность.

Актуальность диссертационного исследования определяется тем, что появление и массовое распространение компьютерных систем во второй половине XX в., а также последующее формирование глобальных и корпоративных сетей, сделали проблему защиты информации сопоставимой по значимости с самой информатизацией общества. Современные распределённые сети подвержены множеству угроз, включая сетевые атаки, программные сбои и отказы сетевого оборудования, что напрямую влияет на надежность и безопасность передачи данных.

В научных исследованиях, посвящённых обеспечению доступности информации, особое внимание уделяется комплексному применению механизмов контроля, резервного копирования и дублирования данных. Для поддержания целостности и конфиденциальности информационных ресурсов в сетевых средах широко используются технологии построения защищённых виртуальных каналов, основанные на криптографических методах защиты.

Высокая актуальность изучения возможностей внедрения виртуальных частных сетей (VPN) в корпоративные информационные системы обусловлена рядом факторов. Во-первых, VPN-технологии обеспечивают высокий уровень защиты данных за счёт применения шифрования, что критически важно при передаче конфиденциальной корпоративной информации. Во-вторых, использование VPN существенно снижает вероятность утечки данных и ограничивает несанкционированный доступ к внутренним ресурсам организации. В-третьих, VPN предоставляет сотрудникам возможность безопасного подключения к корпоративной сети независимо от их физического местоположения, что особенно значимо в условиях распространения удалённых и гибридных форм занятости. Кроме того, виртуальные частные сети обеспечивают защищённое взаимодействие между территориально распределёнными офисами, позволяют управлять сетевым трафиком и балансировать нагрузку, а также снижают затраты на создание и эксплуатацию физической сетевой инфраструктуры. Существенным преимуществом VPN является возможность централизованного управления доступом пользователей и сокрытие реальных IP-адресов, что повышает общий уровень защищённости корпоративной сети

Таким образом, внедрение VPN в корпоративную сетевую инфраструктуру представляет собой стратегически обоснованное решение,

направленное на повышение уровня информационной безопасности, гибкости и доступности корпоративных ресурсов при одновременном соблюдении нормативных требований. В условиях трансформации бизнес-процессов и роста доли удалённой работы значимость VPN-технологий продолжает неуклонно возрастать.

Целью диссертационного исследования является внедрение технологии виртуальных частных сетей при построении корпоративной сети ООО «НИСИД».

Для достижения поставленной цели предполагается решение следующих задач:

– проведение анализа отечественных и зарубежных литературных источников, посвящённых повышению эффективности функционирования VPN-сетей;

– исследование и сравнительный анализ современных технологий реализации виртуальных частных сетей;

– проектирование корпоративной VPN-инфраструктуры;

– осуществление расчета и исследования основных показателей функционирования виртуальной частной сети;

– анализ результатов моделирования и оценка эффективности предлагаемых решений.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрены проблемы функционирования корпоративных систем. В связи с этим актуальность исследования потенциала внедрения виртуальных частных сетей (VPN) в корпоративные структуры компаний обусловлена несколькими ключевыми аспектами: VPN-сети обеспечивают высокий уровень безопасности передаваемой информации, что особенно актуально для защиты конфиденциальных корпоративных данных; использование VPN позволяет существенно снизить риски утечки данных, предотвращая несанкционированный доступ к внутренней информации компании; с помощью VPN сотрудники получают возможность подключаться к корпоративной сети независимо от своего местоположения, что крайне важно в условиях растущей популярности гибридных и удаленных режимов работы; удаленные работники благодаря VPN имеют беспрепятственный доступ ко всем необходимым ресурсам компании, включая внутренние базы данных и приложения; при наличии у организации нескольких офисов, VPN обеспечивает безопасное и надежное соединение между ними; VPN способствует управлению трафиком и

распределению нагрузки между различными узлами сети; внедрение VPN-сетей позволяет создать защищённую сеть без необходимости прокладывания физических линий связи, что существенно снижает затраты на развитие инфраструктуры; VPN предоставляет возможность централизованного управления доступом и правами пользователей, что упрощает процессы администрирования безопасности и позволяет оперативно реагировать на потенциальные угрозы; использование VPN позволяет скрыть реальный IP-адрес пользователей, затрудняя проведение атак на корпоративную сеть и повышая общую безопасность компании.

