УДК 004.056.5

С.В. Корякин, srgkoryakin1@gmail.com
Институт информационных технологий КГТУ им. И.Раззакова
Институт машиноведения автоматики и геомеханики НАН КР
А.Э. Мергешева, mergesevaalia@gmail.com
Институт информационных технологий КГТУ им. И. Раззакова

АНАЛИТИЧЕСКИЙ ОБЗОР МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА БАЗЕ VPN В РАСПРЕДЕЛЕННЫХ КОРПОРАТИВНЫХ СЕТЯХ

В статье рассматриваются актуальные проблемы обеспечения информационной безопасности в распределенных корпоративных сетях предприятий, включающих территориально удаленные филиалы, подключенные по каналам VPN. Целью исследования является разработка эффективных методов и способов защиты данных в таких сетях. В ходе работы проведен анализ существующих угроз и уязвимостей, связанных с использованием VPN-технологий, а также рассмотрены современные подходы к их нейтрализации. В статье предлагается комплекс мероприятий по повышению уровня безопасности, включающий использование криптографических методов защиты данных, внедрение систем обнаружения и предотвращения вторжений, а также организационные меры по управлению безопасностью информации. Результаты исследования могут быть полезны для специалистов в области информационной безопасности и IT-администраторов, занимающихся обеспечением защиты корпоративных сетей.

Ключевые слова: информационная безопасность, корпоративная сеть, виртуальная частная сеть, распределенная сеть, шифрование данных, предотвращение вторжений, защита данных, меры безопасности, угроза, уязвимость, политики безопасности, безопасность сетевой инфраструктуры, сетевые атаки, контроль доступа, защита от утечек данных, архитектура безопасности, безопасность удаленного доступа, комплексная защита.

В современном мире информационные технологии играют ключевую роль в деятельности предприятий и организаций. С развитием глобализации и распространением корпоративных сетей растет потребность в обеспечении надежной и эффективной связи между головным офисом и территориально удаленными филиалами. В этом контексте технологии виртуальных частных сетей (VPN) становятся неотъемлемой частью инфраструктуры, обеспечивая безопасный и защищенный канал связи через интернет. Однако использование VPN-сетей также приводит к возникновению новых угроз и уязвимостей, которые могут быть использованы злоумышленниками для несанкционированного доступа к корпоративным данным [1,2,3].

Важность разработки и внедрения эффективных методов и способов защиты распределенной корпоративной сети невозможно переоценить. Атаки на информационные системы могут привести к серьезным финансовым потерям, утечке конфиденциальной информации и ущербу репутации компании. В связи с этим цель данной статьи заключается в исследовании существующих угроз, связанных с использованием VPN-сетей, и предложении комплекса мер, направленных на обеспечение безопасности данных в распределенных корпоративных сетях [4,5,6].

В ходе исследования будет проведен анализ современных технологий защиты, включая криптографические методы, системы обнаружения и предотвращения вторжений, а также организационные меры по управлению безопасностью. Основное внимание будет уделено практическим аспектам реализации этих мер в условиях реальной корпоративной инфраструктуры, что позволит минимизировать риски и повысить уровень защиты информации [7].

Настоящая работа ориентирована на специалистов в области информационной безопасности, IT-администраторов и руководителей предприятий, заинтересованных в повышении уровня защиты своих информационных систем и данных. Результаты исследования помогут разработать и внедрить эффективные стратегии и решения для защиты

распределенных корпоративных сетей, обеспечивая надежную работу компании и сохранность её информационных ресурсов [8,9].

Актуальность и проблема комплексной защиты информации

Проблема защиты распределенных корпоративных сетей с использованием VPN актуальна как никогда, поскольку успешные атаки могут привести к серьезным финансовым потерям, репутационному ущербу и утечке критически важной информации. Использование виртуальных частных сетей (VPN) позволяет обеспечить безопасный обмен данными между различными подразделениями компании, однако это также приводит к возникновению новых угроз и уязвимостей. В условиях, когда многие сотрудники работают удаленно, а географически распределенные филиалы подключены через интернет, риск несанкционированного доступа и утечки данных значительно возрастает. Разработка и внедрение эффективных методов защиты таких сетей является неотъемлемой частью стратегии информационной безопасности любой компании, стремящейся защитить свои ресурсы и данные [10].

