

# ЗАЩИТА ИНФОРМАЦИИ

ЛЕКЦИЯ 7



# ИНФОРМАЦИЯ

Источник информации

Канал связи

Приемник информации

ПО КАКОМУ КАНАЛУ  
ИНФОРМАЦИЯ?



# СВОЙСТВА ИНФОРМАЦИИ



# ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

- **Защита информации** - это комплекс мероприятий, направленных на обеспечение информационной безопасности.
- **Информационная безопасность** - защита целостности, доступности и конфиденциальности информации.

# ДОСТУПНОСТЬ



•  
А  
г  
т  
и  
по  
Ес  
ус  
оч  
ве,  
уп  
По  
Эл

у.

го,



# ЦЕЛОСТНОСТЬ

- Цел  
инф  
несо

Цел  
случая  
действ  
предп  
проце  
данны  
смерт  
инфор



ИВЕСТЬ  
И

ИБ в тех  
К

ческого  
В  
сле  
й



# КОНФИДЕНЦИАЛЬНОСТЬ

- Кон  
нео

По  
инф  
дост  
целс  
услу  
инф  
мом  
орго  
отде



ии.

СТОИТ

й



# УГРОЗА

- Угроза безопасности
- Потеря информации
- Потеря целостности

Угроза безопасности системы. Есть (пож) при защите ее п



ым  
ть.

тот,

шок в

ых  
а.

лю

алы  
тся.

# УГРОЗЫ ДОСТУПНОСТИ

1. Самыми частыми и самыми опасными с точки зрения размера ущерба являются **непреднамеренные ошибки** штатных пользователей.
2. Самый простой способ сделать информацию недоступной - **повреждения или разрушение оборудования.**
3. **Программные атаки** на доступность, в том числе компьютерными вирусами.

# УГРОЗЫ ЦЕЛОСТНОСТИ

1. Кражи и подлоги.
2. Дублирование данных.
3. Внесение дополнительных сообщений.
4. Нарушение целостности программ (внедрение вредоносного кода).

# УГРОЗЫ КОНФИДЕНЦИАЛЬНОСТИ

1. Раскрытие паролей.
2. Перехват данных.
3. Кража оборудования.
4. Маскарад - выполнение действий под видом лица, обладающим полномочиями для доступа к данным.

# СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

## 1. Без

Безо  
физ  
резе  
унич



омация.

