

- проверьте систему на наличие потенциальных угроз.
- Включите функции родительского контроля с помощью операционной системы компьютера или специализированных программ.

Как защитить смартфон ребенка от киберугроз

- Установите ПИН-код на сим-карту устройства, чтобы предотвратить её использование на других устройствах.
- Воспользуйтесь возможностью биометрической аутентификации, такой как распознавание отпечатка пальца или лица, чтобы надёжно защитить смартфон и его содержимое.
- Активируйте службы геолокации, чтобы иметь возможность контролировать местонахождение устройства ребёнка.
- Настройте функции родительского контроля с помощью операционной системы или отдельных приложений.

Топ бесплатных программ родительского контроля

- **Google Family Link.** Гибкая программа родительского контроля, встроенная в систему Android, начиная с 8-й версии. На этих устройствах вам не понадобятся дополнительные программы.
- **Kaspersky Safe Kids.** Программа родительского контроля от создателей антивируса Kaspersky Lab. Приложение помогает следить за местонахождением ребёнка и использованием устройств, блокирует неподходящий контент и учит поддерживать цифровой баланс.
- **«Родительский контроль» в iOS.** Пользователям не нужно качать дополнительные программы в последних версиях системы на айфоне — функция родительского контроля в нём уже предусмотрена.
- **KIDDOZ.** Программа родительского контроля, предлагающая не только запреты, но и развлечения для детей. Она позволяет получить контроль над установленными играми и приложениями, находить исключительно детские сайты в браузере, добавлять несколько профилей.
- **Kids Place.** Программа родительского контроля для ограничения времени, проведённого за гаджетом. Работает по принципу блокировки доступа к приложениям. Для доступа к настройкам приложения или списку игр и программ на смартфоне требуется ввести ПИН-код.



Школьный меридиан

Информационно-просветительская газета для родителей

Безопасность детей в Интернете: советы для родителей

Выпуск №7, февраль 2024-2025 гг.

Если на самом деле Интернет может многое предложить тем, кто знает, что ищет, то тот же Интернет столь же способен довершить глупость тех, кто ориентируется в нем без компаса.

Сегодня в номере:

- Что такое информационная безопасность в интернете для детей
- Что угрожает ребенку в Интернете
- Возрастные рекомендации по безопасному использованию Интернета детьми.
- Как защитить компьютер и смартфон ребенка от киберугроз.
- Топ бесплатных программ родительского контроля.

Что такое информационная безопасность в Интернете для детей

Безопасный интернет для детей — это цифровое пространство, в котором дети могут безопасно образовываться и развлекаться без потенциальных угроз: кибербуллинга, неприемлемого контента, мошенничества.



Что такое безопасный интернет для детей? Основные составляющие безопасного интернета для детей это:

1. **Контролируемый доступ.** Родители должны контролировать, какие сайты посещают их дети и устанавливать фильтры для блокировки нежелательного контента.
2. **Образование и предупреждение.** Важно, чтобы дети знали о возможных рисках в интернете. Родители должны объяснять, какие сайты безопасны, как правильно общаться в сети и какие действия и влияния могут представлять угрозу.
3. **Конфиденциальность.** Дети должны понимать важность защиты личной информации. Родителям нужно объяснить, какую информацию о себе нельзя выкладывать в сети, какой контент нельзя публиковать в социальных сетях и т.д.

4. **Самоконтроль и ответственность.** Дети должны уметь самостоятельно принимать решения о том, что безопасно и допустимо делать в интернете. Это требует воспитания чувства ответственности за свои действия в сети.
5. **Мониторинг и сопровождение.** Родители должны активно участвовать в онлайн-жизни своих детей. Нужно беседовать о том, что происходит в сети, какие игры и приложения они любят, с кем общаются.

Что угрожает ребенку в Интернете

Кибербуллинг

Травля в Сети — это угрозы и оскорбления агрессивно настроенных пользователей.

Запрещённый контент

Запрещённый контент — это всё, что не должно быть доступно несовершеннолетнему ребёнку. Однако, дети и подростки посещают сайты и смотрят фильмы и сериалы, не соответствующие их возрасту.

Мошенничество

Мошенники обманывают детей и крадут деньги с помощью бесплатных приложений, тестов в социальных сетях и почтовых рассылок: они предлагают жертвам перейти по ссылке, ввести номер телефона или банковской карты родителей, отправить сообщение в бесплатных онлайн-играх, где дети могут покупать дополнительное снаряжение, оружие и способности за реальные деньги.

Кибергрумминг

Кибергрумминг — это широкий спектр мошеннических действий в Сети, когда преступники обманом получают личные данные или деньги за несуществующие товары и услуги. Часто мошенники используют взломанные аккаунты пользователей для массовой рассылки сообщений среди списков контактов.

Вредоносное ПО

Вредоносное ПО — это программы, которые заражают компьютеры. Последствием заражения может стать кража конфиденциальной информации: паролей, номеров банковских карт и личного контента.

Доступ к личной информации

Даже если смартфон или компьютер подключён к домашней сети, информация, которую дети оставляют или ищут в веб-пространстве, особенно в соцсетях, может быть доступна любому.

Возрастные рекомендации по безопасному использованию Интернета детьми

2-4 года

- Запретите самостоятельный доступ в интернет
- Исключите пугающие изображения
- Не разрешайте переходы по ссылкам
- Ограничьте экранное время



- Обучайте базовым навыкам через возрастные игры

5-7 лет:

- Запретите самостоятельный доступ к интернету и телефонам
- Исключите пугающие изображения
- Не допускайте переходов по ссылкам
- Используйте детские поисковики с родительским контролем
- Ограничьте время в интернете и составьте список разрешённых сайтов
- Держите устройства на виду и учите конфиденциальности



8-10 лет

- Обсуждайте с детьми их интересы и интернет-опасности
- Учите их не разглашать личную информацию
- Объясняйте правила общения и безопасность
- Проводите время в интернете вместе или ограничьте доступ одобренными сайтами
- Установите родительский контроль и используйте фильтры



11-13 лет

- Не размещайте интернет-устройства в детских комнатах
- Настройте родительский контроль и фильтры
- Контролируйте все устройства с доступом в интернет
- Требуйте от детей рассказывать о своих действиях в сети
- Запретите разглашение личной информации и организовывать встречи с незнакомцами
- Защищайте от буллинга и других негативных явлений



14-18 лет

- Установите правила использования интернета
- Используйте родительский контроль и фильтрацию
- Обсуждайте с подростками их интернет-друзей и действия
- Убедите их не общаться с незнакомцами и спрашивать ваше одобрение на новые знакомства
- Учите не разглашать личную информацию и обсуждайте неэтичное поведение в сети



Как защитить компьютер ребенка в киберпространстве

1. Создайте отдельную учётную запись для ребёнка без прав администратора, чтобы ограничить его возможности.
2. Регулярно обновляйте операционную систему, чтобы исправить уязвимости, которыми злоумышленники могут воспользоваться.
3. Используйте только лицензионные программы, чтобы избежать заражения компьютера вредоносными файлами.
4. Установите антивирусное программное обеспечение и регулярно

