Шмидт А.А. Исследование преимуществ использования защищенных локальных сетей передачи данных// Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 1(51) с. 176–180

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.738: 004.897

ИССЛЕДОВАНИЕ ПРЕИМУЩЕСТВ ИСПОЛЬЗОВАНИЯ ЗАЩИЩЕННЫХ ЛОКАЛЬНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Шмидт А.А.
ООО "ГАЗПРОМ ДОБЫЧА ЯМБУРГ", Новый Уренгой, Россия (629306, Ямало-Ненецкий автономный округ, город Новый Уренгой, ул. Геологоразведчиков, д.9); ФГБОУ ВО "СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ", Новосибирск, Россия (630102, Новосибирская область, город Новосибирск, ул. Кирова, д. 86), e-mail: a.shmidt@yamburg.gazprom.ru

Статья посвящена исследованию преимуществ использования защищённых локальных сетей передачи данных. Отмечается, что защищенные локальные сети передачи данных представляют собой эффективное средство обеспечения безопасности и конфиденциальности информации. Автор приводит преимущества использования ЗЛС, выделяет основные компоненты защищённых локальных сетей. В завершение автор делает вывод о том, что использование защищённых локальных сетей передачи данных — это не просто вопрос технологического прогресса, но необходимость в условиях современного информационного мира. Преимущества, такие как защита конфиденциальности, предотвращение несанкционированного доступа, повышение надёжности и соответствие законодательным требованиям, делают защищённые ЛС неотъемлемой частью инфраструктуры любой успешной организации.

Ключевые слова: Защищенные локальные сети, передача данных, конфиденциальность, кибератака, шифрование, защита, контроль, угрозы безопасности.

EXPLORING THE BENEFITS OF USING SECURE LOCAL DATA NETWORKS

Schmidt A.A.
GAZPROM DOBYCHA YAMBURG LLC, Novy Urengoy, Russia (629306, Yamalo-Nenets Autonomous Okrug, Novy Urengoy, Geologorazvedchikov St., 9);
SIBERIAN STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS, Novosibirsk, Russia (86, Kirova st., Novosibirsk, Novosibirsk region, 630102, Russia), e-mail: a.shmidt@yamburg.gazprom.ru

The article is devoted to the study of the advantages of using secure local data networks. It is noted that secure local data transmission networks are an effective means of ensuring the security and confidentiality of information. The author cites the advantages of using a VPN, highlights the main components of secure local area networks. In conclusion, the author concludes that the use of secure local data transmission networks is not just a matter of technological progress, but a necessity in the modern information world. Advantages such as privacy protection, prevention of unauthorized access, increased reliability and compliance with legal requirements make secure personal data an integral part of the infrastructure of any successful organization.

Keywords: Secure local area networks, data transmission, confidentiality, cyberattack, encryption, protection, control, security threats.

Цель исследования – установить преимущества использования защищённых локальных сетей передачи данных. Проблема исследования состоит в том, что в наше время, когда информация становится одним из самых ценных ресурсов, вопросы её безопасности выходят

на первый план. В условиях стремительного развития технологий и увеличения количества киберугроз обеспечение безопасности данных становится особенно актуальным. Одним из решений для повышения безопасности передачи данных является использование защищённых локальных сетей. Методология исследования включает в себя анализ отечественной и зарубежной научной литературы[1].

Защищённая локальная сеть передачи данных — это сеть, которая использует специальные меры и технологии для обеспечения конфиденциальности, целостности и доступности передаваемой информации. Основная цель таких сетей — минимизация рисков, связанных с угрозами, которые могут возникнуть в процессе передачи и хранения данных. Защищённые ЛСПД могут быть реализованы как в рамках организации, так и между различными организациями. Основные компоненты защищённых локальных сетей:

1. Шифрование данных.
2. Системы аутентификации.
3. Межсетевые экраны и системы предотвращения вторжений.
4. Сегментация сети[2].

Первое и самое очевидное преимущество защищённых локальных сетей – это обеспечение конфиденциальности передаваемой информации. Использование шифрования и других методов защиты позволяет избежать несанкционированного доступа к данным. Это особенно актуально для организаций, которые работают с чувствительной информацией, такой как финансовые данные, личные данные клиентов и сотрудники. Защищённые локальные сети значительно снижают риск кибератак. Киберпреступники часто нацеливаются на уязвимости в сетевой инфраструктуре для получения доступа к данным. Применение современных технологий защиты, таких как системы предотвращения вторжений, межсетевые экраны и аутентификация пользователей, делает сети более стойкими к атакам, таким как DDoS, фишинг и других видов киберугроз[3].