Ы ОТ  
Х НА

# СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

## 2. К

Для  
исп

□ В

□ П  
у

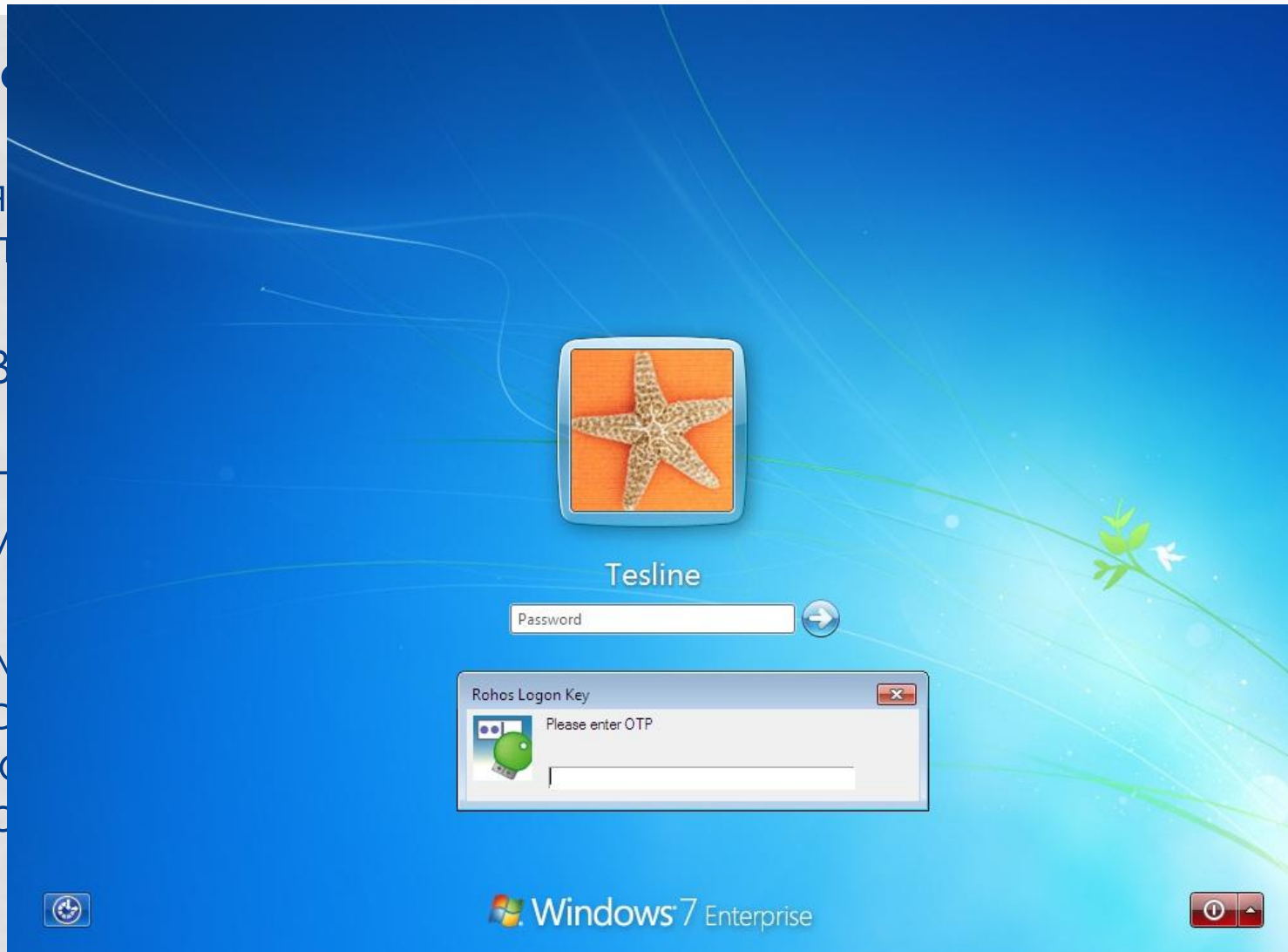
Пом  
сис  
по  
обо

мации

BIOS.

быть

е  
ции  
ой  
ки.

