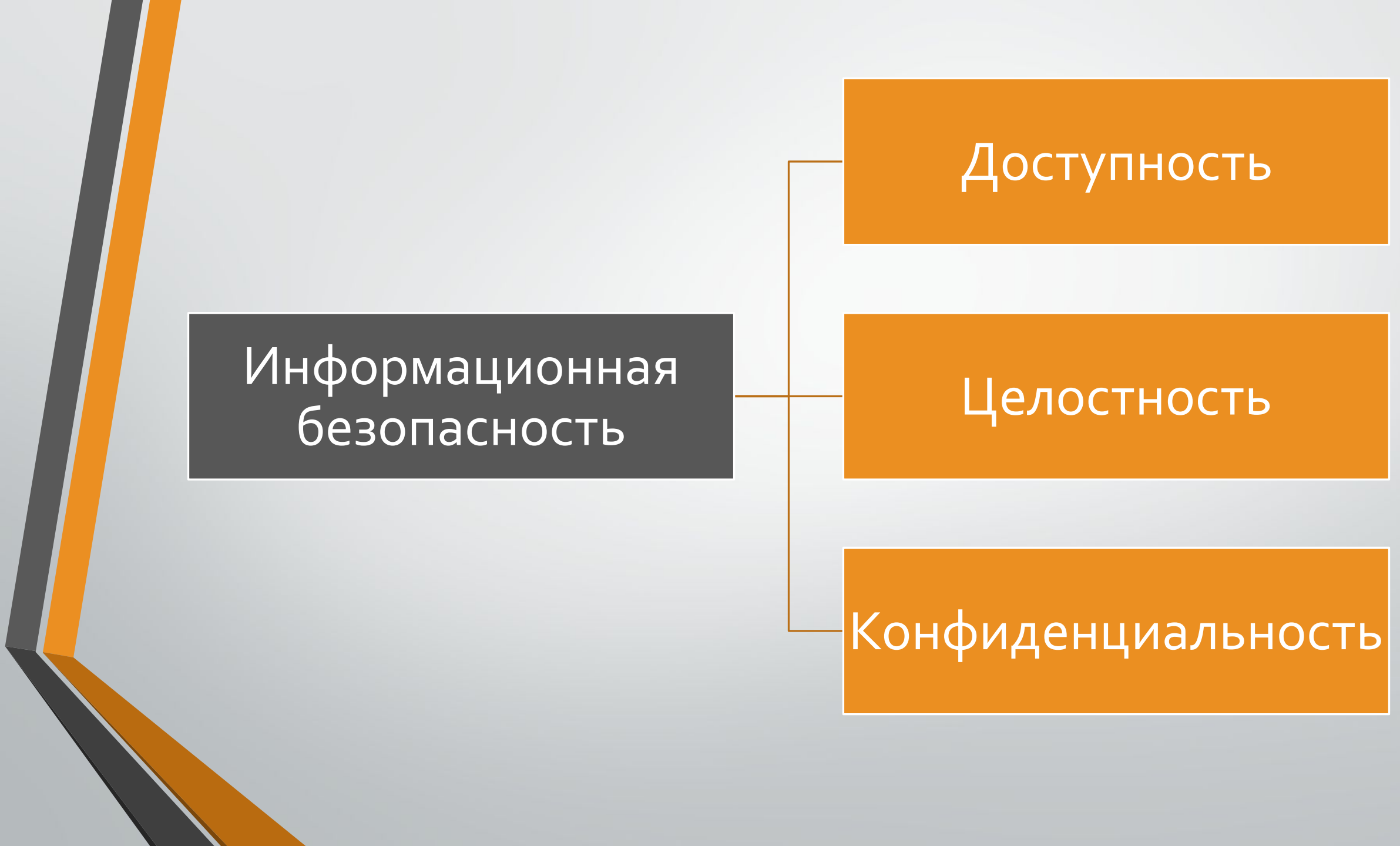
# Информационная безопасность

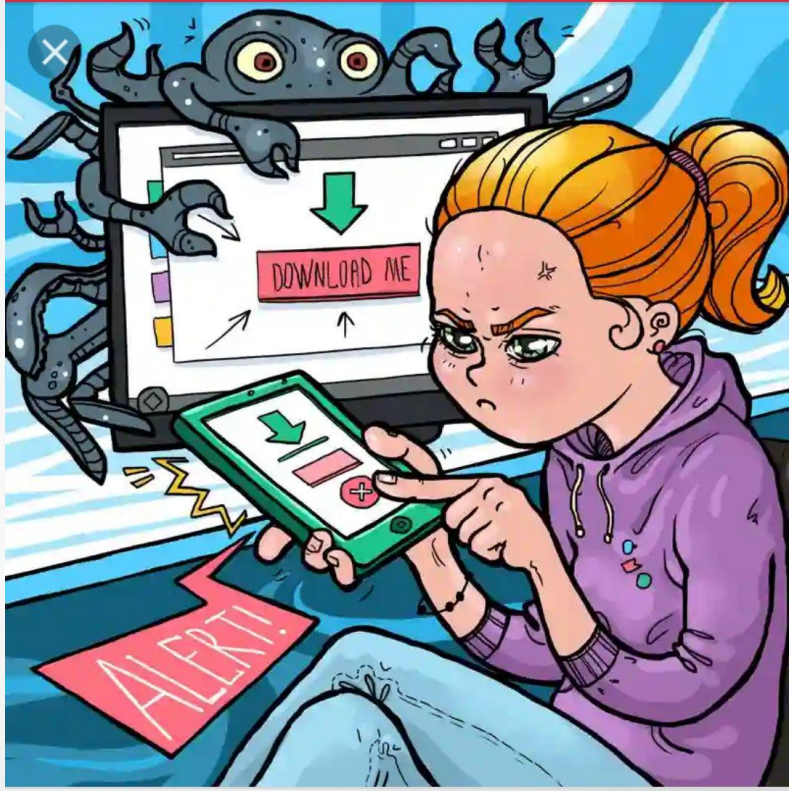
# Что мы сегодня узнаем?

- Вредоносные программы и способы защиты от них
- Безопасность работы в сети Интернет
- Защита личной информации


Информационная безопасность
Доступность
Целостность
Конфиденциальность

- ***Доступность*** информации заключается в том, что информация в безопасном состоянии должна быть доступна для пользователя
- ***Целостность*** информации – это соответствие логической структуры информации определённым правилам, логически корректное её состояние
- ***Конфиденциальность*** информации – это выполнение тех или иных операций с информацией, в соответствии с некоторыми правилами политики безопасности

# Угроза




- Возможность нарушения или нежелательного изменения одного из аспектов безопасности называется угрозой.

- **Вредоносная программа** – программа, целью работы которой является выполнение действий, затрудняющих работу или ущемляющих права пользователя, а также приводящих к нарушению безопасности.

# Классификация вредоносных программ

- К вредоносному программному обеспечению (ПО) относятся: вирусы, черви, трояны, руткиты, бэкдоры, загрузчики


- **Спам** - массовая несанкционированная рассылка сообщений рекламного или несанкционированного характера.

