ЗАЩИТА ИНФОРМАЦИИ

ЛЕКЦИЯ 7

ИНФОРМАЦИЯ

Источник информации → Канал связи → Приемник информации

СВОЙСТВА ИНФОРМАЦИИ

езная

По

понятная

Информация

Актуальная

Достоверная

Какие у информации свойства?

ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

- **Защита информации** - это комплекс мероприятий, направленных на обеспечение информационной безопасности.

- **Информационная безопасность** - защита целостности, доступности и конфиденциальности информации.

доступность

ЦЕЛОСТНОСТЬ

- **Цел нивость инф и нес**

Целс ИБ в тех случая к действ предп ческого проце в данны сле смерт й инфор

КОНФИДЕНЦИАЛЬНОСТЬ

- **Ко**
  не **ии.**

По
инф стоит
дост
цело й
усл
инф
мом
орг
отде

УГРОЗА

- **Уг… …ым об… …ть.**
- **По… …тот, кто… зло…**

Угро… …бок в про… сущ… …ых сист… …а. Есть … (пож… …лю прих… защ… …алы ее п… …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. **Бе** **ормация.**

Безо ты от
физ х на
резе
унич

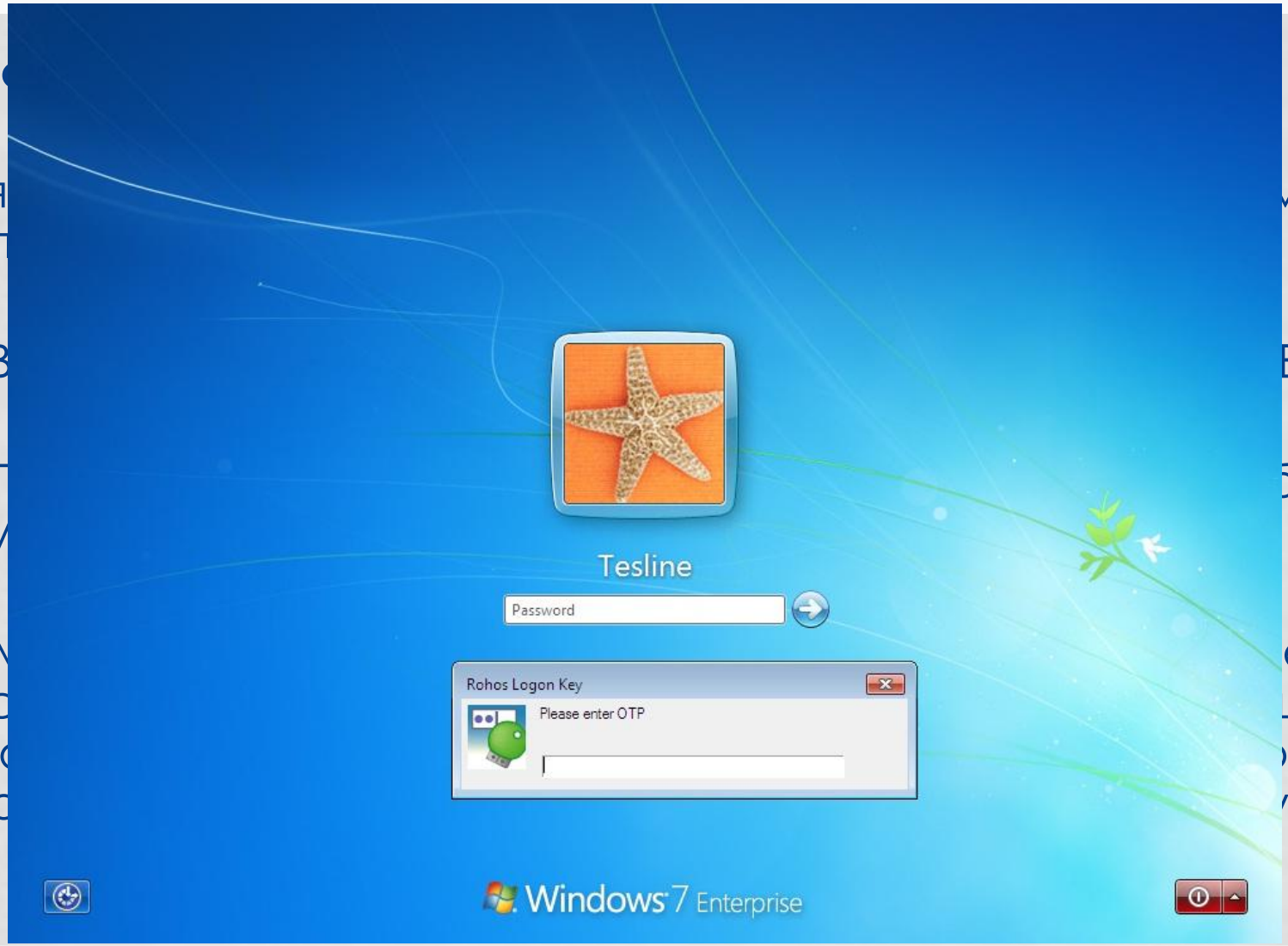
СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