Принято считать, что информационная безопасность (ИБ) — это комплекс мер и средств, направленных на защиту конфиденциальности, целостности и доступности информации. [11]

ИБ играет важную роль в современном мире, где цифровые технологии проникают во все сферы жизни. Её главная цель — обеспечить надёжную защиту информационных ресурсов от угроз и атак.

Фундаментально информация делится на 2 вида: конфиденциальную и общедоступную.

Конфиденциальная информация может быть разделена на несколько категорий:

- персональные данные
- коммерческие тайны
- интеллектуальная собственность
- профессиональная тайна
- служебная тайна
- государственная тайна
- и другие.

Каждая из перечисленных выше категорий предъявляет разные требования к подходу и стандартам обеспечения информационной безопасности.

На сегодняшний день считается, что угроза информационной безопасности — это совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

Таким образом, угрозы информационной безопасности могут быть классифицированы по различным признакам, например:

По аспекту информационной безопасности, на который направлены угрозы:

- угрозы конфиденциальности (неправомерный доступ к информации);
- угрозы целостности (неправомерное изменение данных);
- угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).

По расположению источника угроз:

- внутренние (источники угроз располагаются внутри системы);
- внешние (источники угроз находятся вне системы).

По размерам наносимого ущерба:

- общие;
- локальные;
- частные.

По степени воздействия на информационную систему:

- пассивные;
- активные.

По природе возникновения:

- естественные (объективные);
- искусственные (субъективные).

В таблице 1 приведены категории угроз информационной безопасности, считающиеся специалистами по ИБ наиболее актуальными на сегодняшний день.

Таблица 1. Категории угроз информационной безопасности

Категории угроз	**Подкатегории**	**Вид**	**Определение**
Внешние угрозы	Кибератаки	Фишинг	Попытки получить конфиденциальную информацию через поддельные сайты или сообщения
		Спуфинг	Подмена данных для маскировки под доверенные источники
		Брутфорс-атаки	Автоматизированные попытки подобрать пароли
		DDoS-атаки	Распределенные атаки, нацеленные на перегрузку и вывод из строя систем
		Man-in-the-Middle (MitM)	Перехват и изменение передаваемых данных между пользователем и сервером
	Вредоносные ПО	Вирусы	Программы, которые могут копировать себя и заражать другие файлы или системы.
		Черви	Вредоносные программы, распространяющиеся через сеть
		Трояны	Вредоносные программы, которые маскируются под легитимное ПО
		Шпионское ПО	Программы, собирающие информацию о пользователе без его ведома
	Социальная инженерия	Фишинг	Поддельные электронные письма или сайты для

			получения личных данных
		Вишинг	Мошенничество с использованием телефонных звонков для получения конфиденциальной информации
		Смишинг	Использование SMS-сообщений для фишинга
Внутренние угрозы	Злоупотребление со стороны сотрудников	Несанкционированный доступ	Использование внутренними сотрудниками своих привилегий для доступа к конфиденциальным данным
		Утечка данных	Преднамеренная или случайная передача конфиденциальной информации третьим лицам
	Ошибки или небрежность сотрудников	Слабые пароли	Использование простых или одинаковых паролей для нескольких систем
		Неправильная конфигурация систем	Ошибки в настройке программного обеспечения или оборудования
		Несвоевременное обновление ПО	Использование устаревшего ПО с известными уязвимостями
Природные и технические угрозы	Физические угрозы	Кража оборудования	Физическое хищение компьютеров, серверов и других устройств
		Пожары и наводнения	Природные катастрофы, которые могут повредить ИТ-инфраструктуру
	Технические сбои	Сбои в электроэнергии	Отключение электричества, приводящее к остановке работы оборудования
		Аппаратные отказы	Поломка компонентов

			компьютеров и серверов
		Сетевые сбои	Проблемы с сетевой инфраструктурой, приводящие к потере связи
Политические и экономические угрозы	Экономические санкции	Санкции	Введение экономических санкций, влияющих на доступность технологий и сервисов
	Шпионаж и саботаж	Шпионаж	Действия, направленные на получение конфиденциальной информации для политических или экономических целей
		Саботаж	Преднамеренные действия, направленные на повреждение или уничтожение ИТ-инфраструктуры

Проводя анализ категорий угроз, представленных в таблице 1 на основе статистических отчетов ведущих экспертов в области ИБ, можно оценить частоту возникновения данных угроз в объектах критической инфраструктуры различных организаций и корпоративных сетях информационных систем (ИС) в процентном соотношении (рис. 1).

