Компьютерные сети

Потребности в компьютерных сетях офиса или комплекса значительно зависят от бюджета, размера, мощности и общих оперативных потребностей организации. Организациям следует изучить возможность найма специализированного ИТ и сетевого персонала для поддержки настройки офисных и подофисных сетей.

Настройка офисов/комплексов

В большинстве случаев в полевых условиях используется несколько видов офисного сетевого оборудования. Сюда может входить:

Подключение к внешнему интернет-провайдеру – подключение к внешнему интернет-провайдеру (ISP) может осуществляться в виде спутникового Интернета, телефонной линии или какой-либо другой формы выделенного подключения к сети, подтвержденной интернет-провайдером.

Модем – модемы принимают сигналы, поступающие от интернет-провайдеров, и преобразуют их в пригодные для использования сигналы по домашним или офисным сетям. Модемы также содержат пользовательскую информацию, которая используется для идентификации, отслеживания и мониторинга трафика в целях безопасности и выставления счетов. Без модема любое домашнее или сетевое оборудование будет неспособно поддерживать связь с внешними сетями.

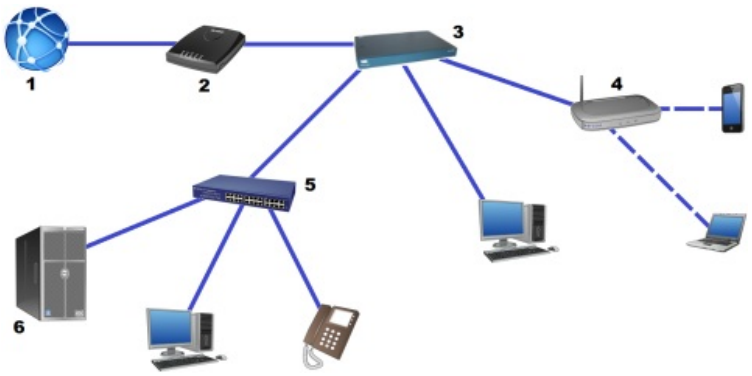
Маршрутизатор – это устройство, которое разделяет и управляет интернет-трафиком, позволяя нескольким вычислительным устройствам иметь свои собственные уникальные IP-адреса и MAC-адреса и одновременно обмениваться данными с Интернетом и друг с другом по сети. Маршрутизаторы имеют различные конфигурации и функции. Некоторые маршрутизаторы могут отслеживать и контролировать трафик в локальной сети, а другие имеют возможность подключения к Wi-Fi. Тип используемого маршрутизатора будет зависеть от эксплуатационных потребностей.

Межсетевой экран – это любое устройство, которое специально отслеживает и фильтрует интернет-содержимое, поступающее из внешних сетей. Межсетевые экраны полезны для предотвращения вредоносного программного обеспечения, случайного несанкционированного вторжения в сети или даже для блокировки содержимого, не разрешенного ИТ-политикой отдельных организаций. В упрощенных сетях межсетевые экраны часто объединяются с модемами или маршрутизаторами, при этом расширенные сети могут иметь автономные межсетевые экраны, которые имеют различные протоколы для разных пользователей сервиса.

Коммутатор – сетевой коммутатор представляет собой усовершенствованную форму маршрутизатора: он контролирует и распределяет Интернет между несколькими сетевыми устройствами, однако коммутаторы способны осуществлять детальный мониторинг и контроль вплоть до уровня отдельных устройств. Коммутаторы также используются для фильтрации, блокировки и защиты внутренних сетей, аналогично межсетевым экранам, защищающим от внешних угроз.

Сервер – это компьютеры, полностью предназначенные для хранения и совместного использования файлов в сети. Серверы могут быть такими же простыми, как обычные настольные компьютеры, или такими же сложными, как большие специализированные вычислительные устройства, предъявляющие особые требования к установке. В последние годы многие организации начали использовать «внешние» серверы, на

которых хранятся и управляются файлы и данные из местоположений, расположенных за пределами офисов, иногда в другой стране. Серверы вне помещений — вполне приемлемые решения, однако, если пользователи сервера имеют нестабильное подключение к Интернету, локализованный сервер может быть предпочтительнее.



1 Внешний интернет-провайдер

2 Модем

3 Маршрутизатор/межсетевой экран

4 Маршрутизатор Wi-Fi

5 Сетевой коммутатор

6 Сервер

Операционная безопасность

Требования к эксплуатационной безопасности каждой из локальных сетей должны соответствовать основным правилам.

Контроль доступа – только уполномоченные лица должны иметь доступ к сетям и вычислительным устройствам. Все компьютеры должны быть защищены паролем, а для маршрутизаторов Wi-Fi также должны требоваться учетные данные. Некоторые сети предоставляют временный гостевой доступ, однако потребности в специальных настройках варьируются в зависимости от операционной среды.

Вредоносное программное обеспечение – все вычислительные устройства в сетях должны иметь ту или иную форму антивирусного программного обеспечения, а операционные системы всегда должны быть обновлены. Организациям следует рассмотреть возможность установки межсетевых экранов и/или коммутаторов с управляемыми настройками, чтобы также сократить попытки вторжения или передачи вредоносного программного обеспечения.

Политика в области ИТ – организациям следует разрабатывать и распространять внутреннюю политику в области ИТ среди всех сотрудников и пользователей сети. Политики в области ИТ должны включать правила и положения о том, что считается приемлемым поведением, каковы правила использования различных типов оборудования, и устанавливать руководящие принципы в случае несоблюдения.