В **общей характеристике работы** показана связь работы с приоритетными направлениями научных исследований, цель и задачи исследования, личный вклад соискателя ученой степени.

В первой главе было выявлено, что в современных реалиях значение корпоративных сетей сложно переоценить, поскольку они представляют собой не только средство обмена данными внутри организации, но и формируют фундаментальную инфраструктуру, необходимую для эффективной работы сотрудников. Главная задача корпоративной сети заключается в обеспечении непрерывного и безопасного обмена информацией, что становится особенно актуальным на фоне стремительного технологического прогресса и повышенных требований к информационной безопасности.

Корпоративная сеть управляется централизованно, что позволяет устанавливать четкие правила и ограничения для пользователей, в основном сотрудников компании. Это обеспечивает более высокий уровень безопасности по сравнению с открытыми сетями, такими как Интернет, где доступ может быть предоставлен любому пользователю. Корпоративные сети могут функционировать как на локальном, так и на глобальном уровне, объединяя филиалы и офисы, расположенные в разных городах и странах.

Процесс создания корпоративной сети включает несколько важных этапов. Первым шагом является тщательное планирование, во время которого анализируются потребности бизнеса, объемы данных, а также требования к скорости передачи информации. Далее следует выбор подходящего оборудования, установление протоколов и стандартов, а также разработка стратегии управления сетью. Все эти аспекты направлены на формирование масштабируемой и надежной инфраструктуры, способной адаптироваться к изменяющимся бизнес-условиям.

Организация защищенного канала передачи данных является одной из ключевых задач, поскольку информация представляет собой ценный ресурс для любой компании. Корпоративные сети должны обеспечивать высокий уровень безопасности и надежности, что нередко требует использования

сложных технологий, таких как VPN. Виртуальные частные сети позволяют создавать зашифрованные каналы для передачи данных, обеспечивая защиту информации от несанкционированного доступа.

Однако корпоративные сети также сталкиваются с определенными трудностями. Одной из основных проблем является сложность и высокая стоимость организации каналов связи, особенно если речь идет об удаленных филиалах. В таких случаях использование существующих глобальных сетей может быть разумным решением, однако при этом следует предусмотреть возможность масштабирования и интеграции новых технологий с уже имеющейся сетевой инфраструктурой.

Кроме того, безопасность остается одной из ключевых проблем при использовании корпоративных сетей. Обеспечение защиты передаваемой информации от возможных утечек и несанкционированного доступа требует внедрения современных методов шифрования и продвинутых систем безопасности. Использование брандмауэров (Firewall) и VPN-систем существенно повышает уровень защиты данных и создает надежное и доверительное соединение между удаленными филиалами компании.

Следует также учитывать, что с ростом мобильности сотрудников и увеличением числа удаленных подключений, потребность в технологиях, обеспечивающих безопасный доступ к корпоративным ресурсам извне, становится все более актуальной. Применение решений, таких как SSL VPN, предоставляет возможность обойтись без установки дополнительных программных клиентов, делая процесс подключения к корпоративной сети более гибким и доступным с различных устройств.

В целом, создание и управление корпоративной сетью представляет собой сложный и многогранный процесс, включающий аспекты, связанные с инфраструктурой, безопасностью, адаптивностью и интеграцией с другими системами. В условиях современного мира, где информация является одним из наиболее ценных ресурсов, особенно важно обеспечить надежную защиту и эффективность функционирования корпоративной сети. Это позволит не только сохранить конкурентные преимущества, но и обеспечить стабильное развитие и функционирование бизнеса.