Рисунок 1— Возникновение угроз ИБ в объектах КИ

Таким образом, исходя из изложенного выше, имеется возможность определить степени угроз для распределенной корпоративной сети (РКС) ИС организации.

Считается, что в качестве основных угроз для РКС рассматривают:

- Многочисленные вирусные программы: «сетевые черви», «трояны», «вымогатели» и прочие;

- Фишинг-атаки;
- Установка шпионского ПО на оборудование компании;
- Спам;
- Действия неблагонадежных сотрудников, приводящие к внутренней утечке сведений.[12]

На сегодняшний день, по мнению специалистов по ИБ распределённой корпоративной сетью, являются компоненты ИС с территориально распределенной сетевой структурой, объединяющей офисы, подразделения и здания компании, находящиеся на значительном удалении друг от друга и объединенные различными видами каналов связи. Принципы, по которым строится такая сеть, основаны на принципах организации сети передачи защищенных маршрутизируемых данных с заданным уровнем качества обслуживания (рис. 2) [13].

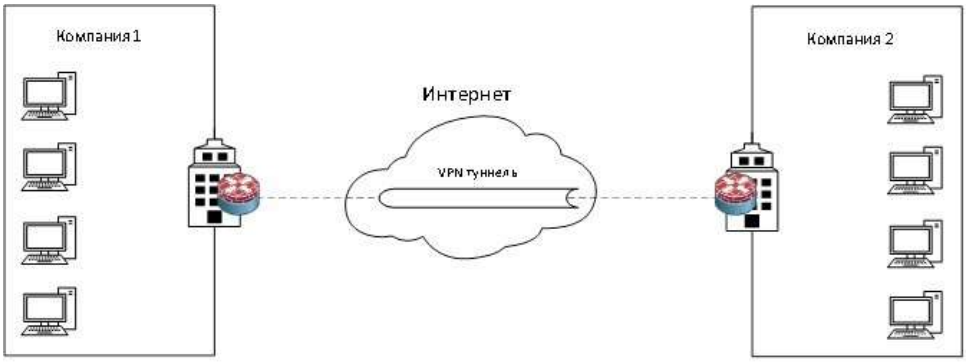

Рисунок 2 — Типовая структурная схема распределенной корпоративной сети

Исходя из рисунка 2, считается, что на сегодняшний день современные предприятия, имеющие распределенную организационную структуру с филиалами, расположенными в разных географических точках, сталкиваются с множеством вызовов в области обеспечения информационной безопасности объектов КИ организаций. Поскольку одна из основных задач специалистов по ИБ – обеспечить безопасную и эффективную передачу данных между географически распределенными филиалами. Рассматривая спектр возможных технических решений для решения поставленной задачи, можно с уверенностью сказать, что решения с использованием технологии «Виртуальные частные сети» (VPN) являются одним из ключевых решений для такого рода задач. Рассмотрим основные методы и способы защиты информации в РКС с использованием технологии VPN[14].

Виды VPN и их особенности

- L2 VPN
  - L2 VPN (Layer 2 VPN) – это технология, позволяющая создать защищенную виртуальную сеть на канальном уровне модели OSI. Она предоставляет возможность построения прозрачной локальной сети между несколькими точками клиента. Основные особенности L2 VPN включают:
    - Закрытая сеть без доступа к интернету: данные передаются только внутри корпоративной сети, что уменьшает риски внешних атак.
    - Изолированный VLAN: каждое подключение имеет свой виртуальный локальный сегмент, обеспечивающий дополнительную изоляцию данных.
    - Простота настройки: первоначальная настройка L2 VPN достаточно проста, что позволяет быстро развернуть сеть.
    - Гибкость конфигурации: возможность изменения и настройки параметров сети в зависимости от потребностей клиента[15].

- L3 VPN
  - L3 VPN (Layer 3 VPN) – это технология, которая работает на сетевом уровне модели OSI. Она позволяет создавать сложные топологии и масштабируемые сети. Основные особенности L3 VPN включают:
    - Закрытая сеть без доступа к интернету: как и в случае с L2 VPN, данные передаются только внутри корпоративной сети.
    - Масштабируемость: L3 VPN позволяет легко добавлять новые узлы и расширять сеть.
    - Удобство управления: изменения в сети согласуются с оператором, что позволяет быстро и эффективно управлять сетью.