Защищённые локальные сети позволяют применять строгие меры контроля доступа к данным. Системы аутентификации и авторизации гарантируют, что только уполномоченные пользователи могут получить доступ к определённым ресурсам. Это значительно снижает риск утечки данных и несанкционированного доступа, так как только определённые сотрудники могут работать с конфиденциальной информацией. Современные системы защищённых локальных сетей часто сопровождаются инструментами для мониторинга и управления сетевым трафиком. Администраторы могут отслеживать активность пользователей, выявлять подозрительные действия и оперативно реагировать на возможные угрозы. Это позволяет не только предотвратить инциденты, но и улучшить общую безопасность сети.

Кибератаки и утечки данных могут привести к значительным финансовым потерям для организаций. Инвестиции в защищённые локальные сети могут помочь избежать высоких затрат, связанных с восстановлением после инцидента, утратой репутации и юридическими последствиями. В долгосрочной перспективе это может значительно уменьшить общие расходы на управление безопасностью[4].

Одним из главных преимуществ защищенных локальных сетей передачи данных является повышенный уровень безопасности. Защита данных важна для предотвращения утечек конфиденциальной информации, хакерских атак и других угроз. Защищенные сети предоставляют возможность шифрования передаваемых данных, авторизации пользователей,

контроля доступа и других методов, обеспечивающих безопасность передачи данных. Защищенные локальные сети также способствуют повышению производительности и эффективности работы предприятия. Благодаря защите данных и их надежной передаче устраняются возможные задержки, сбои и потери информации. Это позволяет сотрудникам работать более эффективно и безопасно, не тратя время на восстановление данных или борьбу с угрозами. Создание защищенных сетей передачи данных также способствует сокращению расходов на обслуживание и поддержку информационной инфраструктуры предприятия. Благодаря надежной защите данных уменьшается вероятность возникновения проблем, снижается риск потери информации и снижаются затраты на устранение последствий нарушений безопасности.

Еще одним важным преимуществом защищенных локальных сетей передачи данных является обеспечение соблюдения законодательства и нормативных требований по защите данных. В современном мире все чаще встречаются случаи нарушения конфиденциальности информации и утечек данных. Защищенные сети позволяют предотвратить подобные ситуации и обеспечить соблюдение законодательства в области информационной безопасности[5].

Одним из самых эффективных способов защиты информации является шифрование трафика, особенно в рамках защищённых локальных сетей передачи данных. Шифрование трафика — это процесс преобразования данных в такую форму, которая делает их недоступными для несанкционированного доступа. Это достигается с помощью криптографических алгоритмов, которые кодируют информацию, передаваемую по сети. Лишь авторизованные пользователи с соответствующими ключами могут расшифровать и получить доступ к данным. Преимущества шифрования трафика:

1. Защита конфиденциальности: Одним из самых очевидных преимуществ шифрования является обеспечение конфиденциальности передаваемой информации. Это особенно критично для бизнеса, работающего с личными данными клиентов, финансовой информацией и другим чувствительным контентом.

2. Защита от утечек данных: Шифрование снижает риск утечек и несанкционированного доступа к данным. Даже если злоумышленник перехватит трафик, он не сможет расшифровать информацию без доступа к ключам. Это становится особенно важным в условиях растущей киберугрозы.

3. Соблюдение нормативных требований: Во многих странах существуют законы и нормативные акты, требующие защиты данных. Шифрование помогает компаниям соблюдать эти правила, минимизируя риски юридических последствий[1].

В современном мире, где информация становится одним из самых ценных ресурсов, вопросы безопасности передачи данных и оптимизации производительности сетей выходят на первый план. Защищенные локальные сети (ЗЛС) предлагают решение этих задач, обеспечивая не только высокий уровень защиты информации, но и улучшение её обработки. Одной из главных задач любой организации является защита корпоративных данных от несанкционированного доступа. ЗЛС используются для создания безопасного информационного пространства, где данные передаются через защищенные каналы. Основные механизмы защиты включают:

- Шифрование данных: Применение современных алгоритмов шифрования делает информацию недоступной для посторонних лиц. Даже в случае перехвата данных, без ключа шифрования они остаются бесполезными.
- Аутентификация пользователей: Использование многофакторной аутентификации и ограничение прав доступа помогает гарантировать, что только уполномоченные пользователи могут получить доступ к важной информации.
- Системы защиты от вторжений: Интеграция технологий обнаружения и предотвращения вторжений (IDS/IPS) позволяет сразу выявлять и блокировать подозрительную активность в сети.
- Файрволлы и VPN: Защита периметра сети с помощью файрволлов и создание виртуальных частных сетей (VPN) способствуют созданию дополнительного уровня безопасности и позволяют безопасно передавать данные между удаленными офисами и пользователями[6].