Во второй главе было проведено исследование и анализ современных технологий реализации сетей VPN. В ходе исследования и анализа современных технологий создания сетей VPN было выявлено, что за последние годы технологии виртуальных частных сетей (VPN) значительно эволюционировали. Этот прогресс обусловлен растущей потребностью пользователей в обеспечении безопасности данных и свободном доступе к информации. Одной из ключевых тенденций является совершенствование

методов криптографического шифрования, что сделало протоколы, такие как OpenVPN и WireGuard, более надежными и актуальными. Их интеграция способствует не только укреплению защиты данных, но и повышению доверия пользователей к используемым VPN-сервисам.

Одновременно с этим наблюдается активное внедрение VPN в облачные технологии, что обеспечивает высокую степень гибкости и масштабируемости, позволяя компаниям разрабатывать децентрализованные сетевые архитектуры. Это особенно важно в условиях растущего спроса на удаленную работу. В современном бизнесе мобильные решения также приобретают все большую значимость, предоставляя возможность сотрудникам подключаться к корпоративным сетям из различных точек мира. Это, в свою очередь, требует оптимизации производительности и безопасности сетей.

В результате проведенного исследования особый интерес вызвал выбор протоколов IGMP и RIP. Их сочетание позволяет обеспечить эффективное управление мультикаст-трафиком и надежную маршрутизацию, что особенно важно для приложений, работающих в режиме реального времени. Протокол IGMP оптимизирует использование сетевой пропускной способности, а RIP, благодаря своей простоте, быстро адаптируется к изменениям в сети, обеспечивая тем самым стабильное и эффективное функционирование VPN-сетей.

Также была выделена технология MPLS L3 VPN, которая обеспечивает эффективное подключение удаленных сетей через общую инфраструктуру. Благодаря использованию коммутации по меткам и высокой степени изоляции трафика, данная технология является одним из самых безопасных решений на рынке. Кроме того, MPLS предоставляет возможности управления качеством обслуживания (QoS), что имеет решающее значение для приложений с повышенными требованиями к стабильности и скорости передачи данных.

В третьей главе было осуществлено проектирование виртуальной частной сети (VPN) в корпоративной сети ООО «НИСИД». Корпоративная сеть ООО «НИСИД» предназначена для организации услуг передачи данных между центральным офисом, филиальной структурой и корпоративными заказчиками на основе сервисов, функционирующих в рамках протокола IP. Интеграция различных клиентских подсетей реализуется посредством транспортировки IP-пакетов через сетевую инфраструктуру оператора связи.

К ключевым функциональным возможностям корпоративной IP-сети относятся:

– обмен данными между отдельными абонентами и территориально распределёнными сегментами корпоративных сетей клиентов на сетевом уровне модели OSI (уровне IP);

– управление качеством обслуживания (QoS) на уровне IP-пакетов с предоставлением разных уровней сервиса, адаптированных под потребности клиента;

– маршрутизация клиентского трафика через инфраструктуру сети оператора;

– формирование и предоставление согласованного адресного IP-пространства для корпоративных клиен.

Топология сети центрального офиса ООО «НИСИД» представлена на схеме (рисунок 1); аналогичная архитектура применяется и во всех филиалах компании.