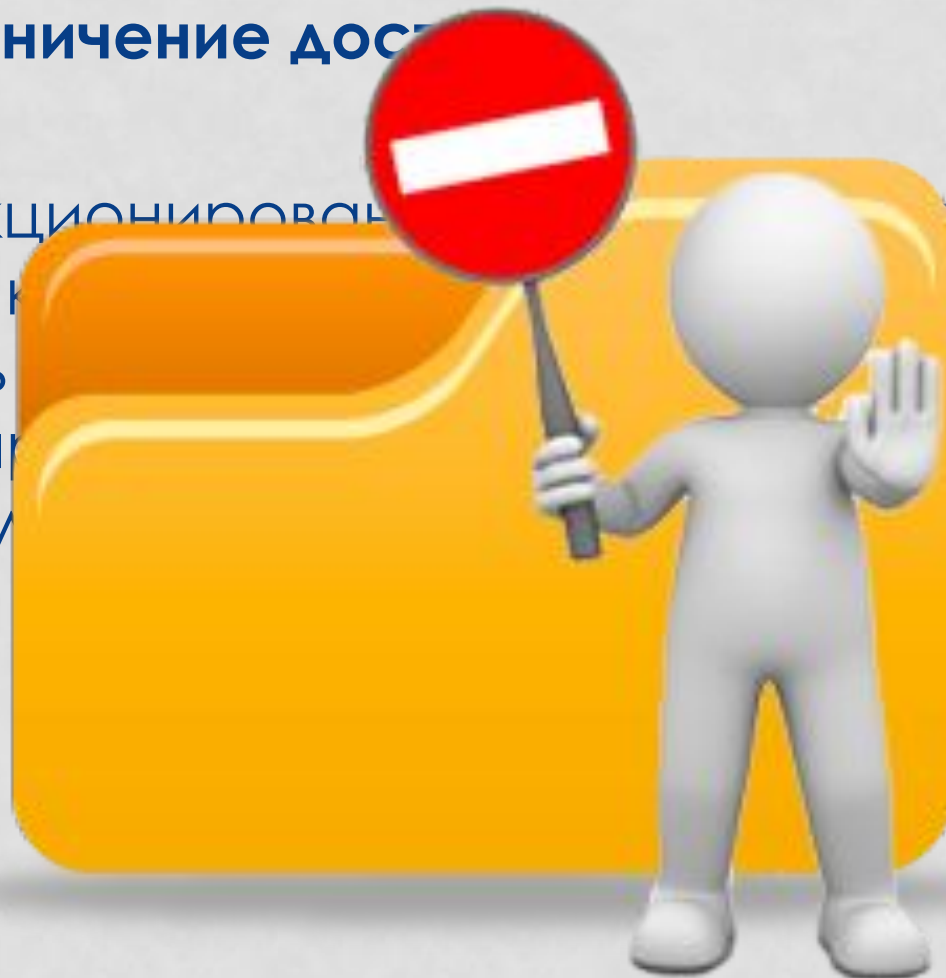


# СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

## 3. Разграничение доступа

От несанкционированного доступа к информации может быть защищена информация, которая может быть доступна, при этом для разных пользователей

может быть  
л. Для них  
права  
ными для



# СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

## 4. Дублирование канала связи и создание резервных

Дуб  
возм  
запо  
сис  
Соз  
при

и  
дих  
  
нных

## 5. Криптография

Кри  
шиф

я еще

со времен Цезаря и даже более ранних.

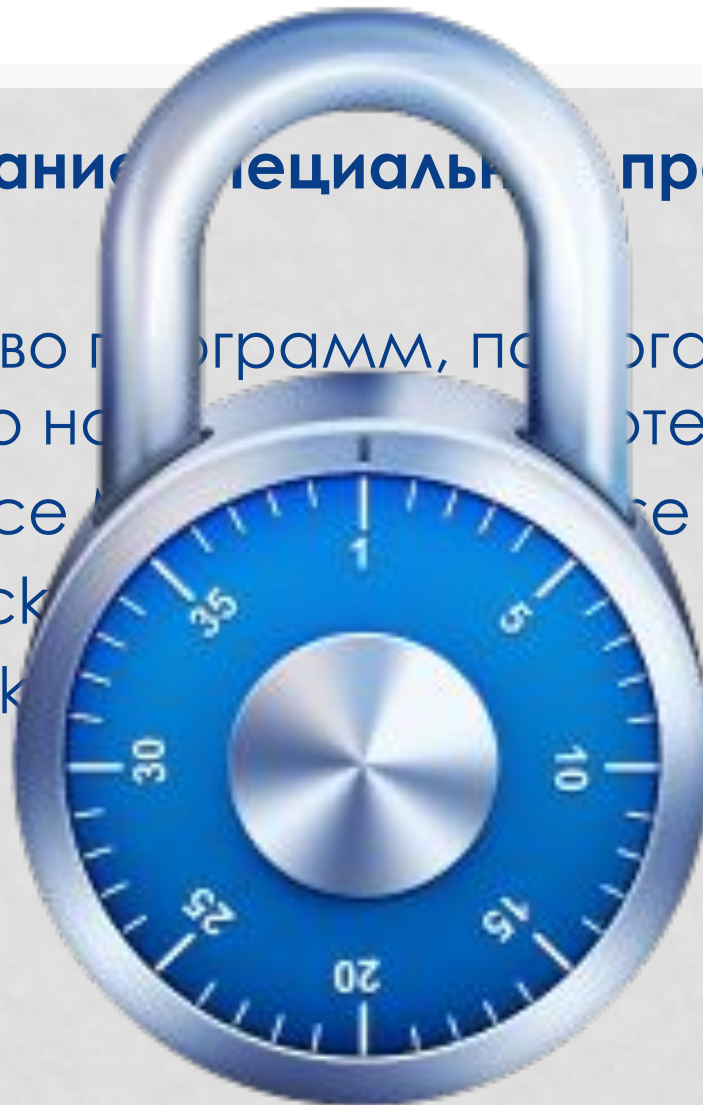


# СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

## 6. Использование специальных программ.

Есть множество программ, позволяющих защитить информацию на компьютере. Например:

- ❑ SysUtils Device Manager Lock Professional Edition;
- ❑ CD-DVD Lock;
- ❑ Paragon Disk Lock;
- ❑ TimeBoss;
- ❑ Lock 2.0.



# КОМПЬЮТЕРНЫЕ ВИРУСЫ

# КОМПЬЮТЕРНЫЕ ВИРУСЫ

**Компьютерные вирусы** - это вредоносные программы, которые могут «размножаться» и скрытно внедрять свои копии **в исполнимые файлы, загрузочные секторы дисков и документы.**

После заражения компьютера вирус может начать выполнение вредоносных действий и распространение своих копий, а также заставлять компьютер выполнять какие-либо действия.

Активация компьютерного вируса может вызывать уничтожение программ и данных и может быть связана с различными событиями (наступлением определенной даты, запуском программ и т.д.).



# КЛАССИФИКАЦИЯ ВИРУСОВ

**По величине вредных воздействий:**



## НЕОПАСНЫЕ

(последствия действия вирусов - уменьшение свободной памяти на диске, графические и звуковые эффекты)



## ОПАСНЫЕ

(последствия действия вирусов - сбои и «зависания» при работе компьютера)



## ОЧЕНЬ ОПАСНЫЕ

(последствия действия вирусов - потеря программ и данных форматирование винчестера и т.д.)

# КЛАССИФИКАЦИЯ ВИРУСОВ

По способу сохранения и исполнения своего кода:



**ЗАГРУЗОЧНЫЕ**

**ФАЙЛОВЫЕ**

**МАКРО-ВИРУСЫ**

**СКРИПТ-ВИРУСЫ**

# ЗАГРУЗОЧНЫЕ ВИРУСЫ

**Загрузочные вирусы** заражают **загрузочный сектор** гибкого или жесткого диска.



При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и отдают управление не оригинальному коду загрузчика, а коду вируса.



# ФАЙЛОВЫЕ ВИРУСЫ

**Файловые вирусы** внедряются в **исполняемые файлы** (командные файлы \*.bat, программы \*.exe, системные файлы \*.com и \*.sys, программные библиотеки \*.dll и др.) и обычно активируются при их запуске.



После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т.е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.

По способу заражения файловые вирусы разделяют на **перезаписывающие вирусы**, **вирусы-компаньоны** и **паразитические вирусы**.