2. К

Для мации
исп

- В BIOS.
- П быть
  у

Пол е
сис ции
по й
обо ки.



СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

3. **Разграничение дос**

От несанкциониров жет быть защищен л. Для них могут быть права доступа, п ными для разных по

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

4. **Дублирование канала связи и создание резервных**

Дуб
воз
зап
сис
Соз
при

5.

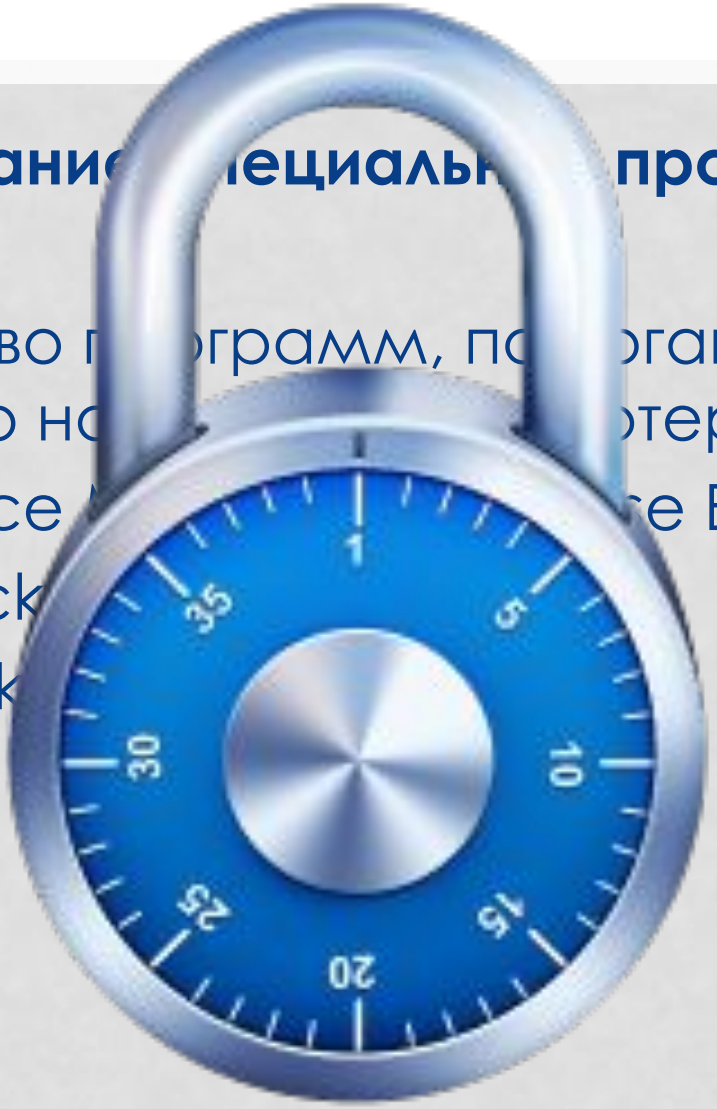
Кри
ши
со времен Цезаря и даже более ранних.

