Частные сети используются организациями для соединения с удаленными сайтами и с другими организациями. Частные сети состоят из каналов связи, арендуемых у различных телефонных компаний и поставщиков услуг интернета. Эти каналы связи характеризуются тем, что они соединяют только два объекта, будучи отделенными от другого трафика, так как арендуемые каналы обеспечивают двустороннюю *связь* между двумя сайтами. Частные сети обладают множеством преимуществ.

Информация сохраняется в секрете.

Удаленные сайты могут осуществлять обмен информацией незамедлительно.

Удаленные пользователи не ощущают себя изолированными от системы, к которой они осуществляют доступ.

К сожалению, этот тип сетей обладает одним большим недостатком - высокой стоимостью. Использование частных сетей - очень дорогое удовольствие. Используя менее скоростные каналы связи, можно сэкономить деньги, но тогда удаленные пользователи начнут замечать недостаток в скорости, и некоторые из указанных выше преимуществ станут менее очевидными.

С увеличением числа пользователей интернета многие организации перешли на использование виртуальных частных сетей (*VPN*). *Виртуальные частные сети* обеспечивают многие преимущества частных сетей за меньшую цену. Тем не менее, с внедрением *VPN* появляется *целый* ряд вопросов и опасностей для организации. Правильно построенная виртуальная частная *сеть* может принести организации большую пользу. Если же *VPN* реализована некорректно, вся *информация*, передаваемая через *VPN*, может быть доступна из интернета.

**Определение виртуальных частных сетей**

Итак, мы намереваемся передавать через *интернет* секретные данные организации без использования арендуемых каналов связи, по-прежнему принимая все меры для обеспечения *конфиденциальности трафика*. Каким же образом нам удастся отделить свой трафик от трафика остальных пользователей глобальной сети? Ответом на этот вопрос является *шифрование*.

В интернете можно встретить трафик любого типа. Значительная часть этого трафика передается в открытом виде, и любой *пользователь*, наблюдающий за этим трафиком, сможет его распознать. Это относится к большей части почтового и веб-трафика, а также сеансам связи через протоколы telnet и *FTP*. Трафик *Secure* *Shell* (*SSH*) и *Hypertext Transfer Protocol* *Secure* (*HTTPS*) является шифруемым трафиком, и его не сможет просмотреть *пользователь*, отслеживающий пакеты. Тем не менее, трафик типа *SSH* и *HTTPS* не образует виртуальную частную *сеть* *VPN*.

*Виртуальные частные сети* обладают несколькими характеристиками.

Трафик шифруется для обеспечения защиты от прослушивания.

Осуществляется аутентификация удаленного сайта.

Виртуальные частные сети обеспечивают поддержку множества протоколов.

Соединение обеспечивает связь только между двумя конкретными абонентами.

Так как *SSH* и *HTTPS* не способны поддерживать несколько протоколов, то же самое относится и к реальным виртуальным частным сетям. *VPN*-пакеты смешиваются с потоком обычного трафика в интернете и существуют отдельно по той причине, что данный трафик может считываться только конечными точками соединения.

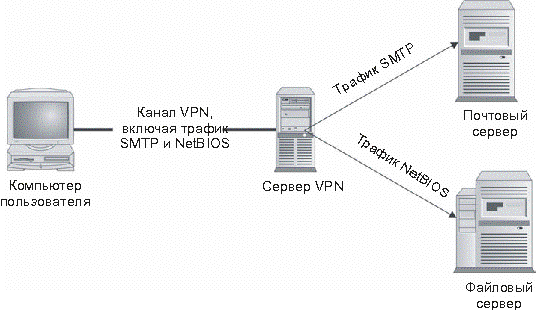
**Примечание**

Возможно реализовать передачу трафика через *сеанс* *SSH* с использованием *туннелей*. Тем не менее, в рамках данной лекции мы не будем рассматривать *SSH* как *VPN*.

Рассмотрим более детально каждую из характеристик *VPN*. Выше уже говорилось о том, что трафик *VPN* шифруется для защиты от прослушивания. *Шифрование* должно быть достаточно мощным, чтобы можно было гарантировать *конфиденциальность* передаваемой информации на тот период, пока она будет актуальна. Пароли имеют срок действия, равный 30 дням (подразумевается политика изменения пароля через каждые 30 дней); однако секретная *информация* может не утрачивать своей ценности на протяжении долгих лет. Следовательно, *алгоритм* шифрования и применение *VPN* должны предотвратить нелегальное *дешифрование* трафика на несколько лет.

Вторая характеристика заключается в том, что осуществляется *аутентификация* удаленного сайта. Эта характеристика может требовать аутентификацию некоторых пользователей на центральном сервере либо взаимную аутентификацию обоих узлов, которые соединяет *VPN*. Используемый механизм аутентификации контролируется политикой. Политика может предусмотреть аутентификацию пользователей по двум параметрам или с использованием динамических паролей. При *взаимной аутентификации* может потребоваться, чтобы оба сайта демонстрировали *знание* определенного общего секрета (под секретом подразумевается некоторая *информация*, заранее известная обоим сайтам), либо могут потребоваться *цифровые сертификаты*.

