УДК 004.77

КОРПОРАТИВНАЯ СЕТЬ ОДЕССКОГО НАЦИОНАЛЬНОГО ПОЛИТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

Майборода В.О.
к.т.н., доцент кафедры КИСС Шапорин В.О.
Одесский Национальный Политехнический Университет, УКРАИНА

АННОТАЦИЯ. Рассмотрена гибридная и неоднородная ЛВС. Состоит из беспроводных и проводных сетей, что позволяет настроить ее под любые потребности конечного пользователя.

Введение. Wi-Fi является источником повышенного риска несанкционированного доступа. Проникнуть в беспроводную сеть значительно проще, чем в обычную, — не нужно подключаться к проводам, достаточно оказаться в зоне приема сигнала.

В защите Wi-Fi сетей применяются сложные алгоритмические и математические модели аутентификации и шифрования данных, контроля целостности их передачи, тем не менее, вероятность доступа к информации посторонних лиц является весьма существенной. И если при настройке сети не уделить должного внимания, то злоумышленник может:

1. получить доступ к ресурсам и дискам пользователей Wi-Fi сети, а через неё и к ресурсам LAN;
2. прослушивать трафик, извлекать из него конфиденциальную информацию;
3. искажать проходящую в сети информацию;
4. внедрять поддельные точки доступа;
5. рассылать спам и совершать другие противоправные действия от имени Вашей сети.
6. **Цель работы.**
7. Проектирование корпоративной сети для ОНПУ;
8. Обеспечение защиты беспроводной и проводной сети;
9. Обеспечить отказоустойчивость системы.

Основная часть работы.

Данная сеть гибридная, предполагает подключение, как по проводу, так и по WI-Fi. Обеспечивает взаимодействие стационарных ЭВМ и другой устройств при помощи доменной сети. Данные устройства подключаются по кабелю. Данное решение дает возможность гибкой настройки сети. Неоднородность сети обоснована возможностью подключения телефонов, планшетов, возможно IP-телефония и так далее.

Виртуализация ЛВС [1] являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы, несмотря на их физическое размещение в сети. Стоит заметить, что при использовании виртуальных локальных сетей уже не требуется подключать пользователей одного отдела к отдельному коммутатору. Данное решение даст возможность сократить количество используемых устройств и кабелей.

Для данного решения необходимо наличие коммутатор, программное обеспечение которого поддерживает функцию виртуальных локальных сетей, позволяет выполнять логическую сегментацию сети путем соответствующей программной настройки. Это дает возможность подключать пользователей, находящихся в разных сегментах, к одному коммутатору, а также сокращает количество необходимых физических интерфейсов на маршрутизаторе.

Интеллектуальная система управления сетью с использованием SNMP протокола[2]. В процессе функционирования сети возникает необходимость определить определенные параметры некоторого устройства, такие как, например, размер MTU (максимальный объём данных, который может быть передан протоколом за одну итерацию), количество принятых пакетов, открытые порты, установленную на машине операционную систему и ее версию и многое другое. Для осуществления этого как нельзя лучше подходят

SNMP клиенты. Данное решение предоставляет возможность мониторинга всей сети и предотвращения возможных неполадок в сети и их своевременного устранения.

Бесшовный Wi-Fi. Контроллер, который своевременно "направляет" на ваше устройство сигнал с наиболее близко расположенной точки доступа. Данная сеть получила применение только как сеть общего пользования студентами и персоналом.

Для повышения безопасности сети был использован многоуровневый доступ. Система обладает семью уровнями доступа. Первый – самый низкий, а седьмой – самый высокий.

Уровни доступа к сети и краткое описание:

1. Незарегистрированные пользователи:
   1.1. Пользователь(первый);
2. Зарегистрированные пользователи:
   2.1. Студент(второй);
   2.2. Секретарь, администрация(третий);
   2.3. Преподаватель, декан(четвертый);
   2.4. Администратор(пятый);
   2.5. Старший Администратор(шестой);
   2.6. Системные администратор(седьмой).

Защита беспроводной сети [4] обеспечивается трехфакторной аутентификацией: подтверждение MAC-адреса устройства, пароля от своего профиля и наличие устройства, с которого совершается подключение на территории покрытия Wi-Fi сети либо подключение к проводной сети.

Выводы. Данная модель ЛВС актуальна не только для университетов, школ, училищ, но и для крупных частных предприятий. Сеть предусматривает возможное развитие и увеличение вычислительных мощностей. Автоматизация сети обеспечивает: гибкую настройку под каждый из видов задач конечного пользователя, простоту в обслуживании благодаря возможности быстрого обнаружения неполадок и их скорой ликвидации, высокий уровень защиты сети, возможность проверять наличие студента (работника) на территории учебного заведения (предприятия).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Виртуальные локальные сети [Электронной ресурс]. – Режим доступа:
2. URL: https://www.osp.ru/lan/2002/12/136942/
3. SNMP протокол – принципы, безопасность, применение [Электронной ресурс]. – Режим доступа: URL: http://www.codenet.ru/webmast/snmp/
4. Биячуев Т.А. / под ред. Л. Г. Осовецкого Безопасность
5. корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.
6. Защита информационных в компьютерных сетях. /В. Ф. Шангин. Москва: ДМК Пресс, 2012. – 592с.: ил.