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

6. **Использование специальных программ.**

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

- SysUtils Device … ce Edition;
- CD-DVD Lock;
- Paragon Disk …
- 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

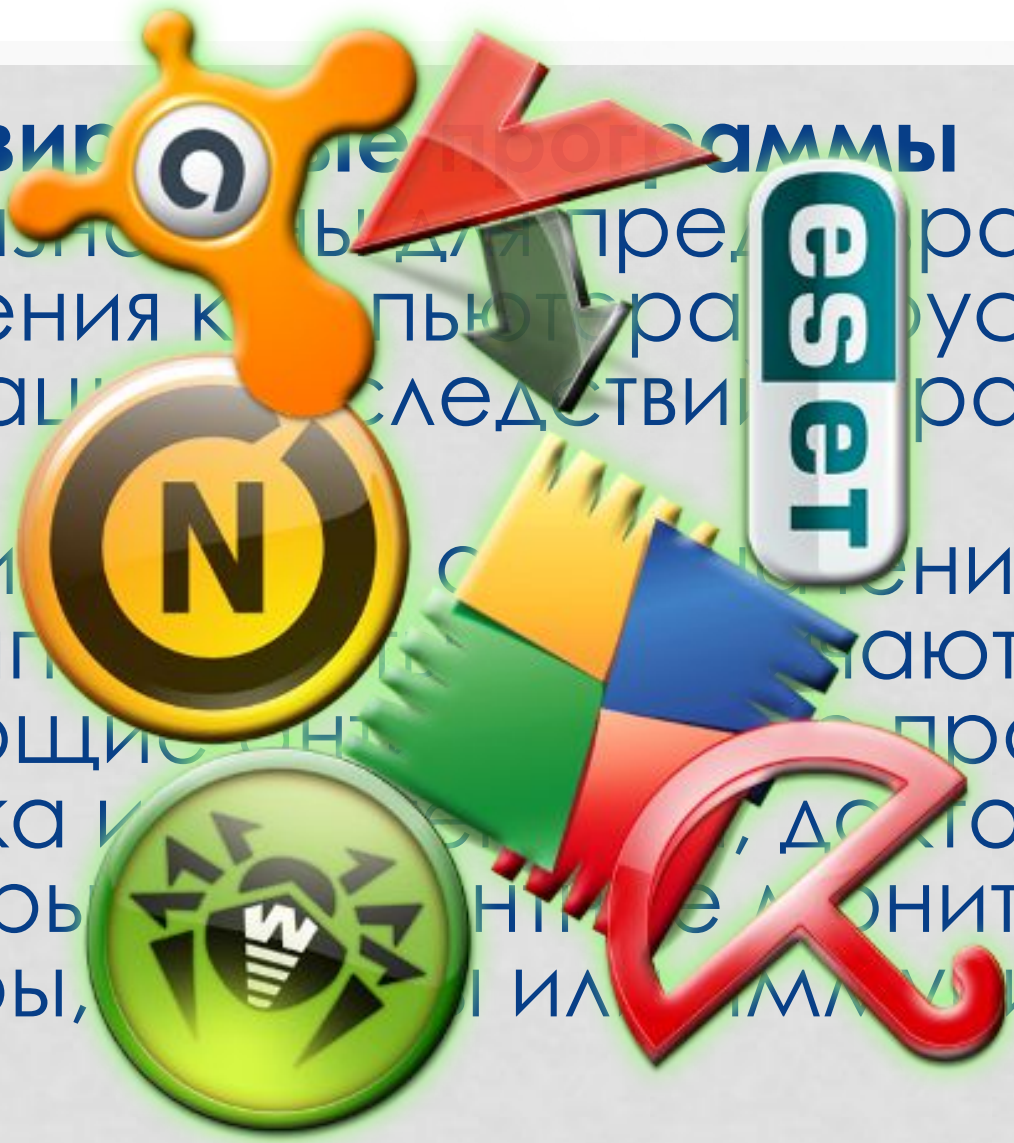
По особенностям алгоритма

- **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 обнаружения и принципа работы различают следующие антивирусные программы: сторожа и доктора, ревизоры, мониторы или фильтры, иммунизаторы.



