

# ПРАВОВАЯ ОХРАНА ПРОГРАММ И ДАННЫХ. ЗАЩИТА ИНФОРМАЦИИ.



Презентацию подготовила Смолева  
Екатерина ученица 11 «а» класса  
МОУ Объячевская СОШ

# ПРАВОВАЯ ОХРАНА ИНФОРМАЦИИ

---



Правовая охрана программ для ЭВМ и баз данных в полном объёме введена в Российской Федерации Законом **"О правовой охране программ для ЭВМ и баз данных"**, который вступил в силу в 1992 году.

# ПРАВОВАЯ ОХРАНА ИНФОРМАЦИИ

---

Для оповещения о своих правах разработчик программы использует знак охраны авторского права.

Знак охраны авторского права состоит из трёх элементов:

- буквы С в окружности © или круглых скобках (с);
- наименования (имени) правообладателя;
- года первого выпуска программы в свет.



# ПРАВОВАЯ ОХРАНА ИНФОРМАЦИИ

В 2002 году был принят Закон **«Об электронно-цифровой подписи»**, который стал законодательной основой электронного документооборота в России.



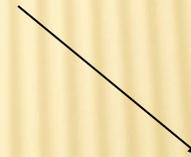
# ПРАВОВАЯ ОХРАНА ИНФОРМАЦИИ

---

При регистрации электронно-цифровой подписи в специализированных центрах корреспондент получает два ключа:



***секретный***



***открытый***

# ПРАВОВАЯ ОХРАНА ИНФОРМАЦИИ

---



Секретный ключ хранится на дискете или смарт-карте и известен только корреспонденту.

# ПРАВОВАЯ ОХРАНА ИНФОРМАЦИИ

---

Открытый ключ  
должен быть у всех  
потенциальных  
получателей  
документов.



Обычно  
рассылается по  
электронной  
почте.

# ЗАЩИТА ИНФОРМАЦИИ

---

## Защита от несанкционированного копирования

— система мер, направленных на противодействие несанкционированному копированию информации, как правило представленной в электронном виде (данных или программного обеспечения).



# ЗАЩИТА ИНФОРМАЦИИ

---



При защите от копирования используются различные меры:

- 
- организационные
- юридические
- физические
- в интернете

# ЗАЩИТА ИНФОРМАЦИИ

---

Для защиты данных, хранящихся на компьютере, используются пароли.



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

# ЗАЩИТА ИНФОРМАЦИИ

## Организационные меры защиты от несанкционированного копирования

полноценное использование программного продукта невозможно без соответствующей поддержки со стороны производителя: подробной пользовательской документации, «горячей линии», системы обучения пользователей и т.п. Организационные меры защиты применяются крупными разработчиками к достаточно большим и сложным программным продуктам.



# ЗАЩИТА ИНФОРМАЦИИ

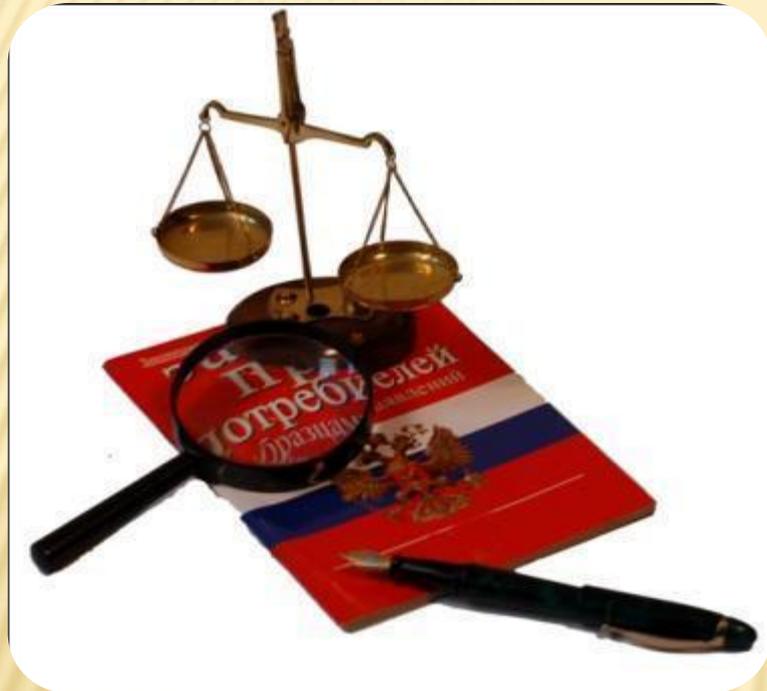
## Организационные меры защиты от несанкционированного копирования

