

Презентация подготовлена для конкурса  
«Интернешка» <http://interneshka/org/>.

Конкурс-презентаций по информатике  
(от АО «Лаборатория Касперского»)

**«Защита собственной  
информации от  
несанкционированного доступа»**



Выполнила  
ученица 10 класса  
МБОУ «Школа № 8», г. Ачинска  
Красноярского края  
Ефремова Алёна



# «Защита собственной информации от несанкционированного доступа»



**В настоящее время наша жизнь, немислима без современных информационных технологий.**

**Однако именно высокая степень автоматизации порождает риск снижения безопасности.**

# Несанкционированный доступ (Unauthorized access to information)

## **Несанкционированный доступ**

**-чтение, обновление или  
разрушение информации при  
отсутствии на это  
соответствующих  
полномочий.**



**Несанкционированный доступ осуществляется, как правило, с адресов устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи.**

## Виды несанкционированного доступа



Угроза информации - пути реализации воздействий, которые считаются опасными для информационной системы. По характеру возникновения их можно разделить на 2 вида: **преднамеренные и непреднамеренные.**

### \* **ПРЕДНАМЕРЕННЫЕ**

- это несанкционированное получение информации и несанкционированная манипуляция данными, ресурсами, самими системами.

### \* **НЕПРЕДНАМЕРЕННЫЕ**

- это случайные действия, выраженные в неадекватной поддержке механизмов защиты или ошибками в управлении.

## По типу реализации угрозы можно различать

### \* **ПРОГРАММНЫЕ**

К программным относят те, которые реализованы в виде отдельного программного модуля или модуля в составе программного обеспечения.



### \* **НЕПРОГРАММНЫЕ**

\* К непрограммным относят злоупотребления, в основе которых лежит использование технических средств информационной системы (ИС) для подготовки и реализации компьютерных преступлений (например, несанкционированное подключение к коммуникационным сетям, съём информации с помощью специальной аппаратуры).

# Причины несанкционированного доступа к информации

- ❑ ошибки конфигурации прав доступа;
- ❑ слабая защищённость средств авторизации ошибки в программном обеспечении;
- ❑ злоупотребление служебными полномочиями;
- ❑ прослушивание каналов связи;
- ❑ использование клавиатурных шпионов, вирусов на компьютерах.





## Безопасность данных

### Защита данных от несанкционированного доступа

- \* Идентификация и авторизация пользователя
- \* Защита каналов передачи данных

### Резервное копирование и восстановление информации

- \* Резервное копирование
- \* Безопасное хранение
  - \* Восстановление

# Защита информации



**Защита информации** – это деятельность по предотвращению утраты и утечки защищаемой информации.



# Информационная безопасность

- \* **Информационная безопасность** – это меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.

Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода.

Информационная безопасность дает гарантию, что достигаются следующие **цели**:

- \* конфиденциальность информации;
- \* целостность информации;
- \* доступность информации, когда она нужна;
- \* учет всех процессов, связанных с информацией.



# Защита собственной информации



## Существует четыре уровня защиты компьютерных и информационных ресурсов:

- \* **Предотвращение** предполагает, что только ты имеешь доступ к защищаемой информации.
- \* **Обнаружение** предполагает раннее раскрытие, даже если механизмы защиты были обойдены.
- \* **Ограничение** уменьшает размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению.
- \* **Восстановление** обеспечивает эффективное воссоздание информации при наличии документированных и проверенных планов по восстановлению.

# Метод парольной защиты



**Метод паролей считается достаточно слабым, так как пароль может стать объектом хищения, перехвата, перебора, угадывания.**

**Однако простота метода стимулирует поиск путей его усиления.**

**Для повышения эффективности парольной защиты рекомендуется**

- \* выбирать пароль длиной более 6 символов, избегая распространенных, легко угадываемых слов, имен, дат и т.п.;
- \* использовать специальные символы;
- \* пароли, хранящиеся на сервере, шифровать при помощи односторонней функции;
- \* периодически менять пароли.





# Метод профилактики для защиты от вирусов

**В целях профилактики для защиты от вирусов рекомендуется:**

- \* работа с дискетами, защищенными от записи;
- \* хранение программ на жестком диске в архивированном виде.

**Для того чтобы избежать появления компьютерных вирусов, необходимо соблюдать прежде всего следующие меры:**

- \* не переписывать программное обеспечение с других компьютеров;
- \* не допускать к работе на компьютере посторонних лиц, особенно если они собираются работать со своими дискетами, USB;
- \* не пользоваться посторонними дискетами.
- \* Регулярно тестируйте компьютер на наличие вирусов с помощью антивирусных программ перед считыванием информации.
- \* Не используйте программы, поведение которых непонятно.
- \* Регулярно обновляйте антивирусные программы.



**ДОСТУП ЗАПРЕЩЁН**



**Несмотря на имеющиеся способы защиты информации в глобальной сети Internet, нельзя недооценивать возможности многочисленных хакеров и других взломщиков.**



**Любая, даже, на ваш взгляд, незначительная информация, находящаяся в более менее свободном или плохо защищенном доступе может быть использована против вас.**

**Поэтому всегда следует интересоваться последними новинками в данной теме.**

## Заключение - вывод



**В заключении хочется сказать, что при организации защиты информации процесс создание и эксплуатация систем защиты информации является сложным и ответственным.**

**Система защиты должна быть достаточной, надежной и эффективной.**

Спасибо за внимание!