*Виртуальные частные сети* обеспечивают поддержку различных протоколов, в особенности на прикладном уровне. Например, удаленный *пользователь* может использовать протокол *SMTP* для связи с почтовым сервером, одновременно используя NetBIOS для соединения с файловым сервером. Оба указанных протокола могут работать через один и тот же цикл связи или канал *VPN*



*VPN* соединяет два конкретных объекта, образуя таким образом уникальный *канал связи* между двумя абонентами. Каждая из конечных точек *VPN* может единовременно поддерживать несколько соединений *VPN* с другими конечными точками, однако каждая из точек является отдельной от других, и трафик разделяется посредством шифрования.

*Виртуальные частные сети*, как правило, подразделяются на два типа: пользовательские *VPN* и узловые *VPN*. Различие между ними заключается в методе использования, а не в способе отделения трафика каждым из двух типов сетей. В оставшейся части данной лекции будет детально рассказываться о каждом из типов *VPN*.

**Развертывание пользовательских виртуальных частных сетей**

Пользовательские *VPN* представляют собой *виртуальные частные сети*, построенные между отдельной пользовательской системой и узлом или сетью организации. Часто пользовательские *VPN* используются сотрудниками, находящимися в командировке или работающими из дома. *Сервер* *VPN* может являться межсетевым экраном организации либо быть отдельным *VPN*-сервером. *Пользователь* подключается к интернету через телефонное подключение к локальному поставщику услуг, через канал *DSL* или *кабельный модем* и инициирует *VPN*-соединение с узлом организации через *интернет*.

Узел организации запрашивает у пользователя *аутентификационные данные* и, в случае успешной аутентификации, позволяет пользователю осуществить *доступ* ко внутренней сети организации, как если бы *пользователь* находился внутри узла и физически располагался внутри сети. Очевиден тот факт, что скорость сетевого соединения будет ограничиваться скоростью подключения пользователя к интернету.

Пользовательские *VPN* позволяют организациям ограничивать *доступ* удаленных пользователей к системам или файлам. Это ограничение должно базироваться на политике организации и зависит от возможностей продукта *VPN*.

В то время как *пользователь* имеет *VPN*-соединение с внутренней сетью организации, он также может соединяться и работать с интернетом или выполнять другие действия как обычный *пользователь* интернета. *Сеть* *VPN* поддерживается отдельным приложением на компьютере пользователя 

**Внимание**!

В некоторых случаях *компьютер* пользователя может выступать в роли маршрутизатора между интернетом и сетью *VPN* (и, следовательно, внутренней сетью организации). Этот тип *сетевого атакующего* воздействия необходимо тщательно изучить перед применением пользовательской виртуальной частной сети. Некоторые клиенты *VPN* содержат политику, снижающую риск проявления данной угрозы.

**Преимущества пользовательских VPN**

Пользовательские *VPN* обладают двумя основными преимуществами:

Сотрудники, находящиеся в командировке, могут осуществлять доступ к электронной почте, файлам и внутренним системам в любое время без необходимости в осуществлении дорогостоящих междугородних и международных телефонных вызовов для соединения с серверами.

Сотрудники, работающие из дома, могут осуществлять доступ к службам сети, как и сотрудники, работающие в организации, без аренды дорогостоящих выделенных каналов.

Оба эти преимущества можно приписать к экономии денежных средств. Экономия может заключаться в отказе от использования дорогостоящих междугородних и международных соединений, арендуемых каналов связи или в выполнении сотрудниками задач по администрированию серверов, принимающих входящие телефонные соединения. Домашние пользователи с *DSL* или кабельными модемами могут добиться увеличения скорости при использовании линий телефонной связи со скоростями 56 Кбит/с. Все больше гостиничных номеров оборудуются соединениями для доступа в *сеть*, поэтому для пользователей, находящихся в поездке, создаются все условия для высокоскоростного доступа в *сеть*.

**Примечание**

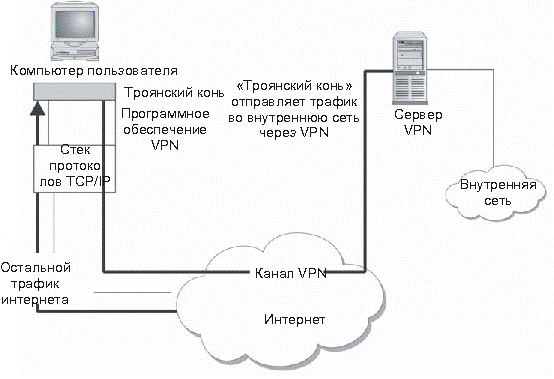
Увеличение скорости через канал 56 Кбит/с не гарантируется. Средняя скорость соединения зависит от *множества* факторов, включая скоростные возможности *интернет*-соединения пользователя, *интернет*-соединения организации, уровень нагрузки интернета, а также число единовременных соединений с *VPN*-сервером.