Считается, что основными методами защиты информации VPN-сетей являются – шифрование данных, аутентификация, контроль доступа, мониторинг и логирование, защита от DDoS-атак, регулярное обновление программного обеспечения[16].

Шифрование данных. По мнению специалистов по ИБ, одним из основных способов защиты данных в VPN является шифрование. Шифрование обеспечивает конфиденциальность передаваемой информации, делая ее недоступной для третьих лиц. Современные VPN используют различные протоколы шифрования, такие как IPsec и SSL/TLS, обеспечивающие высокий уровень безопасности.

Аутентификация. Аутентификация пользователей и устройств является ключевым элементом безопасности в VPN. Использование многофакторной аутентификации (MFA) значительно повышает уровень защиты, требуя подтверждения личности пользователя с помощью нескольких независимых методов (например, пароль и одноразовый код).

Контроль доступа. Контроль доступа к ресурсам сети позволяет ограничить доступ пользователей только к тем данным и системам, которые им необходимы для работы. Это снижает риск несанкционированного доступа и утечки информации.

Мониторинг и логирование. Постоянный мониторинг и логирование сетевого трафика и событий безопасности позволяют своевременно выявлять и реагировать на инциденты. Использование систем обнаружения и предотвращения вторжений (IDS/IPS) помогает обнаруживать подозрительные активности и предотвращать атаки.

Защита от DDoS-атак. DDoS-атаки (распределенные атаки на отказ в обслуживании) могут серьезно нарушить работу корпоративной сети. Использование специализированных решений для защиты от DDoS-атак позволяет фильтровать вредоносный трафик и поддерживать доступность ресурсов сети.

Регулярное обновление программного обеспечения. Обновление программного обеспечения и прошивок сетевого оборудования позволяет устранять уязвимости и повышать общий уровень безопасности сети. Регулярные обновления помогают защитить сеть от новых видов атак.

Таким образом, можно говорить о том, что использование VPN для объединения распределенных филиалов предприятия предоставляет следующие преимущества:

- Безопасный обмен информацией: шифрование и другие меры защиты обеспечивают конфиденциальность и целостность данных.
- Быстрый доступ к корпоративным приложениям: VPN обеспечивает высокую скорость и надежность соединения, что важно для эффективной работы филиалов.
- Унификация сети: все филиалы объединяются в единую защищенную сеть, что упрощает управление и администрирование.
- Гибкость и масштабируемость: VPN позволяет легко добавлять новые филиалы и расширять сеть без значительных затрат[17].

В таблице 2 представлены основные преимущества и недостатки VPN по сравнению с другими методами защиты информации в РКС. (таб. 2)

Таблица 2 — Сравнительный анализ методов защиты информации в РКС

Методы защиты информации	Преимущества	Недостатки
VPN	• Высокий уровень шифрования данных • Защита от перехвата данных • Безопасный удаленный доступ • Гибкость в масштабировании сети	• Возможные проблемы с производительностью • Сложность настройки и управления • Требует специальных знаний и навыков
Файрволлы	• Контроль доступа к сети • Фильтрация трафика • Защита от внешних атак	• Не обеспечивает защиту данных внутри сети • Может быть обойден опытными злоумышленниками • Ограниченные возможности в защите удаленных пользователей
Антивирусное ПО	• Обнаружение и удаление вредоносного ПО • Защита от вирусов и троянов • Постоянное обновление баз данных	• Не защищает от сетевых атак • Возможны ложные срабатывания • Не защищает передаваемые данные
IDS/IPS	• Обнаружение и предотвращение вторжений • Мониторинг сетевого трафика • Реагирование на аномальную активность	• Возможны ложные срабатывания • Требует настройки и мониторинга • Может не обнаружить новые виды атак
Шифрование данных	• Высокий уровень конфиденциальности • Защита данных при передаче и хранении • Применение в различных системах и приложениях	• Требует управления ключами • Сложность интеграции в существующие системы • Возможные проблемы с производительностью

На рисунке 3 в процентном соотношении представлен анализ преимуществ и недостатков методов защиты информации в РКС.

