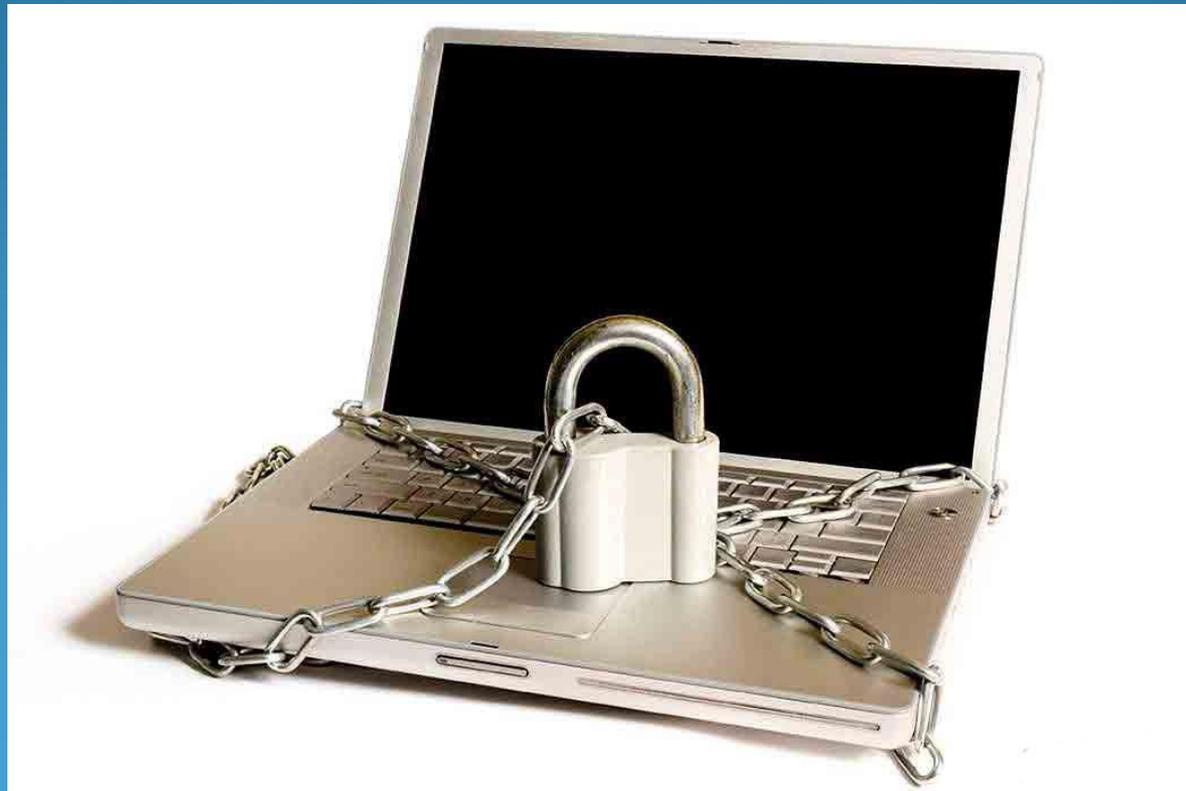


# Защита от несанкционированного доступа к информации



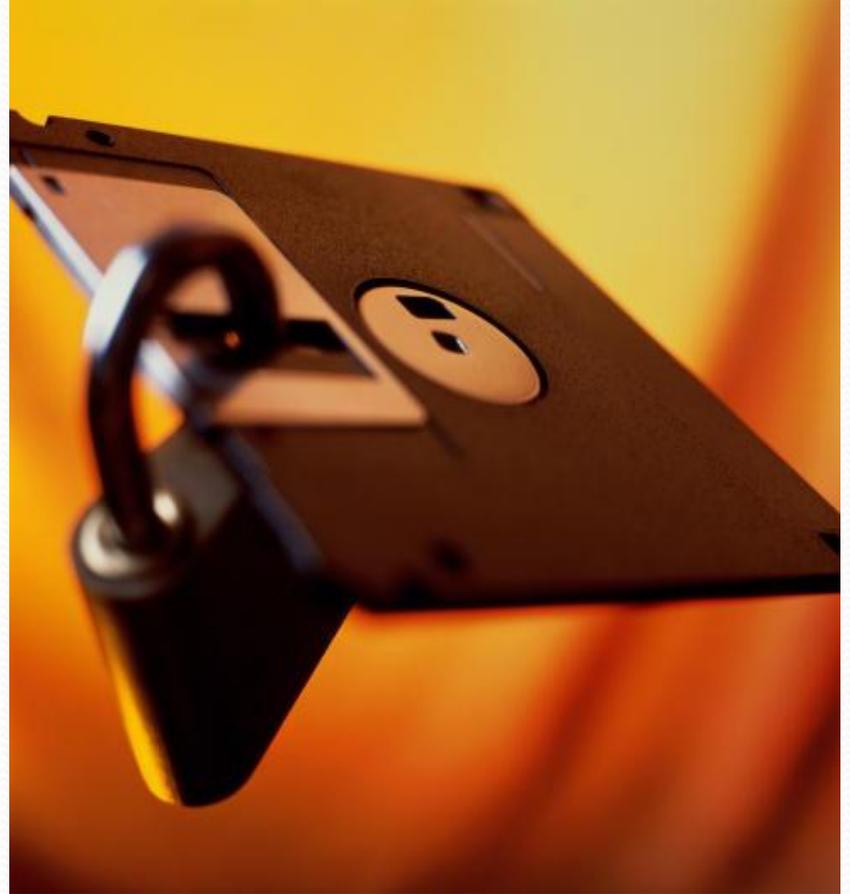
# Защита информации



**Защита** - система мер по обеспечению безопасности с целью сохранения государственных и коммерческих секретов. Защита обеспечивается соблюдением режима секретности, применением охранных систем сигнализации и наблюдения, использованием шифров и паролей.