Для защиты доступа к информации всё чаще используют биометрические системы идентификации: идентификация по отпечаткам пальцев, системы распознавания речи, системы идентификации по радужной оболочке глаза, по изображению лица, по геометрии ладони руки.



# ЗАЩИТА ИНФОРМАЦИИ

## Юридические меры защиты от несанкционированного копирования



Предусматривают ответственность, в соответствии с действующим законодательством, за использование контрафактных экземпляров программ для ЭВМ или баз данных.

# ЗАЩИТА ИНФОРМАЦИИ

## Физическая защита данных

Для обеспечения большей надёжности хранения данных на жёстких дисках используют RAID-массивы. Несколько жёстких дисков подключаются к RAID-контроллеру, который рассматривает их как единый логический носитель информации.



# ЗАЩИТА ИНФОРМАЦИИ

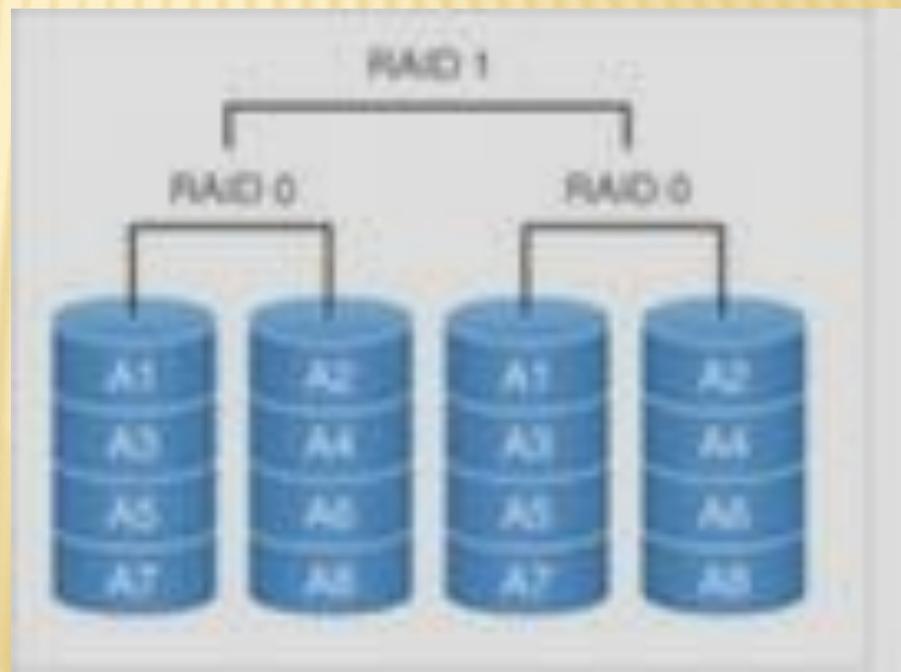
## Физическая защита данных

При записи информации она дублируется и сохраняется на нескольких дисках одновременно, поэтому при выходе из строя одного из дисков данные не теряются.

Существует несколько разновидностей RAID-массивов:

RAID 0

RAID 1



# ЗАЩИТА ИНФОРМАЦИИ

## Защита в Интернете



Для защиты информационных ресурсов компьютера, подключённого к Интернету используют антивирусные программы, например: Антивирус Касперского (Windows) и антивирус KlamAV(Linux).



# ЗАЩИТА ИНФОРМАЦИИ

## Защита в Интернете

Для защиты компьютеров, подключённых к Интернету, от сетевых вирусов и хакерских атак между Интернетом и компьютером устанавливается аппаратный или программный межсетевой экран. Межсетевой экран отслеживает передачу данных между Интернетом и локальным компьютером, выявляет подозрительные действия и предотвращает несанкционированный доступ к данным.

