

**Информационная безопасность в  
условиях функционирования в  
России глобальных сетей**

# Информационная безопасность

Термин «информационная безопасность» появился в нормативных правовых актах, научных и иных публикациях на рубеже 90-х годов, когда пришло окончательное осознание реальной значимости информации в жизни общества и в обеспечении национальной безопасности России. По аналогии с этим определением информационная безопасность чаще всего определяется как «состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере».



▶ Internet создавался как незащищенная система, не предназначенная для хранения и обработки конфиденциальной информации. Следовательно, протоколы используемые в этой сети также не обеспечивают должного контроля безопасности и целостности информационных ресурсов. В Сети не должна находиться информация, раскрытие которой приведет к серьезным последствиям. Наоборот, в Сети необходимо размещать информацию, распространение которой желательно ее владельцу. При этом всегда необходимо учитывать тот факт, что в любой момент эта информация может быть перехвачена, искажена или может стать недоступной.

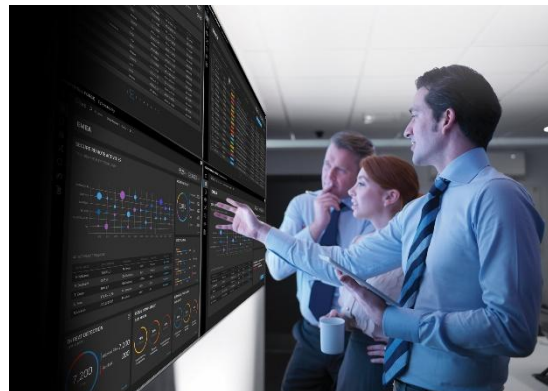
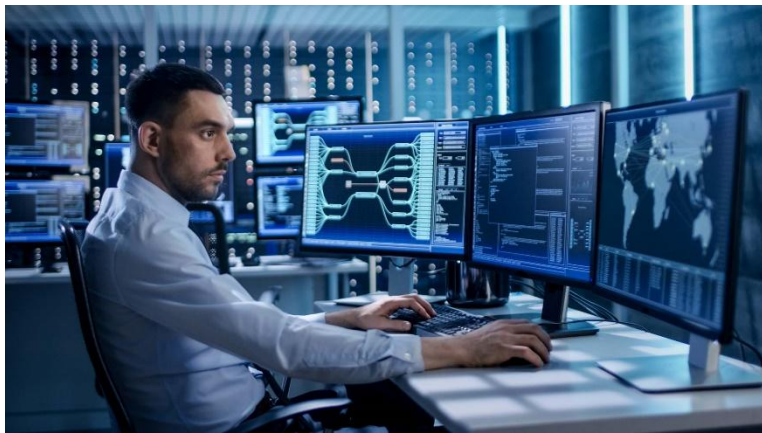


- ▶ Следовательно, особое внимание должно быть уделено информационной безопасности в условиях функционирования глобальных сетей. В России данная проблема особенно актуальна, так как в нашей стране не развита соответствующим образом ни законодательная, ни программная, ни аппаратная база.



# Основные задачи обеспечения защиты информации:

- ▶ - защита информации в каналах связи и базах данных криптографическими методами;
- ▶ - подтверждение подлинности объектов данных и пользователей (аутентификация сторон, устанавливающих связь);
- ▶ - обнаружение нарушений целостности объектов данных;
- ▶ - обеспечение защиты технических средств и помещений, в которых ведется обработка конфиденциальной информации, от утечки по побочным каналам и от возможно внедренных в них электронных устройств съема



- ▶ - обеспечение защиты программных продуктов и средств вычислительной техники от внедрения в них программных вирусов и закладок;
- ▶ - защита от несанкционированных действий по каналу связи от лиц, не допущенных к средствам шифрования, но преследующих цели компрометации секретной информации и дезорганизации работы абонентских пунктов;
- ▶ - организационно-технические мероприятия, направленные на обеспечение сохранности конфиденциальных данных.



спасибо за внимание