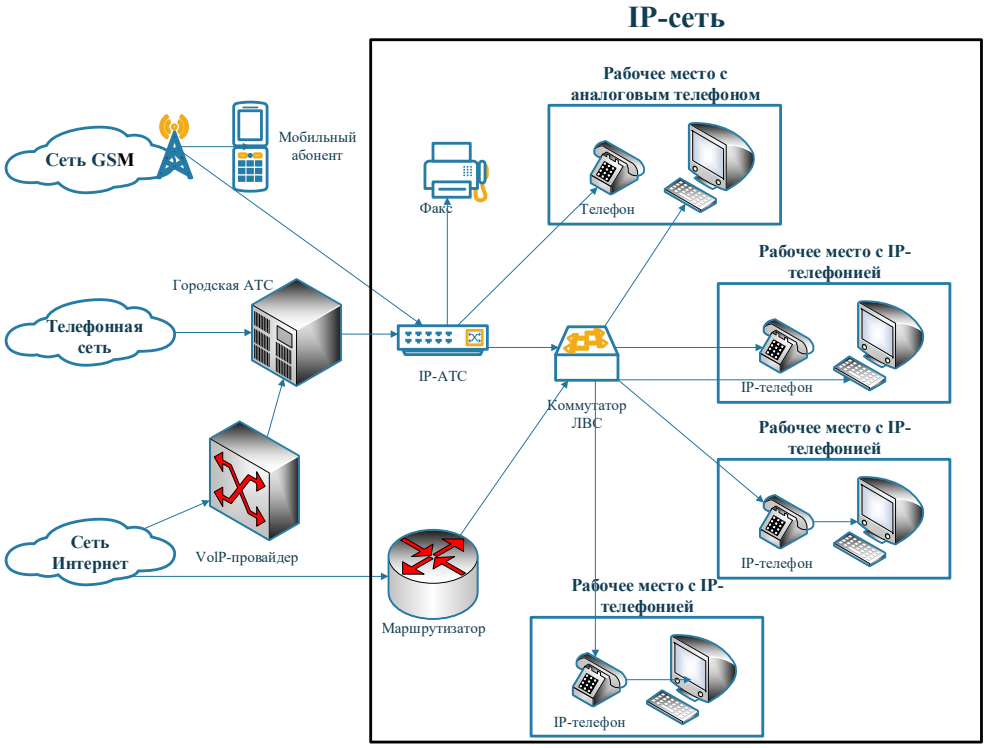


Рисунок 1 – Структурная схема главного офиса ООО «НИСИД» существующей сети

На текущий момент функционирующая сетевая инфраструктура ООО «НИСИД» не обеспечивает требуемого уровня информационной безопасности при передаче данных между корпоративными клиентами и филиалами организации. Для устранения выявленных недостатков планируется внедрение технологии виртуальных частных сетей (VPN). Использование VPN позволяет на базе общей сетевой инфраструктуры, предоставляемой несколькими операторами, формировать сервисы, по своим характеристикам приближенные к услугам частных сетей, включая высокий

уровень безопасности, доступность, стабильную пропускную способность и независимость в выборе схемы адресации.

В рамках диссертационного исследования была осуществлена разработка алгоритма проектирования виртуальной частной сети, состоящий из следующих этапов: определение требований к сети (сбор информации, определение уровня безопасности, анализ существующей инфраструктуры), проектирование архитектуры сети (выбор типа VPN, разработка топологии, определение оборудования), реализация сети (настройка оборудования, проектирование политики безопасности, тестирование конфигурации).

В ходе диссертационного исследования в качестве протоколов для VPN-сети были выделены IGMP и RIP. Протокол IGMP выполняет ключевую функцию в управлении мультикаст-трафиком, что имеет особое значение для сервисов, ориентированных на передачу данных в реальном времени, включая видеоконференцсвязь и потоковую передачу аудио- и видеоконтента. В свою очередь, протокол RIP, характеризующийся относительной простотой конфигурирования и эксплуатации, обеспечивает стабильную динамическую маршрутизацию, позволяя сети оперативно адаптироваться к изменениям топологии.

Поскольку для построения VPN корпоративной сети организации выбран режим Site-to-Site, возникает необходимость модернизации действующей сетевой инфраструктуры с использованием оборудования, поддерживающего соответствующий VPN-функционал. С учётом анализа представленных на рынке решений, а также принимая во внимание производителя уже эксплуатируемых сетевых компонентов, был сделан выбор в пользу оборудования компании Cisco Systems:

– цифровая IP-АТС Cisco BE6000;

– маршрутизатор Cisco 3845;

– коммутатор Cisco Catalyst 2960;

– IP-телефоны Cisco.