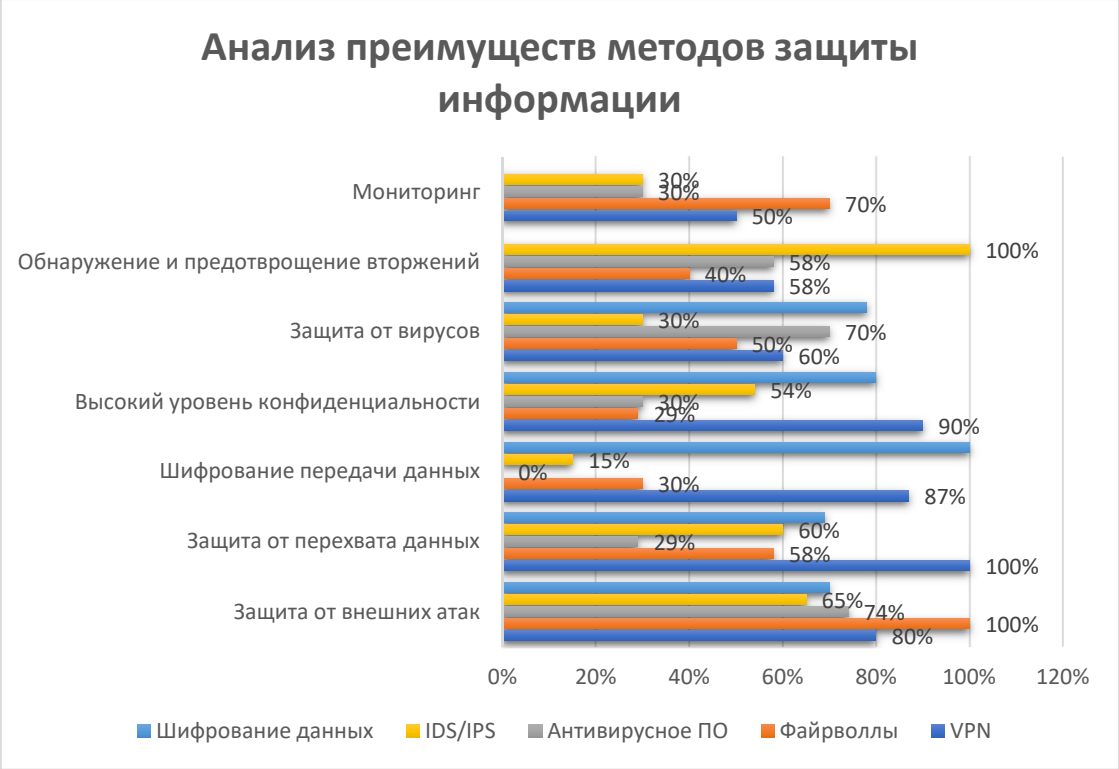

Рисунок 3 —Диаграмма преимуществ методов защиты информации в РКС.

Таким образом, исходя из проведенного анализа, следует выделить основные варианты использования технологии реализации VPN для обеспечения защиты от угроз ИБ в РКС.

1. Site-to-Site VPN

Позволяет соединить несколько офисов в одну защищенную сеть. Каждый офис подключается к центральному серверу через VPN, создавая туннель для передачи данных.

2. RemoteAccess VPN

Обеспечивает доступ удаленных сотрудников к корпоративной сети. Каждый сотрудник подключается к сети через VPN-клиент, что позволяет безопасно работать из любой точки мира.

3. MPLS VPN

Использует технологию мультипротокольной коммутации по меткам (MPLS) для создания виртуальных сетей поверх существующей инфраструктуры оператора связи. Обеспечивает высокую скорость и надежность соединений.

4. Cloud VPN

Обеспечивает защищенное соединение между корпоративной сетью и облачными сервисами. Позволяет безопасно использовать ресурсы облачных провайдеров[18].

В таблице 3 представлен сравнительный анализ вариантов использования реализации технологий VPN в РКС.

Таблица 3 — Сравнительный анализ вариантов использования реализации технологий VPN в РКС

Тип VPN	Преимущества	Недостатки
Site-to-Site VPN	• Объединяет несколько офисов в единую сеть • Высокий уровень безопасности	• Требует сложной настройки и поддержки • Возможны проблемы с производительностью

	• Простота управления для больших сетей	• Зависимость от стабильности интернет-соединения
Remote Access VPN	• Обеспечивает безопасный доступ для удаленных сотрудников • Удобство использования • Гибкость и масштабируемость	• Может замедлять работу при высоких нагрузках • Требует установки и настройки VPN-клиентов • Зависимость от стабильности интернет-соединения
MPLS VPN	• Высокая скорость и надежность соединений • Поддержка качественного обслуживания (QoS) • Хорошая масштабируемость	• Высокая стоимость • Зависимость от провайдера услуг • Сложность настройки и управления
Cloud VPN	• Обеспечивает безопасный доступ к облачным сервисам • Гибкость и масштабируемость • Удобство интеграции с облачными провайдерами	• Зависимость от стабильности интернет-соединения • Возможные проблемы с совместимостью • Требует дополнительных мер безопасности для защиты данных в облаке

На рисунке 4 в процентном соотношении представлен анализ преимуществ и недостатков каждого из предоставленных вариантов реализации технологий VPN в РКС.

