Модели угроз локальной сети в учреждении образования

Силич С.С.
гр.267041
Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Шевчук О.Г. – кандидат технических наук, доцент кафедры ИКТ

Аннотация. Сегодня привычным инструментом коммуникаций являются компьютерные сети, что вызывает необходимость обеспечения их безопасности, здесь рассматриваются возможные угрозы и средства обеспечения безопасности локальных сетей.

Ключевые слова: локальная сеть, безопасность, угроза, программное обеспечение.

Введение. Настоящее время характеризуется большим количеством числа компьютеров, связанные между собой с помощью особых каналов, предназначенных для распространения информации и
Одной из основных проблем в ЛС является обеспечение их безопасности. Но, необходимо понимать, что безопасность представляет собой совокупность мер технического, организационного и административного плана, которым требуется регулярная проверка. Не менее важно, что в систему безопасности всегда включены и люди. Поэтому сеть нельзя считать безопасной при отсутствии доверияк персоналу, который с ней работает. Кроме того, абсолютная безопасность локальной сети недостижимав принципе, поскольку даже если к ней допущено крайне ограниченное число доверенных пользователей, существует вероятность, что и среди них отыщется «слабое звено».[1]

Основная часть. Угрозы ЛС можно разделить следующим образом:

Техническая угроза:

- Ошибки в программном обеспечении (ПО), чем сложнее ПО, тем больше вероятность обнаружения ошибок. Большая часть не представляет никакой опасности, но некоторые могут привести к серьёзным последствиям. Действующий способ предотвращению возникших проблем является своевременная установка обновления ПО.

- Различные DoS- и DDoS-атаки. Denial Of Service (отказ в обслуживании) — особый тип атак, направленный на выведение сети или сервера из работоспособного состояния. DoS-атака (Denial of Service) — попытка нарушения или снижения доступности ресурса, как правило, сайта, сетевого сервиса или софта. Задача в том, чтобы перегрузить целевую систему или сделать ее недоступной, приводя к отказу в обслуживании.

- Компьютерные вирусы, черви, троянские кони. Они используют для своего распространения электронную почту, уязвимость в ПО или их совокупность, выполняют функцию похищения информации и использования заряженной системы для своего распространения.

- Технические средства съема информации. Сюда можно отнести такие средства, как клавиатурные жучки, различные мини-камеры, звукозаписывающие устройства и т. д.

- Анализатор трафика, или сниффер (от англ. to sniff — нюхать) — сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

Человеческий фактор:

- Уволенные или недовольные сотрудники.
- Промышленный шпионаж
- Халатность.
- Низкая квалификация.

Данная группа используется в повседневной жизни намного реже вышеперечисленных, так как, кроме наличия спецтехники, требует доступа к сети и ее составляющим. [2]

Заключение. Таким образом, в настоящее время важно быть уверенным в защищённости локальной сети и вовремя выявить возможные угрозы. Знание которых совместно с уязвимыми местами защиты, которые эти угрозы обычно эксплуатируют, необходимо для выбора наиболее экономичных средств обеспечениябезопасности.

Список литературы

1. *Орловская Л.А., Поначугин Л.А., Поначугин А.В. Локальные вычислительные сети // Научное сообщество студентов XXI столетия. Технические науки: сб. ст. по мат. XLII междунар. Студ. Науч.-прак. Конф. – 2016. №5(41). URL:https://sibac.info/archive/techenic/5(41).pdf (дата обращения: 20.004.2018).*
2. *Абраров Р. Д., Курязов Д.А. Информационная безопасность в компьютерных сетях // Молодой ученый. – 2016. - №9.5. – С. 10-12.- URL:https:// moluch.ru/archive/113/29719/ (дата обращения: 20.004.2018).*