Для оценки эффективности функционирования сети VPN было принято решение о проведении имитационного моделирования. Имитационное моделирование является действенным методом повышения эффективности функционирования VPN (виртуальных частных сетей), поскольку позволяет формировать виртуальные представления сетевой инфраструктуры и проводить исследования при различных параметрах и сценариях работы. Применение данного подхода дает возможность изучать поведение сети в искусственно созданной и полностью контролируемой среде, что в реальных условиях часто затруднено из-за финансовых затрат и потенциальных рисков для действующей инфраструктуры.

На основе интегральной оценки в качестве программного продукта для имитационного моделирования был выбран OPNET IT Guru Academic Edition.

Для моделирования частной виртуальной сети (VPN) было проанализировано три различных сценария:

– сеть без защиты;

– сеть с использованием межсетевого экрана;

– сеть VPN с использование межсетевого экрана.

Схема сети VPN с защитой межсетевого экрана представлена на рисунке 2.

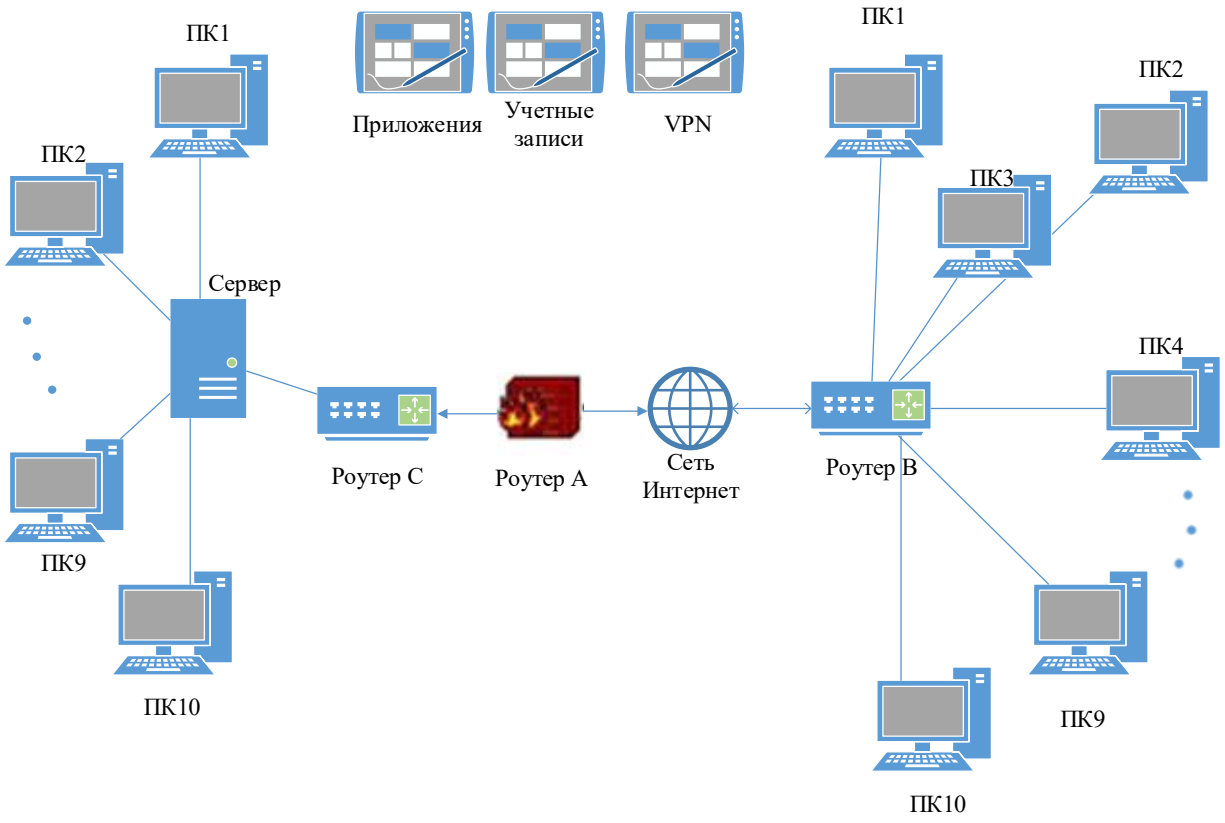


Рисунок 2 – Схема сети VPN с защитой межсетевого экрана

В четвертой главе были осуществлены расчет и исследование показателей виртуальной частной сети компании ООО «НИСИД».