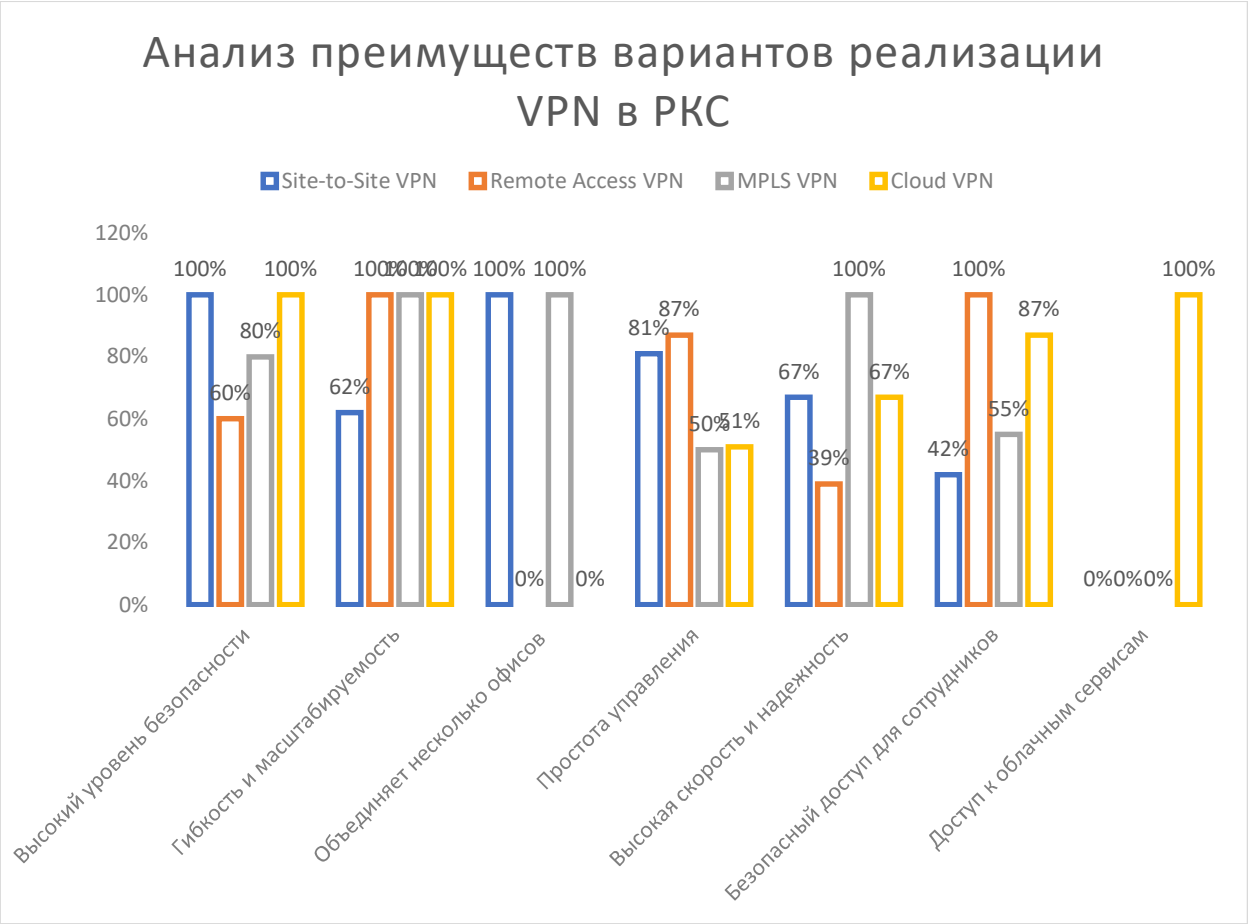

Рисунок 4 — Диаграмма преимуществ вариантов реализации VPN в РКС

Таким образом, можно говорить о том, что использование технологии VPN для защиты распределенных корпоративных сетей позволяет обеспечить достаточно высокий уровень обеспечения безопасности, передаваемой между географически распределенными объектами КИ организации, сохраняя конфиденциальность и целостность данных. Применение различных методов и способов защиты, таких как шифрование, аутентификация, контроль доступа, мониторинг, защита от DDoS-атак и регулярное обновление программного обеспечения, помогает надежно защитить распределенные корпоративные сети и обеспечить их стабильную работу[19].