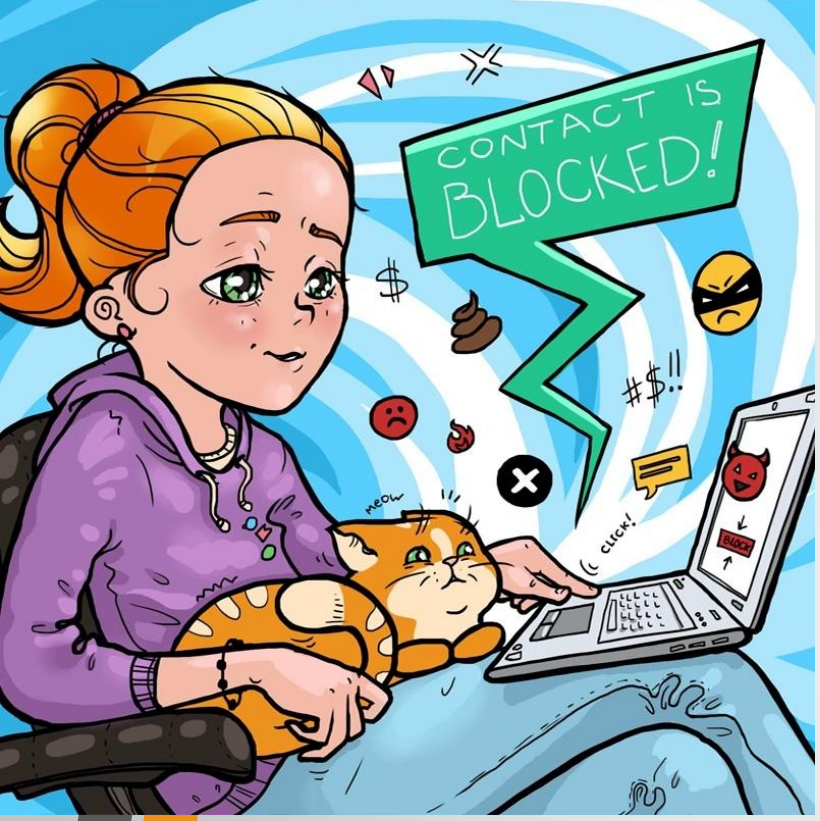
- **Антивирусы**– специализированные программы для выявления и устранения вирусов
- В качестве примеров антивирусных программ можно назвать: антивирус Касперского, Доктор Веб, НОД 32, Аваст




# Для полноценной защиты от появления на личном компьютере вредоносных программ рекомендуется:

- 1) установить и своевременно обновлять систему антивирусной защиты;
- 2) проверять все носители (карты памяти, флэшки и т. д.), которые находились за пределами Вашей системы перед использованием;
- 3) не открывать вложений, полученных от неизвестных адресатов с неизвестными целями;
- 4) регулярно проводить полную проверку системы.

- Для защиты компьютерных сетей или отдельных компьютеров от несанкционированного доступа используют межсетевые экраны.
- Современные **брандмауэры** (межсетевые экраны) – сложные и многофункциональные комплексы программ, задача которых – обеспечение безопасного взаимодействия сетей.




# Доступ к данным

- **Логин** – это сочетание различных символов, которые сервис ассоциирует с пользователем; иначе говоря, это имя пользователя, под которым его будут «видеть» другие пользователи.
- **Пароль** – это сочетание различных символов, подтверждающих, что логином намеревается воспользоваться именно владелец логина.

# К мерам защиты пароля относятся:

- Не разглашать пароль (не записывать их в тетради, не оставлять записанные пароли в доступных местах).
- Не использовать простые пароли. Простыми считаются короткие пароли (до четырёх символов), пароли,состоящие только из букв или только из цифр, предсказуемые сочетания типа qwerty (кверти).
- Не использовать легко отгадываемые пароли – год рождения, своё имя, имена родственников и т. д.
- Нежелательно использовать осмысленные слова.
- Время от времени пароли нужно менять (например, раз в два месяца).

В представленном облаке тэгов выберите стойкие варианты паролей и разместите их в первый столбец, вредоносное программное
обеспечение — во второй столбец, названия антивирусных программ — в третий  столбец.

Nod#Mary-12!

Вирусы

Pro*sL_2020

Целостность

Dr. Web

sVet_4$yOu#

NOD32

Доступность

Трояны

Конфиденциальность

Черви

Avast

| Стойкие пароли | Вредоносное программное обеспечение | Антивирусные программы | Аспекты ИБ |
|---|---|---|---|
| | | | |


теперь я могу...
я научился...
было трудно ...
у меня получилось ...
было интересно ...
меня удивило ...
сегодня я узнал (а) ...

# Спасибо за внимание!