

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТРАНСНАЦИОНАЛЬНОЙ КОРПОРАТИВНОЙ СЕТИ

Студент гр. 113025 Шилов А.В.,
кандидат техн. наук, доцент Артамонов В.А.
Белорусский национальный технический университет

Выход технологий глобальных сетей на новый уровень, когда скорости обмена данными в локальных и глобальных сетях практически не отличаются, приводит к всё большему распространению транснациональных корпоративных сетей.

В транснациональных компьютерных сетях, в отличие от сетей регионального уровня, очень дорого использовать выделенные линии связи, поэтому приходится использовать сеть Internet. Это порождает множество проблем в обеспечении безопасности. Одной из главных является общедоступность сети Internet, что дает возможность любому пользователю перехватывать sniffером передаваемые по этой сети данные. Решением этой проблемы является применение VPN каналов, шифрование и снабжение цифровой подписью передаваемых сообщений.

В транснациональных компьютерных сетях, использующих Internet, большой проблемой также является огромное количество точек входа в сеть. Решением этой проблемы является применение всевозможных брандмауэров и межсетевых экранов с детально проработанными политиками. Угрозу безопасности представляет и тот факт, что не исключены обрывы связи в сети Internet, что может привести, допустим, к потери доступа к серверу аутентификации. Предотвращение этой угрозы осуществляется резервированием наиболее значимых компонентов сети, отказ которых может привести к потере информационной безопасности.

Усугубляет все эти проблемы тот факт, что пользователи зачастую нарушают различные правила безопасности, чем значительно облегчают взлом. Не исключены ошибки и со стороны администраторов. Для решения этой проблемы необходимо составление политики безопасности, которая является основой системы обеспечения информационной безопасности транснациональной сети.

Существенным фактором, влияющим на защиту активов транснациональной сети, является совокупность применяемого оборудования. В сетях такого масштаба очень важно применять системы обнаружения вторжений IDS и IPS. Также очень важно как можно сильнее защитить файловые хранилища от доступа посторонних пользователей.

Все эти меры в совокупности с множеством иных и составляют систему обеспечения информационной безопасности корпоративной сети.