**Проблемы, связанные с пользовательскими VPN**

Правильное использование пользовательских *VPN* может снизить *затраты* организации, но пользовательские *VPN* не являются решением всех возможных проблем. При их использовании имеют *место* значительные риски, связанные с безопасностью, и проблемы реализации, с которыми приходится считаться.

Возможно, самой большой проблемой безопасности при использовании *VPN* сотрудником является одновременное соединение с другими сайтами интернета. Как правило, *программное обеспечение* *VPN* на компьютере пользователя определяет, должен ли трафик передаваться через *VPN*, либо его необходимо отправить на какой-либо другой *сайт* в открытом виде. Если на *компьютер* пользователя была произведена *атака* с использованием "*троянского коня*", возможно, что некий внешний нелегальный *пользователь* использует *компьютер* сотрудника для подключения к внутренней сети организации (см. [рис. 11.3](https://intuit.ru/studies/professional_skill_improvements/1335/courses/102/lecture/2991?page=2#image.11.3)). Атаки данного типа осуществляются довольно сложно, но они совершенно реальны.

Пользовательские *VPN* требуют такого же внимания к вопросам, связанным с управлением пользователями, как и внутренние системы. В некоторых случаях пользователи *VPN* могут быть привязаны к идентификаторам пользователей в домене *Windows* NT или *Windows 2000* или к другой системе централизованного управления пользователями. Эта возможность упрощает управление пользователями, однако администраторам по-прежнему следует сохранять бдительность и следить за тем, каким пользователям требуется удаленный *VPN*-*доступ*, а каким - нет.



**Внимание**!

Если управление *VPN*-пользователями не связано с центральной системой управления пользователями, этот факт должен учитываться в процедурах управления пользователями, покидающими организацию.

Пользователи должны проходить аутентификацию перед использованием сетей *VPN*. Так как *VPN* позволяет осуществлять удаленный *доступ* ко внутренней сети организации, эта *аутентификация* должна быть двухфакторной, то есть запрашивать два аутентификационных параметра. Одним из параметров может являться сам *компьютер* пользователя. В этом случае вторым параметром должно быть нечто известное пользователю или непосредственно с ним связанное. В любом случае, второй *параметр* не должен находиться на компьютере и не должен быть с ним связан.

В организациях должна приниматься в расчет нагрузка трафиком. Главной точкой нагрузки является *VPN*-*сервер* в узле организации. *Ключевым параметром* нагрузки является ожидаемое число одновременных соединений. При установке каждого соединения *VPN*-*сервер* должен иметь возможность расшифровывать дополнительный трафик. Хотя *процессор* может обеспечивать поддержку больших объемов трафика, он может не обеспечивать *шифрование* и расшифровку большого числа пакетов без значительных задержек. Следовательно, *сервер* *VPN* должен создаваться с учетом ожидаемого числа единовременных соединений.

Еще один момент может повлиять на использование организацией пользовательской *VPN*. Он связан с использованием трансляции сетевых адресов (*NAT*) (для получения дополнительной информации по этой технологии обратитесь к ["Архитектура интернета"](https://intuit.ru/studies/professional_skill_improvements/1335/courses/102/lecture/3001)) на противоположном конце соединения. Если ожидается, что сотрудники организации будут пытаться использовать *VPN* с узлов, защищенных межсетевыми экранами, могут возникнуть проблемы. Например, если организация А является консалтинговой компанией с сотрудниками, работающими в организации Б, в А может возникнуть потребность предоставить своим сотрудникам обратную *связь* для работы с электронной почтой и получения доступа к файлам. Однако, если эти сотрудники работают с компьютеров, входящих в состав внутренней сети организации Б, в которой используется *динамическая* *NAT* для скрытия адресов внутренних систем, это окажется невозможным. Если в вашей организации предпочтение отдается использованию *VPN* именно таким образом, следует проверить возможности программного обеспечения *VPN*.

**Управление пользовательскими VPN**

Управление пользовательскими *VPN*, главным образом, заключается в управлении пользователями и их компьютерами. При разделении сотрудников необходимо выполнять соответствующие процедуры по управлению пользователями.

Разумеется, на компьютерах пользователей должны устанавливаться правильные версии программного обеспечения *VPN* и реализовываться соответствующие конфигурации. Если компьютеры принадлежат организации, это *программное обеспечение* является стандартным компонентом для каждого компьютера. Если организация разрешает сотрудникам использовать *VPN* со своих домашних компьютеров, ей понадобится увеличить общий *уровень поддержки* этих пользователей, так как различные компьютеры и поставщики услуг интернета могут требовать наличие различных конфигураций.

**Совет**

В организациях также может рассматриваться вопрос о предоставлении сотрудникам межсетевого экрана офисного или домашнего уровня. Многие из таких систем могут управляться удаленно, что позволяет организации отслеживать и настраивать системы.

Одним из ключевых аспектов пользовательской *VPN*, о котором не следует забывать, является установка хорошей антивирусной программы на компьютере пользователя. Этот программный пакет должен обеспечивать регулярное обновление своих баз (по крайней мере, ежемесячно) для противостояния вирусам и "*троянским коням*", проникающим на *компьютер* пользователя.