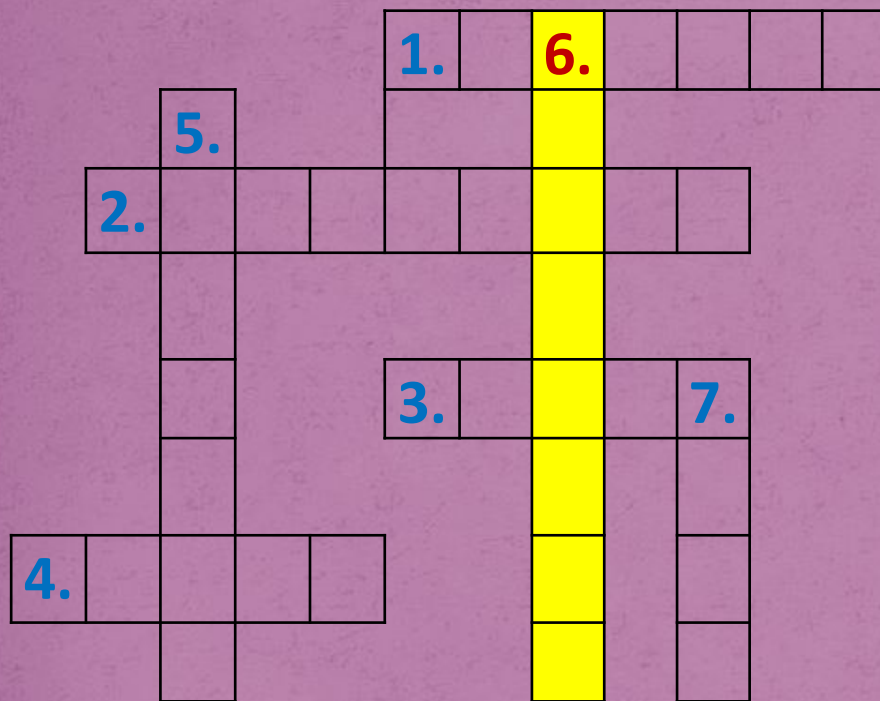


# Чтобы узнать тему внеклассного мероприятия, нужно разгадать кроссворд



## Вопросы:

1. вспомогательная программа, выполняющая некоторое действие (архиватор и т.д.)
2. пользователь на общественных сетевых ресурсах, который следит за соблюдением правил ресурса в определенных разделах, темах.
3. вид вредоносного программного обеспечения
4. часть Интернета
5. информационное наполнение интернет-сайта
6. всемирная система объединённых компьютерных сетей для хранения и передачи информации
7. совокупность логически связанных между собой веб-страниц



# БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ



- **Цель:** сформировать у обучающихся активную позицию в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им.

- **Задачи:**

Обеспечение информационной безопасности обучающихся путём привития им навыков ответственного и безопасного поведения в среде Интернет.

Расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков.

# Основные опасности в Интернете для детей и подростков:

**Кибербуллинг** - коллективная травля одного человека через Интернет.

**Чтобы прекратить атаки кибербуллинга нужно:**

- Заблокировать учетные записи агрессоров, которые они используют для распространения своей ненависти
- Сообщать о фактах кибербуллинга провайдером услуг, как Facebook или Twitter
- Обеспечить защитой ваши пароли, в т. ч. используемые на мобильных устройствах
- Научить детей правилам сетевого этикета.

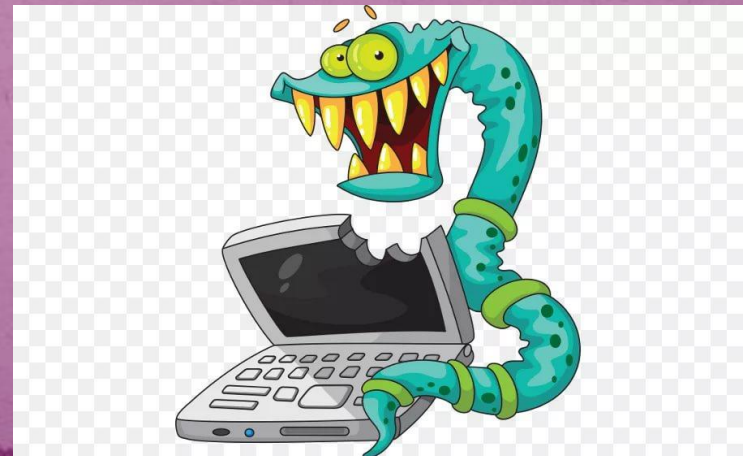
- **Троллинг** - вид виртуальной коммуникации с нарушением этики сетевого взаимодействия, выражающейся в виде проявления различных форм агрессивного, издевательского и оскорбительного поведения.



**Вирусная атака** – одна из самых распространенных угроз сети Интернет. Из-за неё можно потерять информацию, которую вы годами собирали на компьютере.

