***Свиридова Ирина Вячеславовна,***
Ассистент кафедры прикладной информатики
и информационных технологий
НИУ «БелГУ» Россия, г. Белгород
***Sviridova Irina Vyacheslavovna,***
Assistant Department Applied In formatics
and information te chnology
NRU " BelGU" Russia, Belgorod
***Волошкина Елена Викторовна,***
Аспирант кафедры теоретической и экспериментальной физики,
НИУ «БелГУ» Россия, г. Белгород
***Voloshkina Elena Viktorovna,***
Postgraduate student of the Department of Theoretical and Experimental Physics,
NRU "BelGU" Russia, Belgorod
***Цывенко Наталья Валерьевна,***
Преподаватель СПО Инжинирингового колледжа
НИУ « БелГУ» Россия, Белгород
***Tsyvenko Natalia Valerievna,***
VET Teacher at the College of Engineering
NRU "Be lG U" Russia, Belg or od
***Бабенко Анастасия Александровна,***
Аспирант кафедры математического и прикладного программного обеспечения
информационных систем
НИУ « БелГУ» Россия, Белгород
***Babenko Anastasia Alexandrovna,***
Post-graduate student of the Department of Mathematical and Applied
Software of Information Systems

# АНАЛИЗ СУЩЕСТВУЮЩИХ СИСТЕМ УДАЛЕННОГО ДОСТУПА СОТРУДНИКОВ В КОРПОРАТИВНОЙ СЕТИ ПРОМЫШЛЕННОГО ХОЛДИНГА

# ANALYSIS OF EXISTING REMOTE ACCESS SYSTEMS FOR EMPLOYEES IN THE CORPORATE NETWORK OF THE INDUSTRIAL HOLDING

**Аннотация:** в данной статье рассматривается обзор существующих систем удаленного доступа пользоваталей. Проведя анализ было выявлено, что VPN - хорошее средство для удалённого использования всевозможных корпоративных ресурсов и их администрирования.

**Ключевые слова**: удаленный доступ, VPN, работа сотрудников.

**Abstract:** This article provides an overview of existing remote user access systems. After conducting the analysis, it was revealed that VPN is a good tool for remote use of all kinds of corporate resources and their administration.

**Keywords:** remote access, VPN, work of employees.

В настоящее время удалённый доступ активно используется во многих организациях, потому что он просто необходим для тех сотрудников, которые часто работают вне офиса (например, дизайнеры, программисты и др.). Для них открываются возможности удалённого подключения к сети компании, а также появляется доступ к электронной почте, к каким-либо имеющимся сетевым ресурсам и корпоративным активам. В сфере IT удалённый доступ широко применяется для удалённого решения задач администрирования. VPN позволяет обеспечить непрерывность бизнес-процессов, которая, в свою очередь, нужна для того, чтобы не давать конкурентам возможность находить и принимать решение раньше.

Рассматривая подробнее VPN, можно выяснить, что виртуальная частная сеть — это безопасное частное соединение, проходящее через недоверенные общедоступные сети (такие как Интернет), создаваемое с применением протоколов туннелирования и шифрования, которые обеспечивают целостность и конфиденциальность передаваемых данных. Средства криптографии (а также шифрования, аутентификации и инфраструктуры открытых ключей) дают возможность организовать защищенный обмен данными с удалённой локальной сетью через

общедоступную сеть. Как мне кажется, данные VPN-туннелей в общем Интернет-трафике представляют собой поток пакетов специального формата с зашифрованным содержанием. Передача данных через общедоступные сети производится путём формирования потока шифрованного трафика между отправляющей и принимающей стороной, у которых есть публичные(public) IP-адреса и используется оборудование, и программное обеспечение, необходимое для образования шифрованного туннеля, обеспечивающего защиту соединения.

Как правило, между внутренней и внешней сетью компании ставится межсетевой экран. При подключении удалённого пользователя (или при попытке установки соединения с другой защищённой сетью) межсетевой экран потребует прохождения таких процедур, как идентификация и аутентификация. И уже после благополучного прохождения данных процессов, удалённый пользователь (или удаленная сеть) наделяется полномочиями для работы в сети, то есть совершается процедура авторизации. Классифицировать VPN решения возможно согласно нескольким главным характеристикам.