Исходя из результатов проведенного анализа, можно говорить о том, что технология L3 VPN (Layer 3 VPN) представляется наилучшим выбором для реализации мер защиты от угроз ИБ в большинстве корпоративных сетей ИС с территориально распределёнными филиалами.

Следует отметить, что L3 VPN (Layer 3 VPN) имеет следующие преимущества над другими вариантами реализации технологий VPN:

- Обеспечивает высокую масштабируемость, что важно для растущих компаний.
- Предоставляет возможность управления сложными сетевыми топологиями.
- Обеспечивает высокий уровень безопасности за счет закрытой сети и современных протоколов шифрования.

Говоря о вариантах реализации технологий VPN в целом, следует отметить тот факт, что и другие рассмотренные в работе варианты реализации технологии VPN могут на достаточно высоком уровне выполнять задачи по обеспечению защиты от угроз ИБ, например, MPLS VPN также может быть отличным выбором для крупных предприятий, которым требуется высокая скорость и надежность соединений, несмотря на высокую стоимость и зависимость от провайдера услуг.

Для компаний, активно использующих облачные сервисы, Cloud VPN будет лучшим вариантом, обеспечивая безопасное соединение с облачными ресурсами и гибкость в масштабировании.

Таким образом, необходимо отметить, что выбор конкретного вида VPN как способа реализации мер защиты от угроз ИБ зависит от специфических потребностей компании или организации, её организационной структуры, формы управления и бюджета.

Список литературы

1. Войтович, И.А., и Лашкевич, А.Н. (2019). "Основы информационной безопасности: учебное пособие". — Москва: Изд-во МИФИ.
2. Гостев, С.В., и Лукьянов, С.А. (2020). "Современные методы криптографии: учебник для вузов".— Санкт-Петербург: Питер.
3. Щеглов, А.В., и Романов, Д.Е. (2018). "Системы обнаружения и предотвращения вторжений: теория и практика". — Новосибирск: НГТУ.
4. Орешкин, М.В., и Волков, В.А. (2017). "Защита информации в корпоративных сетях".— Москва: Академия.
5. Белкин, Н.Н., и Иванов, И.И. (2021). "Принципы и методы информационной безопасности".— Казань: КФУ.
6. Норман, Д., и Карлсон, М. (2016). "Практическое руководство по сетевой безопасности". — Минск: Вышэйшая школа.
7. Кириллов, С.И., и Попов, М.С. (2022). "Виртуальные частные сети (VPN): теория и практика". —Томск: Изд-во ТГУ.
8. Рейн, А.С., и Зайцев, В.В. (2019). "Кибербезопасность в цифровую эпоху". —Екатеринбург: УрФУ.
9. Лебедев, А.П., и Соловьев, П.А. (2018). "Многофакторная аутентификация и её применение". — Уфа: БГУ.
10. Титов, Е.Л., и Петров, Ю.Н. (2017). "Методы шифрования данных: теория и практика". — Волгоград: ВолГУ.
11. Информационная безопасность и зачем она нужна (cloudseller.ru)
12. Защита корпоративных данных - как защитить коммерческую информацию (it-usluga.ru)
13. Распределённые сети передачи данных - АБАК – системный интегратор (abak.ru)
14. Построение корпоративной распределенной сети (telecomsite.ru)
15. VPN (lankey.ru)
16. Корпоративные сети связи – VPN для бизнеса (bn.by)
17. Организация корпоративных сетей предприятий - IT-Lite
18. Корпоративный VPN - решение является обязательной частью распределенной корпоративной сети, обеспечивающее конфиденциальность и целостность данных, передаваемых по каналам связи за пределами контролируемых зон объектов. (akontech.ru)
19. Защищённая распределённая корпоративная сеть (azone-it.ru)