Проектируемая сеть ориентируется на обеспечение потребностей 15 сотрудников с учётом характера и интенсивности их сетевой активности.

В ООО «НИСИД» было выделено 7 сегментов VPN-сети: серверное помещение (первое подразделение); комната № 1 (второе подразделение); комната № 2 (третье подразделение); комната № 3 (четвертое подразделение); комната № 4 (пятое подразделение); комната № 5 (шестое подразделение); комната № 6 (седьмое подразделение).

В рамках расчета объема передаваемых данных проектируемой сети VPN было определено, что для обеспечения стабильной и комфортной работы персонала в проектируемой VPN-сети требуется пропускная способность, позволяющая обрабатывать не менее 3,67 ГБ данных в сутки. При этом необходимо учитывать влияние дополнительных сервисов, возможные пиковые нагрузки, а также резервирование ресурсов для повышения устойчивости и надёжности функционирования сети.

Определение требуемой пропускной способности сети было выполнено с применением метода суммирования, который основан на учёте совокупного объёма трафика, передаваемого через сеть за заданный временной интервал. Расчётное максимальное значение нагрузки на пограничный маршрутизатор составляет 42,6 Мбит/с. При этом данный показатель соответствует ситуации, при которой все сотрудники одновременно используют сетевые ресурсы на предельной пропускной способности. В реальных условиях эксплуатации подобный режим работы встречается крайне редко, что делает экономически нецелесообразным резервирование канала под максимальную нагрузку.

Для более точного анализа параметров канала связи и проверки соответствия сети требованиям QoS целесообразно использовать аппарат теории массового обслуживания (ТМО), позволяющий формализовать процессы обработки сетевого трафика. Выполненные расчёты показали, что оптимальным значением пропускной способности для проектируемой сети является 26 Мбит/с, при котором образование очередей в системе не наблюдается. При увеличении пропускной способности коэффициент загрузки маршрутизатора снижается, что свидетельствует о нерациональном использовании его вычислительных ресурсов и, как следствие, экономической неэффективности такого решения.

В рамках исследования влияния временных задержек в проектируемой сети VPN для проверки корректной работы сети был выполнен расчет времени двойного оборота сигнала (PDV). В качестве базовой технологии использовалась технология Fast Ethernet. В связи с этим было определено, что общее время двойного оборота должно складываться из задержек, возникающих при прохождении через сетевые адаптеры, кабель и концентраторы, и не должно превышать 512 бит, что соответствует времени передачи кадра минимальной длины без преамбулы. В рамках расчета было определено, что двойной оборот сигнала составит 396,3 бит, что соответствует требованиям.

В рамках повышения эффективности работы сети VPN было предложено внедрение технологии Quality of Service (QoS), которая позволит

назначить приоритет критически важным приложениям, таким как видеоконференции и доступ к базам данных. Это обеспечит более стабильную работу сети в периоды пиковой нагрузки и повысит производительность сотрудников при работе с важными ресурсами.

Также следует рассмотреть возможность увеличения пропускной способности канала до 35 Мбит/с (несмотря на то, что ранее оптимальным значением было выбрано 26 Мбит/с) и внедрение механизмов резервирования. Это позволит повысить надежность и устойчивость сети к перегрузкам.

Неотъемлемым элементом обеспечения устойчивости VPN-сети является непрерывный мониторинг ее состояния с использованием специализированных программных средств. Регулярный анализ параметров работы сети позволяет оперативно выявлять отклонения от нормального режима функционирования и своевременно вносить корректировки в конфигурацию.