## ***Защита информации***

представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.



# Несанкционированный доступ

## *Несанкционированный*

*доступ* - действия, нарушающ установленный порядок доступа или правила разграничения, дос к программам и данным, который получают абоненты, которые не прошли регистрацию и не имеют права на ознакомление или рабс этими ресурсами.

Для предотвращения несанкционированного доступа осуществляется контроль доступа.



# Защита с использованием паролей



ITQ

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются **пароли**.

Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль.

Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам.

При этом может производиться регистрация всех попыток несанкционированного доступа.

# Биометрические системы защиты

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются **биометрические системы идентификации**.

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

К биометрическим системам относятся системы идентификации

- по отпечаткам пальцев;
- по характеристикам речи;
- по радужной оболочке глаза
- по изображению лица;
- по геометрии ладони руки.



# Идентификация по отпечаткам пальцев

Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш-диски, а также применяются в виде отдельных внешних устройств и терминалов (например, в аэропортах и банках).

Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен.

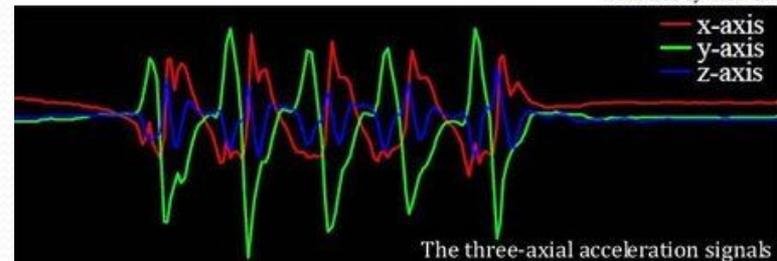
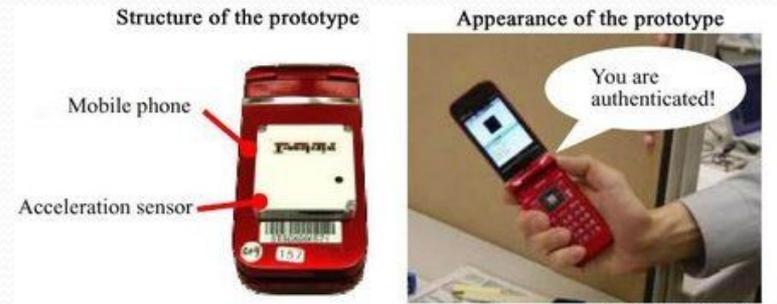


. Оптический сканер отпечатка пальца, вмонтированный в ноутбук

# Идентификация по характеристикам речи

Идентификация человека по голосу — один из традиционных способов распознавания, интерес к этому методу связан и с прогнозами внедрения голосовых интерфейсов в операционные системы.

Голосовая идентификация бесконтактна и существуют системы ограничения доступа к информации на основании частотного анализа речи.



The three-axial acceleration signals

# Идентификация по радужной оболочке глаза



Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой.

Изображение глаза выделяется из изображения лица и на него накладывается специальная маска штрих-кодов. Результатом является матрица, индивидуальная для каждого человека.

Для идентификации по радужной оболочке глаза применяются специальные сканеры, подключенные к компьютеру.

# Идентификация по изображению лица

Для идентификации личности часто используются технологии распознавания по лицу.

Распознавание человека происходит на расстоянии.

Идентификационные признаки учитывают форму лица, его цвет, а также цвет волос. К важным признакам можно отнести также координаты точек лица в местах, соответствующих смене контраста (брови, глаза, нос, уши, рот и овал).

В настоящее время начинается выдача новых загранпаспортов, в микросхеме которых хранится цифровая фотография владельца.



# Идентификация по ладони руки

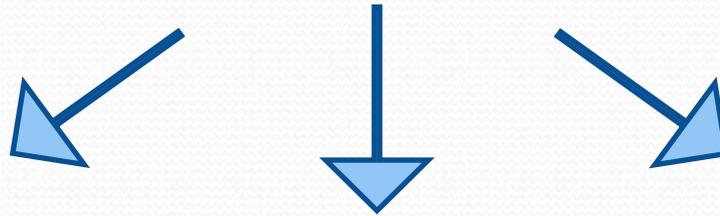
В биометрике в целях идентификации используется простая геометрия руки — размеры и форма, а также некоторые информационные знаки на тыльной стороне руки (образы на сгибах между фалангами пальцев, узоры расположения кровеносных сосудов).

Сканеры идентификации по ладони руки установлены в некоторых аэропортах, банках и на атомных



# Вредоносные программы

Вирусы, черви,  
троянские и  
хакерские  
программы



Потенциально  
опасное  
программное  
обеспечение

Шпионское,  
рекламное  
программное  
обеспечение



# программ

## Антивирусные программы

Современные антивирусные программы обеспечивают **комплексную защиту программ** и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компью

- Интернет,
- локальная сеть,
- электронная почта,
- съемные носители информации.

Для защиты от вредоносных программ каждого типа в антивирусе предусмотрены отдельные компоненты.

**Принцип работы антивирусных программ** основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.



**КОНЕЦ**