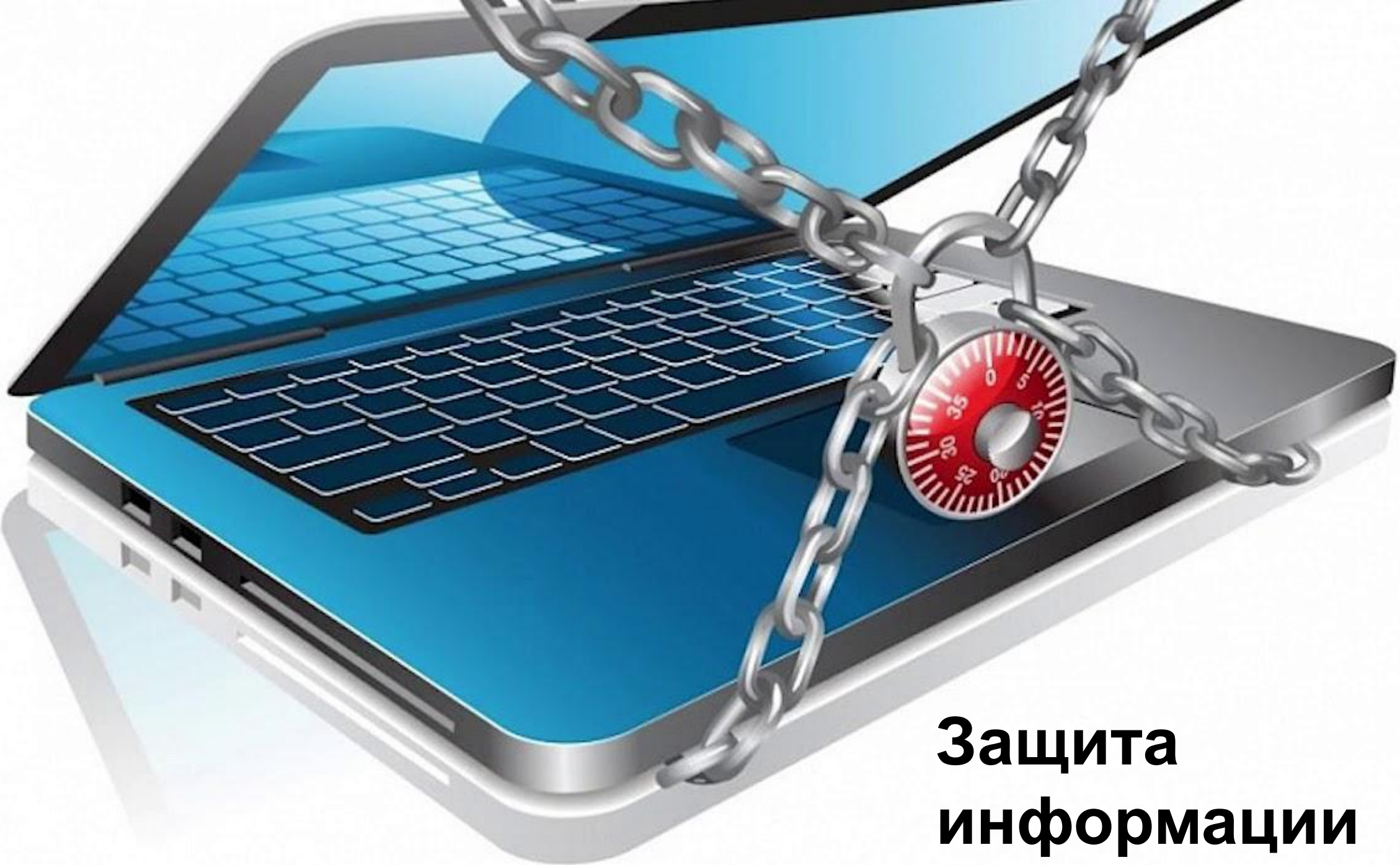
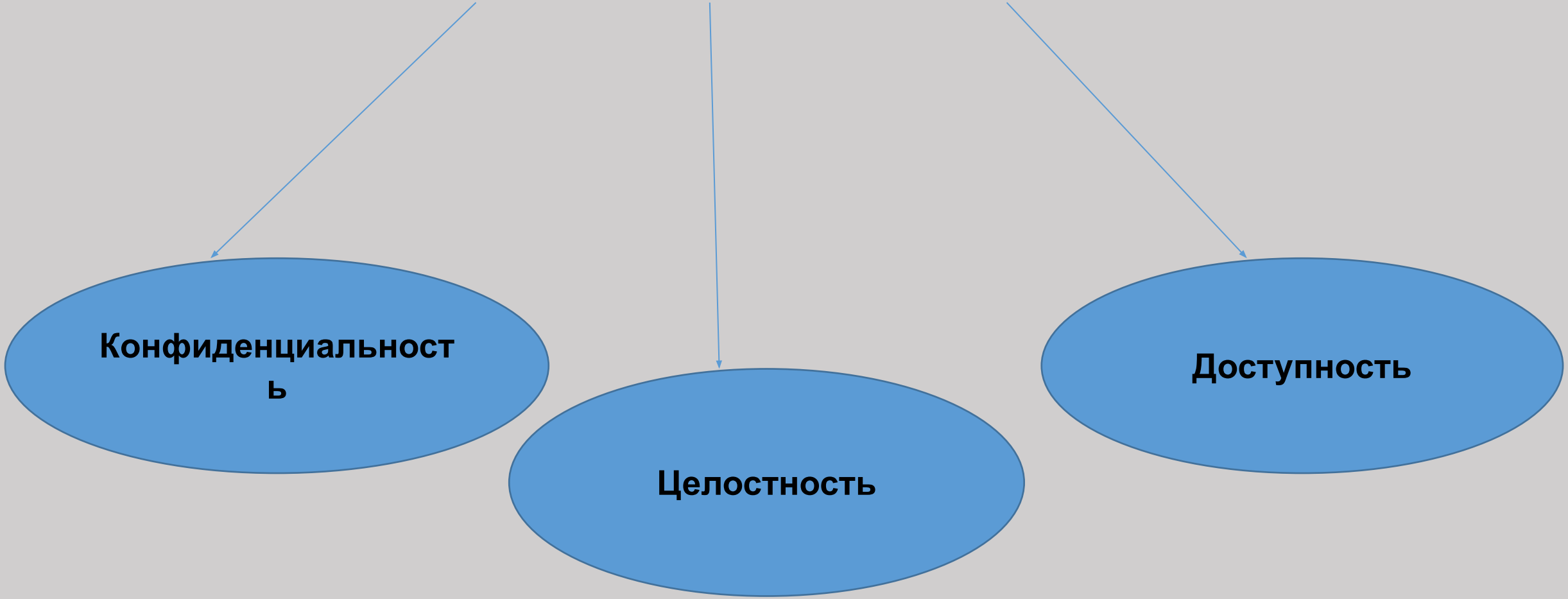