В целях снижения нагрузки на VPN MPLS канал также предлагается внедрение систем управления трафиком и применение политики QoS (Quality of Service), что обеспечит оптимальное распределение нагрузки между различными сервисами и приложениями, что позволит более эффективно использовать ресурсы. Следующим шагом может стать внедрение виртуализации на уровне отдельных приложений, что обеспечивает сегментацию трафика и сокращение объёма передаваемых данных без нарушения ключевых бизнес-процессов.

В рамках данной работы был настроен виртуальный туннель между маршрутизаторами B и C, а также настроен межсетевой экран для узла 2. Для остальных узлов, с целью проведения эксперимента, защита не была установлена. Также был проведен сравнительный анализ результатов моделирования ранее определенных сценариев, из которых основное внимание уделено двум: работе в корпоративной сети с межсетевым экраном и функционированию сети VPN с использованием межсетевого экрана.

Проведенный анализ статистики входящего трафика на узел 1 показал, что при использовании сценария работы в VPN с защитой межсетевого экрана максимальный входящий трафик на узел 1 главного офиса достигает 14 байт/сек от всех узлов внутри корпоративной сети.

При сценарии только с межсетевым экраном весь трафик из корпоративной сети блокируется полностью. В случае отсутствия защитных механизмов объем входящего трафика из корпоративной сети остается стабильным.

В данной ситуации для эффективной работы сети необходим баланс между безопасностью и доступностью – оптимально использовать гибко

настроенные защитные механизмы, позволяющие контролировать, но не полностью блокировать корпоративный трафик.

Анализ статистики входящего трафика из сети Интернет на узел 1 корпоративной сети главного офиса, было выявлено, что он максимально обрабатывается и частично блокируется при использовании VPN с межсетевой защитой, что свидетельствует о более высоком уровне безопасности в этом сценарии.

При анализе трафика, поступающего на узел 2 из сети Интернет, было выяалено, что сначала активируется защита межсетевого экрана, а затем – виртуальной сети.

Обобщая результаты анализа сценариев с межсетевым экраном и VPN на узле 1 главного офиса, можно сделать вывод, что использование VPN существенно повышает уровень безопасности: максимальный объем поступающего трафика составляет 14 байт/с, при этом трафик из корпоративной сети блокируется полностью. В случае узла 2, при настроенном межсетевом экране, трафик из корпоративной сети проходит без преград, однако при взаимодействии с сетью Интернет защита усиливается. Это подчеркивает важность внедрения мер безопасности и применения защищенных виртуальных туннелей для обеспечения конфиденциальности и надежности корпоративной сети.

ЗАКЛЮЧЕНИЕ

Одним из приоритетных направлений при проектировании корпоративной сети является формирование защищённого канала обмена данными, поскольку информация выступает стратегически значимым ресурсом для любой организации. Современные корпоративные сети обязаны обеспечивать высокий уровень защищённости и отказоустойчивости, что, как правило, достигается за счёт внедрения специализированных технологий, в том числе виртуальных частных сетей (VPN).

В последние годы наблюдается интенсивное развитие VPN-технологий. Существенным направлением данного процесса стало совершенствование криптографических механизмов, благодаря чему такие протоколы, как OpenVPN и WireGuard, получили широкое распространение и признание как надёжные и современные решения. Их использование способствует не только повышению уровня защиты передаваемых данных, но и росту доверия со стороны пользователей к VPN-инфраструктуре в целом.

По результатам проведённого анализа в рамках исследования было обосновано применение протоколов IGMP и RIP. Использование IGMP

позволяет более рационально задействовать пропускную способность сети, тогда как RIP, отличающийся простотой конфигурирования, обеспечивает оперативную адаптацию маршрутизации при изменениях сетевой топологии, что в совокупности способствует стабильной и эффективной работе VPN-сети.