Кроме обеспечения безопасности, ЗЛС также способствуют повышению производительности организации. Их преимущества можно выделить следующим образом:

- Оптимизация трафика: Защищенные локальные сети позволяют использовать технологии управления трафиком, что снижает задержки и увеличивает скорость передачи данных. Это особенно важно для приложений в реальном времени, таких как видеоконференции и онлайн-совещания.
- Снижение нагрузки на серверы: Использование ЗЛС позволяет распределять нагрузки между несколькими серверами, что способствует более равномерному распределению ресурсов и увеличивает общую производительность системы.
- Улучшение качества обслуживания (QoS): Современные ЗЛС могут использовать механизмы QoS для приоритизации трафика, что позволяет минимизировать задержки критически важных приложений и сервисов.
- Локализация данных: Хранение и обработка данных в пределах защищенной сети позволяет существенно сократить время доступа к информации и снизить риск потери данных.

Таким образом, защищенные локальные сети передачи данных представляют собой эффективное средство обеспечения безопасности и конфиденциальности информации. Их использование позволяет повысить уровень защиты от киберугроз, обеспечить безопасное подключение к общественным сетям и увеличить производительность сети. Использование защищённых локальных сетей передачи данных — это не просто вопрос технологического прогресса, но необходимость в условиях современного информационного мира. Преимущества, такие как защита конфиденциальности, предотвращение несанкционированного доступа, повышение надёжности и соответствие законодательным требованиям, делают защищённые ЛС неотъемлемой частью инфраструктуры любой успешной организации. Инвестирование в безопасность локальных сетей не только защищает данные, но и создает стабильную основу для роста и развития бизнеса.

Список литературы

1. Визавитин, О. И. Применение современных алгоритмов шифрования при обеспечении информационной безопасности беспроводных локальных сетей / О. И. Визавитин, Д. А. Логинова, С. Д. Таякин. — Текст : непосредственный // Молодой ученый. — 2016. — №

10 (114). — С. 138-142. — URL: https://moluch.ru/archive/114/29954/ (дата обращения: 21.11.2024).
2. Храмов Н.Р. ЗАЩИТА РЕСУРСОВ СЕТЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ VPN // Международный студенческий научный вестник. – 2019. – № 1. ; URL: https://eduherald.ru/ru/article/view?id=19473 (дата обращения: 21.11.2024).
3. Кондратьев А.А., Талалаев А.А., Тищенко И.П., Фраленко В.П., Хачумов В.М. МЕТОДОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК // Современные проблемы науки и образования. – 2014. – № 2. ; URL: https://science-education.ru/ru/article/view?id=12875 (дата обращения: 21.11.2024).
4. Кондратьев А.А., Тищенко И.П., Фраленко В.П. Разработка распределенной системы защиты облачных вычислений // Программные системы: теория и приложения : электрон. научн. журн. — 2011. — № 4 (8). — С. 61-70
5. Морозов А. В., Шахов В. Г. Анализ атак на беспроводные компьютерные интерфейсы // Омский научный вестник. 2012. № 3 (113). С. 323-327.
6. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2015. – С. 193-197.

References

1. Vizavitin O. I., Loginova D. A., Tayakin S. D. Primenenie sovremennykh algoritov kripirovanii pri obespecheniye informatsionnoy bezopasnosti wireless local networks [Application of modern encryption algorithms in ensuring information security of wireless local networks]. — Text : immediate // Young scientist. — 2016. — № 10 (114). — .pp. 138-142. URL: https://moluch.ru/archive/114/29954/ (accessed: 21.11.2024).
2. Khramov N.R. PROTECTION OF NETWORK RESOURCES BASED ON VPN TECHNOLOGY // International Student Scientific Bulletin. – 2019. – № 1. ; Available at: https://eduherald.ru/ru/article/view?id=19473 (accessed: 21.11.2024).Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks. – 2018.
3. Kondratiev A.A., Talalaev A.A., Tishchenko I.P., Fralenko V.P., Khachumov V.M. METHODOLOGICAL SUPPORT OF INTELLIGENT SYSTEMS OF PROTECTION FROM NETWORK ATTACKS. – 2014. – № 2; Available at: https://science-education.ru/ru/article/view?id=12875 (accessed: 21.11.2024).
4. Kondratiev A.A., Tishchenko I.P., Fralenko V.P. Development of a distributed system for the protection of cloud computing. Scientific. Journ. — 2011. — № 4 (8). — pp. 61-70/
5. Morozov A. V., Shakhov V. G. Analysis of attacks on wireless computer interfaces. 2012. № 3 (113). pp. 323-327.
6. Andrianov V. I., Romanov G. G., Shterenberg S. I. Expert systems in the field of information security. – 2015. – pp. 193-197.