# КЛАССИФИКАЦИЯ ВИРУСОВ

## По особенностям алгоритма

**Паразитические** (меняют содержимое файлов и секторов диска)

**Мутанты** (применяют алгоритм шифрования, вследствие чего их трудно обнаружить)

**Репликаторы** (они же сетевые черви, проникают через компьютерные сети)

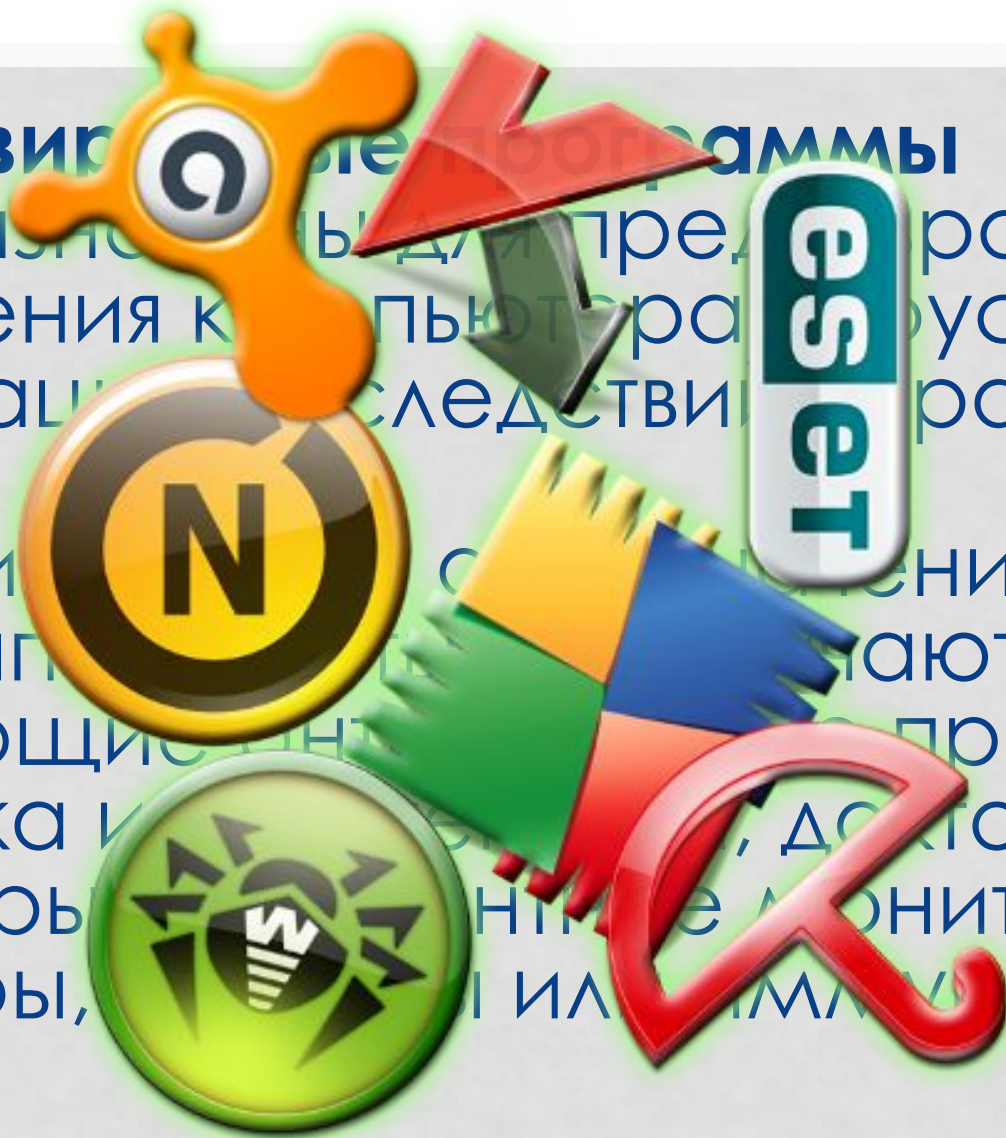
**Троянский конь** (один из самых опасных вирусов, так как трояны не размножаются, а воруют ценную)

**Невидимки** (трудно обнаружимые вирусы)

# АНТИВИРУСНЫЕ ПРОГРАММЫ

**Антивирусные программы** предназначены для предотвращения заражения компьютера вирусом и ликвидации последствий заражения.

В зависимости от принципа действия и принципов работы выделяют следующие типы антивирусных программ: сторожа и ревизоры, мониторы или фильтры, и т.д.



# АНТИВИРУСНАЯ ПРОГРАММА

1

2

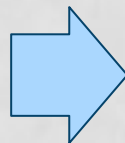
3

# АНТИВИРУСНАЯ ПРОГРАММА

Антивирусный  
сканер



Антивирусный  
монитор



Антивирус

# КАК ЗАЩИТИТЬСЯ ОТ ВИРУСОВ



# САМОСТОЯТЕЛЬНАЯ РАБОТА

1. Семакин И.Г. Базовый уровень: 11 класс.  
стр. 160-162
2. Способы защиты информации

## **Рефераты:**

1. Вирусы и антивирусы для смартфонов.
2. Брандмауэр.