

Информационная безопасность в сетях ЭВМ

Ковалькова И.А.

Белорусский национальный технический университет

Защита данных в компьютерных сетях – одна из самых открытых проблем в современных информационно-вычислительных системах. На сегодняшний день сформулировано три базовых принципа информационной безопасности, задачей которой является обеспечение:

конфиденциальности информации – защиты от несанкционированного доступа к информации или гарантии того, что информация будет доступна только тем субъектам, которым разрешён доступ (т.е. авторизованным пользователям);

доступности информации – возможности за приемлемое время получить требуемую информационную услугу или гарантии того, что авторизованные пользователи всегда получают доступ к хранящейся в компьютерной системе информации (в любое время, по первому требованию);

целостности данных – защищённости информации от разрушения и несанкционированного изменения или гарантии сохранения данными правильных значений, которая обеспечивается запретом их модификации для неавторизованных пользователей.

При рассмотрении проблем, связанных с защитой данных в сети, возникает вопрос о классификации сбоев и несанкционированности доступа, что ведёт к потере или нежелательному изменению данных. Это могут быть сбои оборудования (кабельной системы, дисковых систем, серверов, рабочих станций и т.д.), потери информации (из-за инфицирования компьютерными вирусами, неправильного хранения архивных данных, нарушений прав доступа к данным), некорректная работа пользователей и обслуживающего персонала. Перечисленные нарушения работы в сети вызвали необходимость создания различных видов защиты информации. Условно их можно разделить на три класса: *средства физической защиты* (архивирование и дублирование информации); *программные средства* (антивирусные программы, программные средства контроля доступа); *административные меры защиты* (доступ в помещения, разработка стратегий безопасности фирмы и т.д.).

Для исключения неавторизованного проникновения в компьютерную сеть используется комбинированный подход – использование пароля и идентификации пользователя по персональному "ключу".