По типу используемой среды: доверительные, защищённые

По способу реализации**:** программное решение, программно-аппаратное решение, интегрированное решение

По назначению:

1. Remote-Access VPN: применяется с целью формирования защищённого канала между сегментом корпоративной сети и пользователем, который, работая удалённо, подсоединяется к корпоративным ресурсам с домашнего компьютера либо, будучи в командировке, подключается к корпоративным ресурсам при помощи ноутбука или даже планшета.

2. Extranet VPN: применяют с целью организации VPN сетей между различными организациями, а также для сетей, к которым подсоединяются пользователи извне.

Построение VPN на базе межсетевых экранов согласно многим источникам, является самым сбалансированным и оптимальным решением для обеспечения комплексной безопасности корпоративной информационной системы от атак из внешних открытых сетей. Через МСЭ, равно как и через маршрутизатор, пропускается весь трафик, следовательно, функции зашифрования исходящего трафика и расшифрования входящего трафика можно возложить и на МСЭ. В настоящее время ряд VPN-решений основывается на расширении МСЭ дополнительными функциями поддержки VPN, что дает возможность установки шифрованного соединения с другим МСЭ через Интернет.

МСЭ многих производителей поддерживают туннелирование и шифрование данных. Любые аналогичные продукты базируются на том, то что в случае если уж трафик идет через МСЭ, то почему бы его попутно не зашифровать. Большая часть МСЭ представляют собой серверное ПО, поэтому актуальный вопрос повышения производительности может быть решен за счёт использования высокопроизводительной компьютерной платформы.

Невзирая на то, что построение VPN на основе МСЭ смотрится вполне грамотным и сбалансированным решением, ему присущи определенные недостатки. В первую очередь, это высокая стоимость подобного решения в пересчете на одно рабочее место корпоративной сети и довольно высокие требования к производительности МСЭ, в том числе и при умеренной ширине полосы пропускания выходного канала связи. Разумеется, что проблеме производительности МСЭ следует уделять повышенное внимание при построении VPN, так как, по сути, вся нагрузка по криптообработке трафика ложится на МСЭ даже в том случае, если требуется объединить в localnet-VPN двух клиентов локальной сети. Также не стоит забывать, что для работы VPN существуют разные протоколы туннелирования и авторизации.

Рассмотрев VPN можно сказать, что VPN - хорошее средство для удалённого использования всевозможных корпоративных ресурсов и их администрирования, которое позволит пользователям удалённо совершенствовать свои практические навыки по работе с программно-аппаратными средствами обеспечения информационной безопасности, а сотрудникам удалённо подключаться к своим рабочим местам.

Подводя итог, нужно сказать, что появление системы удалённого доступа — это большой шаг в развитии мобильности обучения. После завершения работы над у пользователей системы удалённого доступа появилась возможность доступа к внутренним ресурсам. У сотрудников теперь есть возможность удалённого подключения к своим рабочим местам. Системные администраторы имеют возможность удалённого доступа к оборудованию, находящемуся во внутренней сети отделения.

Стоит отметить, что изначально система удалённого доступа проектировалась и внедрялась для студентов. Но со временем практическое применение стало расширяться: у сотрудников появилась потребность в удалённом доступе к своим рабочем местам и им была предоставлена такая возможность. Со временем стало понятно, что удалённый доступ - это удобное средство удалённого администрирования оборудования и системные администраторы получили возможность удалённого доступа в этих целях. Также по определённым причинам потребовался удалённый доступ и к другим отделениям, после чего возможность удалённого доступа стала доступна и для них.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Агальцов, В. П. Базы данных. В 2 книгах. Книга 2. Распределенные и удаленные базы данных / В.П. Агальцов. - М.: Форум, Инфра-М, 2020. - 272 с./ http://www.bookre.org/reader?file=739477

2. Девянин, П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. - М.: Радио и связь, 2020. - 176 с.