Защита информации

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

Защита информации-представляет собой деятельность по предотвращению утечки защищаемой информации несанкционированных и непреднамеренных воздействий на защищаемую информацию, т.е процесс, направленный на достижение этого состояния.

К безопасности информации относятся



ОПРЕДЕЛЕНИЯ

- **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют толь субъекты, имеющие на него право.

- **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамер субъектами, имеющими на него право.

- **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Информационная безопасность-это состояние защищенности информационной среды.

В вычислительной технике понятие безопасности подразумевает:
-надежность работы компьютера,
-сохранность ценных данных,
-защиту информации от внесения в нее изменений неуполномоченными лицами,
-сохранение тайны переписки в электронной связи.

Несанкционированный доступ-действия, нарушающие установленный порядок доступа или правила разграничения.

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

Защита с использованием пароля используется при загрузке операционной системы

От несанкционированного доступа могут быть защищены

-каждый диск,

- каждая папка,

-каждый файл локального компьютера.

Для них могут быть установлены определенные права доступа

-полный доступ,

-возможность внесения изменений,

-только чтение,

-запись

Права могут быть различными для различных пользователей

Биометрические системы идентификации.

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

К биометрическим системам защиты информации относятся системы идентификации:
-по отпечаткам пальцев;
-по характеристикам речи;
-по радужной оболочке глаза;
-по изображению лица;
-по геометрии ладони руки.

Для обеспечения большей скорости чтения, записи и надежности хранения данных на жестких дисках используются RAID-массивы.

RAID-массивы

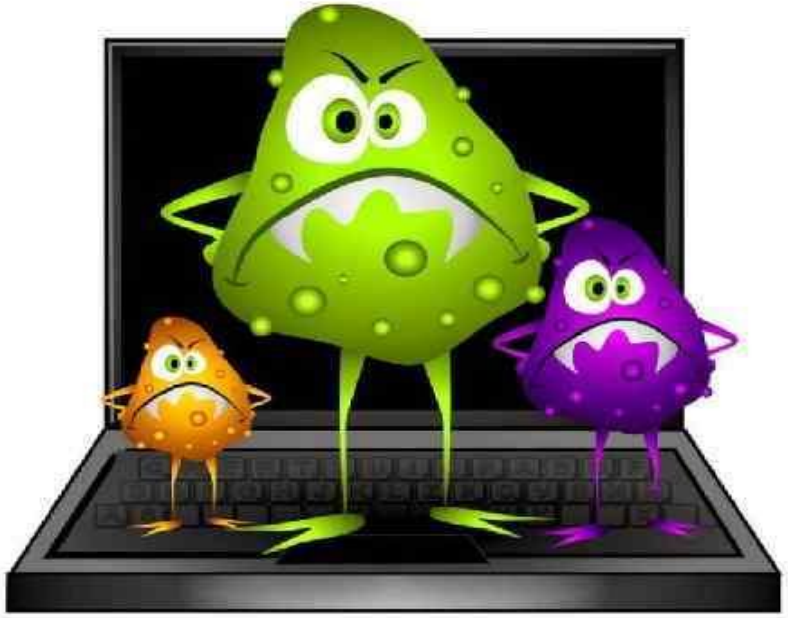
Существуют 2 способа реализации RAID-массива:

1. **аппаратный** (состоит из нескольких жестких дисков, управляемых специальной платой RAID контроллера);

2. **программный** (реализуется при помощи специального драйвера из нескольких логических разделов – менее надежен, но высокая скорость).

Вредоносные программы.

Вредоносная программа — злонамеренная программа, то есть программа, созданная со злым умыслом и/или злыми намерениями



Вредоносные программы

Вирусы, черви, троянские и хакерские программы

Шпионское, рекламное программное обеспечение

Потенциально опасное программное обеспечение

Антивирусные программы

Признаки заражения компьютера

1. На экране появляются неожиданные сообщения или изображения.

2. Вы слышите неожиданные звуки, воспроизводимые в случайном порядке.

3. Происходит самостоятельный запуск программ.

4. Вы видите, что некое приложение пытается соединиться с интернетом, хотя вы эту программу не запускали.

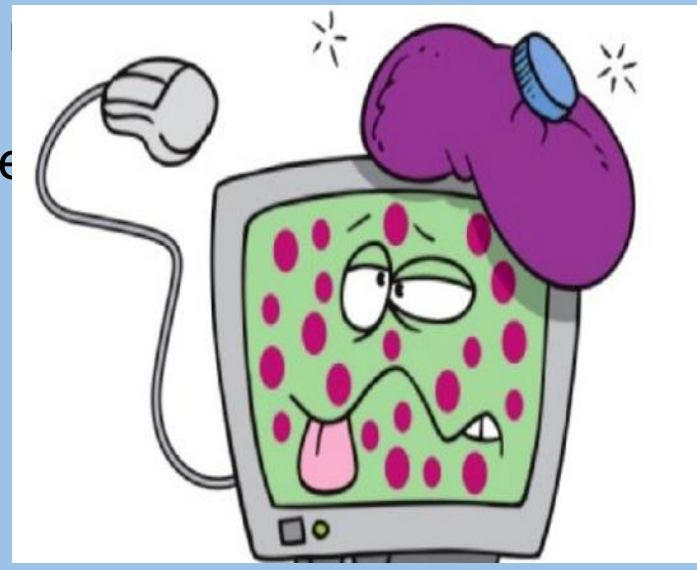
5. Ваши друзья получают от вас по электронной почте сообщения, которых

6. Ваш компьютер часто зависает или программы стали выполняться медле

7. Вы получаете множество системных сообщений об ошибке.

8. При включении компьютера операционная система не загружается.

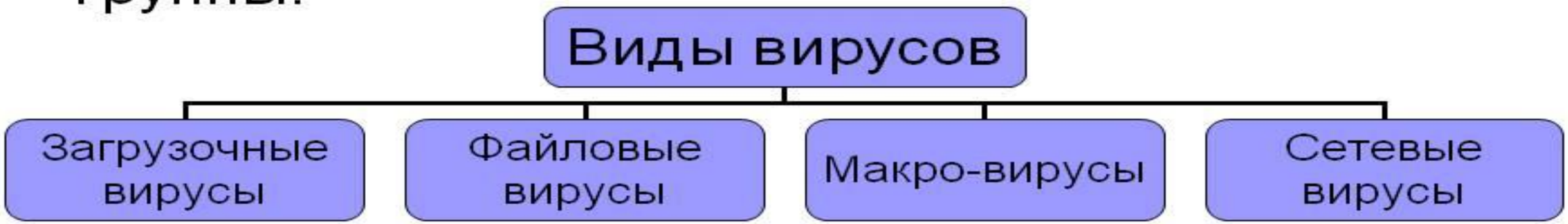
9. Вы обнаружили пропажу или изменение файлов или папок.



Компьютерные вирусы являются вредоносными программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

Виды компьютерных вирусов

- По объектам атаки и распространения вирусы можно разделить на следующие группы:



Защита от вирусов

Основными мерами защиты от вирусов считаются: резервирование (копирование, ежедневное ведение архивов измененных файлов); профилактика (раздельное хранение вновь полученных программ , хранение неиспользуемых программ в архивах, использование специального диска для записи новых программ)

Спасибо за внимание!!!