



ЕДИНЫЙ УРОК БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

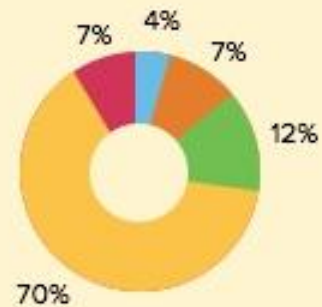
Цикл мероприятий для школьников, направленных на повышение уровня кибербезопасности и цифровой грамотности, а также на обеспечение внимания родительской и педагогической общественности к проблеме обеспечения безопасности и развития детей в информационном пространстве.



О доступе к Интернету

РОДИТЕЛИ

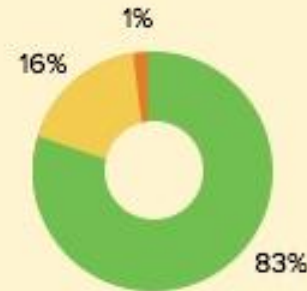
С какого возраста можно разрешать детям пользоваться интернетом?



- До 1 года
- 1-3 лет
- 4-5 лет
- 6 и старше
- Нельзя разрешать пользоваться интернетом

ДЕТИ

Разрешают ли тебе родители пользоваться интернетом?



- Да, всегда
- Да, ограниченное количество времени в день
- Нет

Большинство взрослых (около 70 %) считают, что допускать детей к Интернету следует не раньше 6 лет. При этом более 80 % школьников 6–10 класса заявили, что родители разрешают им пользоваться Интернетом, где бы они ни находились.



ЕДИНЫЙ УРОК
БЕЗОПАСНОСТИ
В ИНТЕРНЕТЕ

ЧЕМ ДЕТИ ЧАЩЕ ВСЕГО ЗАНИМАЮТСЯ В СЕТИ



Общаются
с друзьями



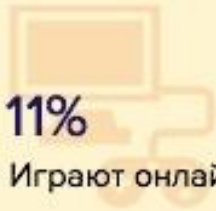
Смотрят видео,
фильмы, сериалы



Слушают музыку



Делают уроки



Играют онлайн



Читают книги,
журналы



Выкладывают
фотографии



Другое



С точки зрения родителей, самыми безопасными устройствами для веб-доступа являются стационарный компьютер (22 %), планшет (21 %) и ноутбук (18 %). У детей же на первое место в пользовании выходит мобильный телефон или смартфон (38 %).



ЕДИНЫЙ УРОК
БЕЗОПАСНОСТИ
В ИНТЕРНЕТЕ

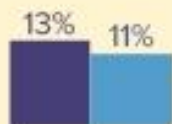
Четверо из пяти детей сталкивались с опасностями в Интернете

Опасности в сети

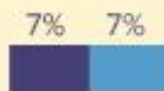
■ С чем столкнулись дети ■ О чем уведомили родителей



Компьютер был заражен вирусом



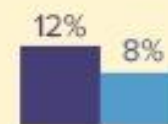
Противоправный контент



Троллинг, киберунижения



Сомнительные сообщения от незнакомцев



Фишинговые рассылки

Источник: Региональная общественная организация «Центр Интернет-технологий» (РОЦИТ)



ЕДИНЫЙ УРОК
БЕЗОПАСНОСТИ
В ИНТЕРНЕТЕ

Угрозы сети

Опасности и угрозы, существовавшие в реальной жизни, модифицировались с приходом интернета

Интернет – средство доставки опасностей

Мошенничест
во

Вирусы

Троллинг и
кибербуллинг

Общение под
ником с
незнакомцами



Вся информация, когда-либо выложенная в сеть, остается там навсегда

Мошенничество

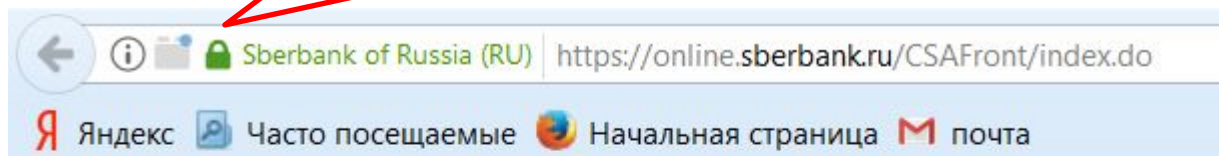
Самый распространенный вид преступности в интернете

Вопрос доверия к сайту, на котором осуществляются финансовые и другие операции в данном случае является решающим. Большое значение имеет имя и репутация сайта. Работайте с проверенными сайтами.

Не тестируйте новые не проверенные сайты.

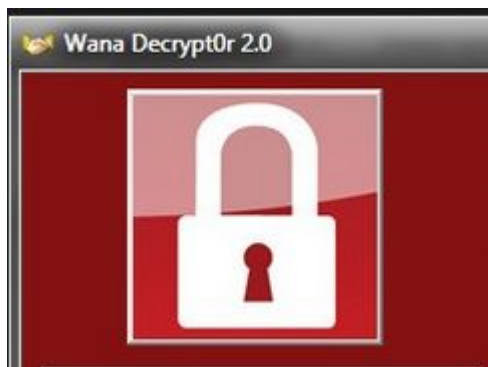


Фишинг самый распространённый вид мошенничества с пластиковыми картами. Для проверки надёжности сайта обратите внимание на адресную строку браузера



Вирус

Написание вирусов это теньевая индустрия промышленных масштабов. Ежедневно появляется до 100 000 вирусов.