Технология MPLS L3 VPN будет обеспечивать эффективное подключение удаленных сетей через общую инфраструктуру. Благодаря использованию коммутации по меткам и высокой степени изоляции трафика, данная технология является одним из самых безопасных решений на рынке. Кроме того, MPLS предоставляет возможности управления качеством обслуживания (QoS), что имеет решающее значение для приложений с повышенными требованиями к стабильности и скорости передачи данных.

В рамках диссертационного исследования было проведено построение корпоративной сети ООО «НИСИД», которая обеспечивает обмен данными между центральным офисом и филиалами с использованием IP-протоколов. Особое внимание уделялось эффективному управлению трафиком и маршрутизацией, а также адаптации сети к потребностям клиентов посредством внедрения технологии VPN.

В результате был сформирован поэтапный алгоритм проектирования VPN, включающий определение функциональных и технических требований, разработку архитектуры сети и её практическую реализацию. Существенную роль при этом играет детальный анализ бизнес-потребностей организации и состояния текущей инфраструктуры, что позволяет обеспечить соответствие проектируемой сети реальным условиям эксплуатации и требованиям безопасности.

Было установлено, что внедрение технологии VPN обеспечит защищённый доступ к корпоративным ресурсам, сократит расходы и улучшит качество передачи данных. В качестве оптимального решения была выбрана топология сети VPN Site-to-Site, которая обеспечивает надежную защиту трафика и позволяет централизованно управлять сетью, тем самым значительно повышая уровень безопасности и эффективности администрирования.

В ходе исследования был обоснован выбор оборудования для построения VPN-сети с приоритетным использованием решений Cisco, включая маршрутизаторы, коммутаторы и IP-телефоны. Применение оборудования одного производителя обеспечивает высокую степень совместимости компонентов и способствует стабильной работе сети. Дополнительно была обоснована необходимость обновления кабельной системы с целью повышения общей производительности. В частности, принято решение о переходе на витую пару FTP категории 5 (CAT 5), что

позволяет улучшить качество соединения, уменьшить влияние электромагнитных помех и снизить вероятность потери данных. Данная модернизация не только повышает пропускную способность сети, но и обеспечивает более стабильное соединение.

В ходе анализа различных сценариев функционирования корпоративной сети с использованием межсетевого экрана и VPN на узле 1 главного офиса установлено, что при активированном VPN входящий трафик достигает максимального значения 14 байт/с, при этом внутренний корпоративный трафик эффективно фильтруется межсетевым экраном. В условиях отсутствия защитных механизмов объём входящего трафика остаётся неизменным, что указывает на более низкий уровень контроля и безопасности.

Исследование входящего трафика из глобальной сети Интернет на тот же узел показало, что совместное применение VPN и межсетевого экрана обеспечивает более высокий уровень защиты за счёт углублённой фильтрации и блокирования несанкционированных соединений.

На узле 2 при отсутствии защиты внутренний корпоративный трафик проходит без ограничений. Однако при анализе трафика, направленного на узел 2 из сети Интернет, установлено, что первоначально срабатывают механизмы межсетевого экрана, после чего активируются средства защиты VPN.

Таким образом, применение защищённого виртуального туннеля между узлами с использованием маршрутизаторов B и C существенно повышает уровень конфиденциальности и надёжности передачи данных, обеспечивая устойчивое и безопасное функционирование корпоративной сети.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А. Ковалько О. А., Кулешов И. С. Выбор протокола маршрутизации для организации VPN = The choice of the routing protocol for the VPN organization / О. А. Ковалько, И. С. Кулешов // Информационная безопасность: сборник материалов 60-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 22–26 апреля 2024 г. / Белорусский государственный университет информатики и радиоэлектроники – Минск, 2024 – С. 148–151.

2-А. Ковалько О. А., Кулешов И. С. Роль VPN-технологий в повышении безопасности корпоративной сети предприятия = The role of VPN technologies in increasing the security of the enterprise's corporate networ / О. А.

Ковалько, И. С. Кулешов // Информационная безопасность: сборник материалов 61-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 21–25 апреля 2025 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2025. – С. 87–91.