**Чтобы избежать проникновения вирусов на устройство:**

- Следите за регулярным обновлением операционной системы. Если этого не происходит, вирусам легче найти уязвимые места и проникнуть в компьютер.
- Пользуйтесь антивирусными программами. Они устранят многие угрозы, подскажут, можно ли посещать неизвестный вам сайт, проверят файлы, скачиваемые из интернета.
- Старайтесь не сообщать даже близким друзьям пароли от личного кабинета, банковских карт, социальных сетей, от рабочей и личной почты.



- **Спам** - массовая рассылка корреспонденции рекламного характера лицам, не выразившим желания её получать. Распространителей спама называют спамерами.
- **Фишинг** - один из видов интернет-мошенничества, целью которого является получение доступа к личным данным пользователей - логинам, паролям, данным лицевых счетов и банковских карт. В основном, используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.





## Чтобы избежать спама и фишинговых атак:

- Старайтесь не оставлять адрес почты на сайтах общего доступа (соцсети, форумы, в комментариях).
- Используйте несколько почтовых ящиков для разных целей.
- Никогда не отвечайте на спам. После вашего отказа от рассылки письма могут пойти с новой силой.



- **Раздражающая и потенциально опасная реклама** не только отвлекает от работы, мешает просматривать сайты, вести переписку; загрузка рекламного сообщения на вашем экране съедает часть вашего интернет-трафика и может содержать вредоносный код или вести на сайты с таким кодом.



**Кибершпионаж** – это методы получения секретной конфиденциальной информации без предварительного разрешения владельцев данной информации.

**Чтобы избежать знакомства с программами-шпионами**, старайтесь не устанавливать на компьютер условно-бесплатные программы и не нажимайте на рекламные ссылки, которые открываются во всплывающих окнах.



- **Браузерный эксплойт** - это форма вредоносного кода, которая использует уязвимость в браузере или компоненте системы, с целью изменить настройки без Вашего ведома.

### **Чтобы избежать изменения работы браузера:**

- Не забывайте его регулярно обновлять.
- Проверьте, работает ли на вашем компьютере брандмауэр — специальная программа, которая сканирует данные из интернета и регулирует их передачу на устройство.
- Не скачивайте условно-бесплатное рекламное программное обеспечение.



- **Нежелательный контент** – это материалы содержащие насилие, порнографию, пропаганду наркотических средств, азартных игр, различные компьютерные вирусы, шпионские программы, задача которых получить доступ к информации на компьютере владельца, а также сайты, запрещенные законодательством.

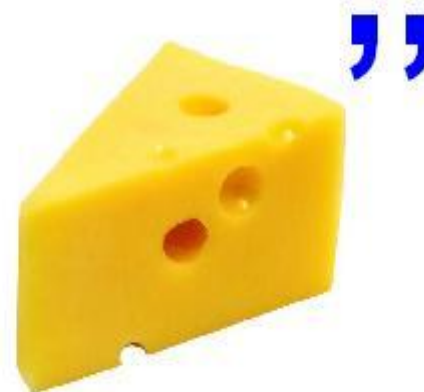
**Чтобы обезопасить детей от нежелательного контента нужно:**

- Установить поисковые фильтры.
- Настроить приватность в браузере или установить программы «родительского контроля».