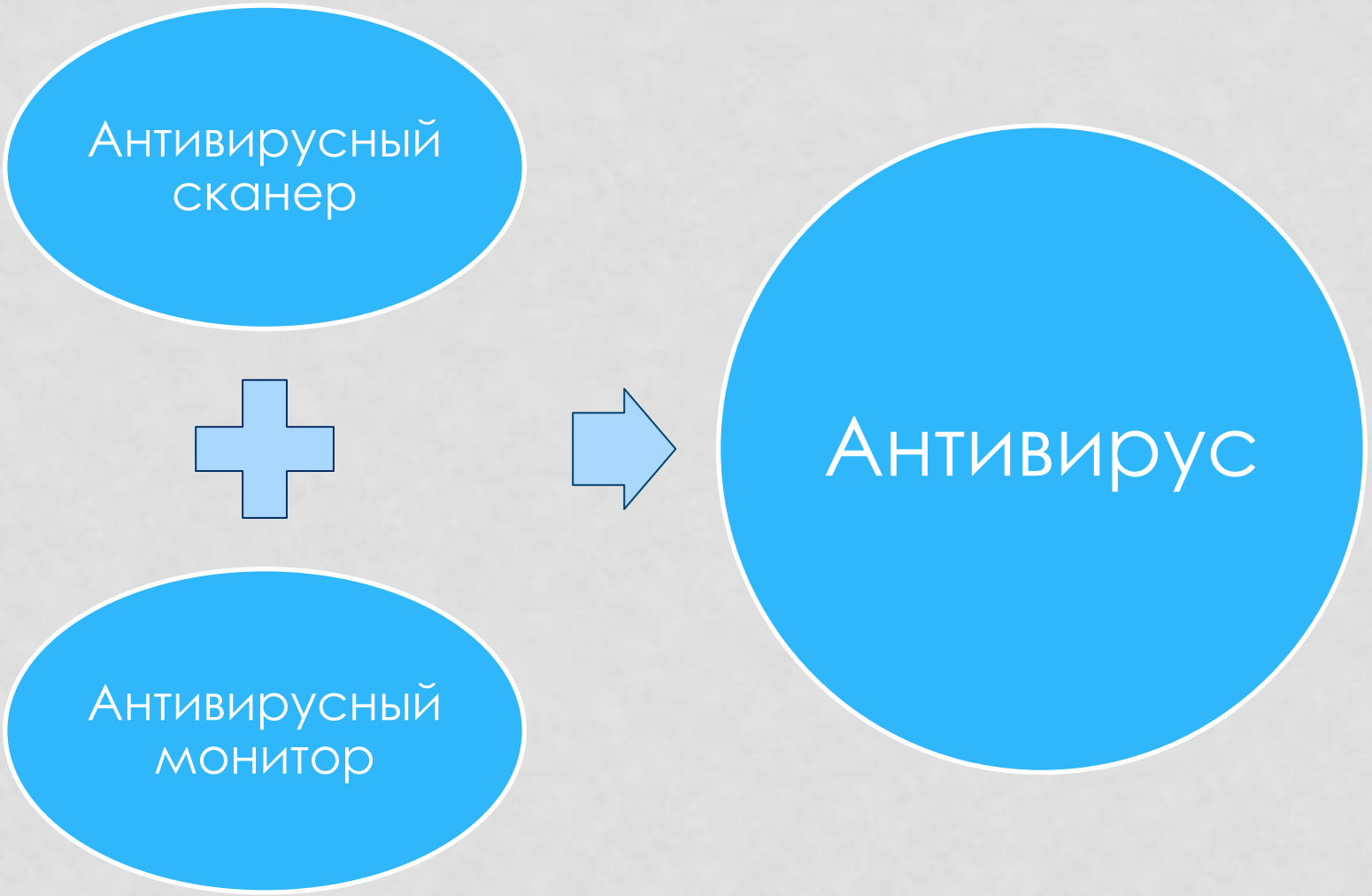
АНТИВИРУСНАЯ ПРОГРАММА

1

2

3

АНТИВИРУСНАЯ ПРОГРАММА



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.