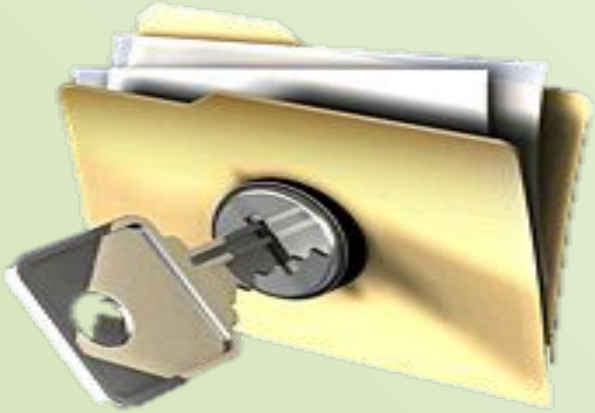
Информационная безопасность

Под ***информационной безопасностью*** понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.



На практике важнейшими являются **три аспекта** информационной безопасности:

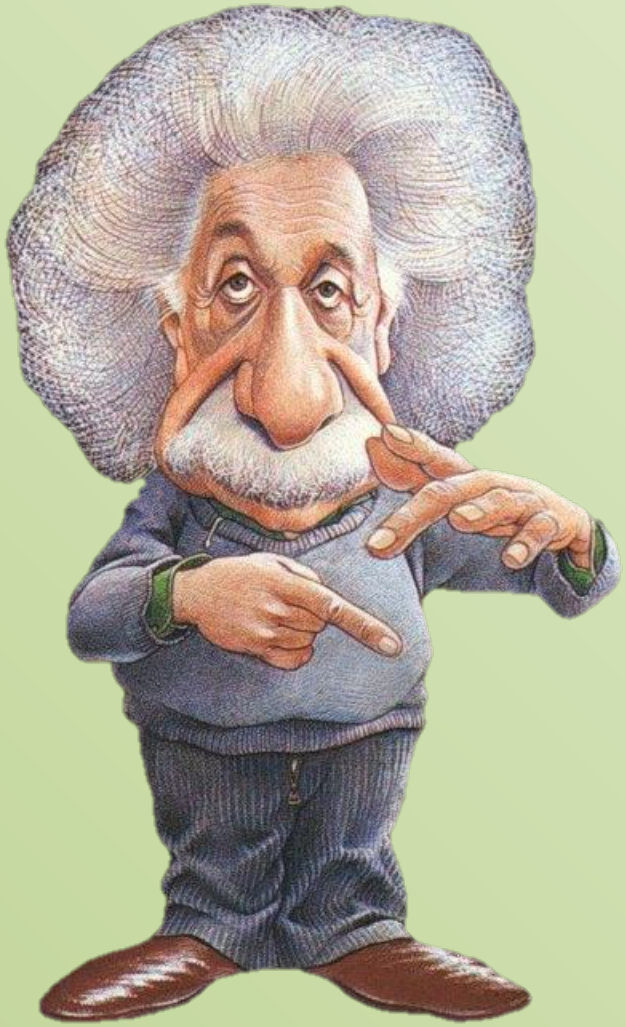
- **доступность** (возможность за разумное время получить требуемую информационную услугу);
- **целостность** (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- **конфиденциальность** (защита от несанкционированного прочтения).

Некоторые виды компьютерных преступлений

- **1. Несанкционированный (неправомерный) доступ к информации.** Лицо получает доступ к секретной информации, например, путем подбора шифра (пароля). Подавляющее большинство разработок в области информационной безопасности посвящено именно этому виду преступлений.

- **2. Нарушение работоспособности компьютерной системы.** В результате преднамеренных действий ресурсы вычислительной системы становятся недоступными, или снижается ее работоспособность. Примером такого рода преступлений является создание и распространение компьютерных вирусов.
- **3. Подделка (искажение или изменение), т. е. нарушение целостности компьютерной информации.** Эта деятельность является разновидностью неправомерного доступа к информации. К подобного рода действиям можно отнести подтасовку результатов голосования на выборах

Методами обеспечения защиты информации в организации являются:



- **Препятствие** – метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т. д.).

- **Управление доступом** – метод защиты информации, связанный с регулированием использования всех ресурсов информационной системы.
- **Маскировка** – метод защиты информации в информационной системе организации путем ее криптографического закрытия.
- **Регламентация** – метод защиты информации, создающий определенные условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней (сетевых атак) сводилась бы к минимуму.

- **Принуждение** – метод защиты, при котором пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.
- **Побуждение** – метод защиты информации, который мотивирует сотрудников не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.