

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации.



Для успешного внедрения систем информационной безопасности на предприятии необходимо придерживаться трех главных принципов :

- 1) Конфиденциальность.
- 2) Целостность.
- 3) Доступность.

Контроль информационной безопасности :

- 1) Административный.
- 2) Логический.
- 3) Физический.



Цель обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения. Информационная безопасность помогает обеспечить непрерывность бизнеса.





Средства защиты информационной безопасности

Средства защиты информационной безопасности — это набор технических приспособлений, устройств, приборов различного характера, которые препятствуют утечке информации и выполняют функцию ее защиты.



Угрозы информационной безопасности можно разделить на следующие:

Естественные.

Искусственные, которые также делятся на:

- непреднамеренные (совершаются людьми по неосторожности или незнанию);
- преднамеренные (хакерские атаки, противоправные действия конкурентов, месть сотрудников и пр.).

Внутренние (источники угрозы, которые находятся внутри системы).

Внешние (источники угроз за пределами системы)



Средства защиты информации делятся на:

Организационные.

Программные.

Технические (аппаратные).

Смешанные аппаратно-программные.