# Проверим знания

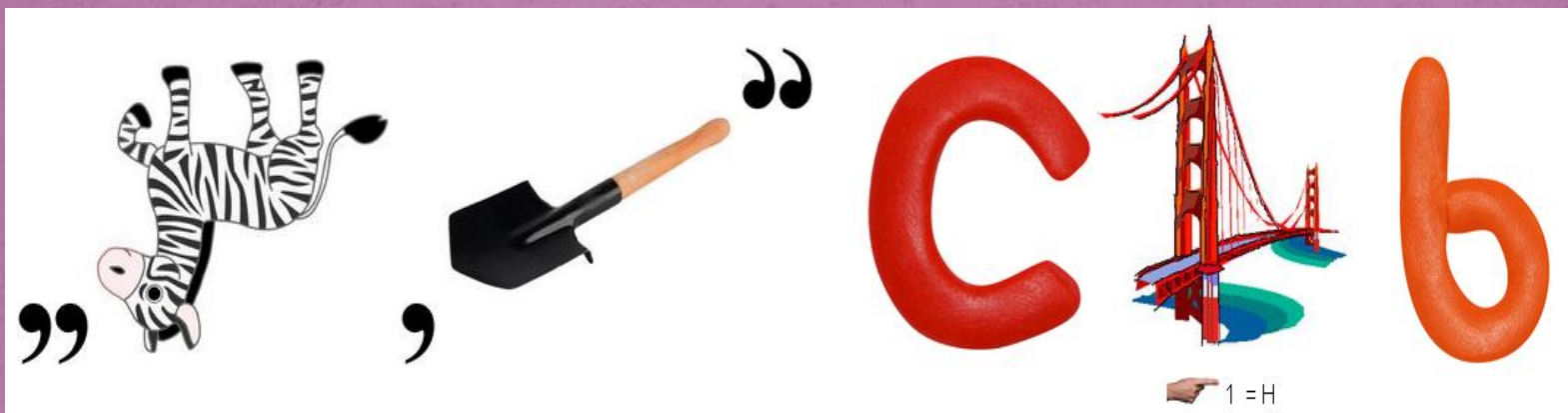
Отгадайте ребусы



вирус



интернет



безопасность





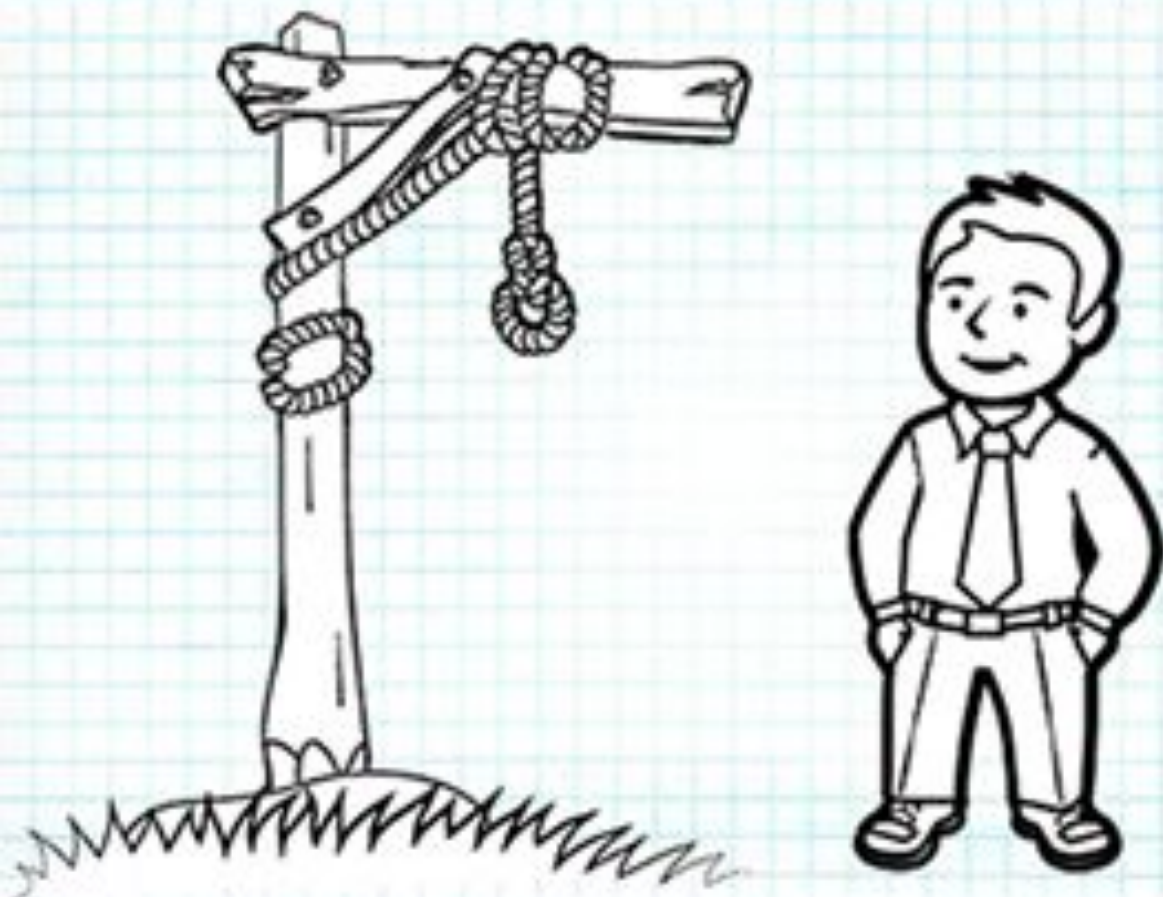
спам



”



атака



ВИСЕЛИЦА

Доступ к информационным ресурсам  
только авторизованным пользователям

<b>К</b>	<b>Н</b>	<b>Е</b>	<b>Ь</b>	<b>И</b>	<b>Л</b>	<b>О</b>	<b>Ц</b>	<b>Т</b>	<b>Н</b>
<b>И</b>	<b>О</b>	<b>Д</b>	<b>С</b>	<b>Ф</b>	<b>Н</b>	<b>М</b>	<b>Ж</b>	<b>Ь</b>	<b>А</b>

● Конфиденциальность

# Процедура проверки идентификационных данных пользователя при доступе к информационной системе

к	н	е	а	и	у	р	ц	т	я
и	б	т	с	ф	н	м	ж	и	а

● Аутентификация

Этот термин, введенный Уильямом Гибсоном, используется для обозначения компьютерных сетей, соединенных между собой. Он часто используется для обозначения сети Интернет

к	т	е	ь	и	р	о	с	т	н
в	о	р	с	ф	н	м	р	б	а

● киберпространство

# Практические советы по безопасности в сети Интернет

- <https://www.youtube.com/watch?v=Xe26HLY9db4>

**Спасибо за внимание!**