Вирусы-
шифровальщики



Троян



СПАМ

Способы заражения:

1. Письма, мессенджеры, социальные сети.
2. Физические носители, распространяемые бесплатно.
3. Мобильные телефоны, планшеты, особенно с ОС Android, во время загрузки и установки приложений



Тролли НГ

Троллинг – форма социальной провокации или издевательства в сетевом общении, получение удовольствия от самого процесса. Задача таких пользователей сети получать эмоциональную реакцию, а не аргументы в дискуссии. (Главный совет – не кормите троллей).



Кибербуллинг – это травля, оскорбления или угрозы, высказываемые жертве с помощью средств электронной коммуникации, в частности, сообщений в социальных сетях, мгновенных сообщений, электронных писем и СМС. С каждым годом стремительно увеличивается количество трагедий, к которым приводит кибербуллинг.



Общение под ником с

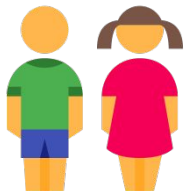
Цели злоумышленников различны, от получения информации до киднеппинга.

СОВЕТ

Проверять достоверность личности.

На Facebook и Twitter – синяя галочка индентификатор личности.

Можно попросить прислать собеседника фото, а затем ещё одно с каким-то условием (с кошкой на руках, в очках, красной кепке и т.п.).



Важно внушить ребенку – не стыдно сообщить взрослым о настойчивых попытках незнакомцев познакомиться в сети, а тем более встретиться.

Родительский контроль. Системы защиты ребенка в сети

| | |
|----------------------|---|
| Настройка ОС | Операционная система «Windows» имеет в своем функционале различные функции родительского контроля, которые родителям необходимо только включить. |
| Поисковая фильтрация | Такие поисковые системы как Yandex и Google позволяют установить семейный фильтр , который ограничивает в поисковой выдаче негативные сайты для ребенка. Использование специально созданных для детей систем «Гугль» и «Спутник.дети» |
| Антивирусное ПО | бесплатный антивирус «KasperskyFree» и программу родительского контроля «Kaspersky Safe Kids» . |
| Интернет Цензор | по умолчанию запрещено все, разрешены только проверенные компанией-разработчиком сайты. |
| NetPolice Lite | разрешает по умолчанию все, запрещает только проверенные компанией-разработчиком сайты и ресурсы, содержание которых программа смогла определить, как наносящие вред здоровью, нравственному, психическому и духовному развитию ребенка. |
| Яндекс DNS | бесплатный сервис от Яндекса для безопасного использования интернета, который фильтрует и блокирует опасные сайты в сети. |
| Мегафон. Опция | «Детский интернет» |
| МТС | Услуга «Родительский контроль» |
| Ростелеком | Услуга «Ребенок в доме» |



<http://kurch-gim2.ru/>

● ИНТЕРНЕТ-БЕЗОПАСНОСТЬ



«Методические рекомендации по заполнению формы сообщения от граждан, юридических лиц, индивидуальных предпринимателей, органов государственной власти, органов местного самоуправления о наличии на страницах сайтов в сети Интернет противоправной информации»

В интернете можно найти информацию и иллюстрации практически на любую тему. Необходимо обеспечить защиту детей от контактов в интернете с нежелательными людьми, от знакомства с материалами недетской тематики или просто опасными для детской психики, от вредоносных программ и интернет-атак.

Безопасность детей в интернете. Системы родительского контроля в сети интернет:

<http://www.сетевичок.пф/roditelyam/roditelskij-kontrol>

В интернете детей подстерегает много опасностей.

- Контакты с нежелательными людьми, в том числе:
 - угроза со стороны интернет-хулиганов;
 - ловушки, расставляемые мошенниками для получения частной информации о вас и ваших детях.
- Нежелательные для просмотра или использования материалы, например:
 - «взрослые» сайты
 - «пиратские» материалы
- Угроза безопасности компьютера.
 - **Попутная загрузка** – когда при простом посещении веб-сайта на компьютер вашего ребенка автоматически загружается вредоносная программа.
 - **Заражение через пиринговые сети (P2P)** – может предоставить доступ к компьютеру вашего ребенка посторонним лицам.
 - **Нежелательная реклама, всплывающие окна и рекламное ПО** – могут автоматически быть установлены при скачивании бесплатных программ или программ для обмена данными.

[KURCHATOV.INFO](http://kurchatov.info)

О ШКОЛЕ

- Сведения об образовательной организации
- Публичные отчеты
- Оценка эффективности деятельности ОО
- Символы гимназии
- История гимназии
- Новости
- Объявления
- Библиотека
- Медицинское обслуживание
- Платные образовательные услуги

БЕЗОПАСНОСТЬ

- Дорога без опасности
- Правила безопасности
- Защита персональных данных

ИНТЕРНЕТ-БЕЗОПАСНОСТЬ

- Интернет-гид. ЭОР
- Обеспечение информационной безопасности школьников