Министерство образования и науки Хабаровского края
Краевое государственное автономное образовательное учреждение дополнительного образования «Центр развития творчества детей (Региональный модельный центр дополнительного образования детей Хабаровского края)»
ЦЕНТР ТЕХНИЧЕСКОГО И ЦИФРОВОГО ОБРАЗОВАНИЯ «ТЕХНО-IT-КУБ»

#вместекуспехукаждого

Кибергигиена, как способ защиты от буллинга в сети Интернет

Методические материалы

г. Хабаровск, 2023 г.

Печатается по решению
научно-методического совета
КГАОУ ДО РМЦ
протокол № 1 от 31.01.2023 г.

Кибергигиена, как способ защиты от буллинга в сети Интернет. Методические материалы / составители: Е.А. Кудревич, Е.А. Фомина, В.В. Шевченко — Хабаровск: КГАОУ ДО РМЦ, 2023.— 28 с.

Ответственный редактор: В.В. Шевченко
Ответственный за выпуск: Е.А. Кудревич
Дизайн обложки: Ю.А. Лубашова

Практически невозможно отделить детей от интернета. Однако, несмотря на то, что Интернет является развлекательной и образовательной платформой, он сопряжён с различными рисками для учащихся, одним из наиболее заметных из которых является кибербуллинг.

Данные методические материалы направлены на то, чтобы начать работу по выявлению инцидентов кибербуллинга, показать педагогам различные возможности предотвращения и вмешательства в ежедневную агрессию, которая происходит в образовательных организациях и изучить способы безопасного поведения в сети Интернет.

Методические материалы рекомендованы педагогическим работникам края, родителям обучающихся.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Технологии и киберпространство стали неотъемлемой частью современного образования. Дети постоянно используют новейшие технологии, включая ПК, смартфоны, интернет и социальные сети для обучения и развлечения.

Практически невозможно отделить детей от интернета. Однако, несмотря на то, что Интернет является развлекательной и образовательной платформой, он сопряжён с различными рисками для учащихся, одним из наиболее заметных из которых является кибербуллинг.

Кибербуллинг вызывает растущую озабоченность как родителей, так и педагогов во всем мире. Около 40 % детей в возрасте 12–17 лет стали жертвами кибербуллинга в своей жизни. Поскольку мир становится всё более и более оцифрованным, вполне естественно, что количество случаев кибербуллинга будет увеличиваться. Таким образом, педагоги и родители должны как можно скорее предпринять шаги, чтобы свести к минимуму риск кибербуллинга.

ПОНЯТИЕ И ОСНОВЫ ПРОФИЛАКТИКИ КИБЕРБУЛЛИНГА СРЕДИ ДЕТЕЙ И ПОДРОСТКОВ

Кибербуллинг: типы, причины и последствия

Кибербуллинг — это онлайн-форма травли, которая происходит через интернет с помощью электронных устройств, таких как компьютеры, смартфоны, планшеты и т. д.

Есть несколько типов онлайн-буллинга, которые составляют кибербуллинг. Некоторые из них включают:

- **Исключение:** исключение кого-либо из онлайн-форума или группы чата в социальной сети.
- **Преследование:** отправка кому-либо текстовых сообщений и сообщений угрожающего и оскорбительного характера.
- **Киберпреследование:** постоянное отслеживание действий других в сети и преследование их в сети.
- **Выдача себя за другое лицо:** кража чьей-либо личности и размещение неприемлемого контента в Интернете.
- **Троллинг:** намеренное размещение подстрекательских сообщений о расе, возрасте, религии и т. д. человека с целью вызвать конфликт и причинить вред.

Кибербуллинг наносит серьёзный вред физической, психической, социальной и эмоциональной жизни жертвы. Подросток не сможет сосредоточиться на учёбе, если над ним издеваются. Низкие оценки, недосыпание, пропуск занятий, развитие социальной тревожности, психические расстройства, депрессия и суицидальные мысли — всё это последствия, которые кибербуллинг может вызвать у жертвы.

Кибербуллинг стал довольно распространённым явлением в школах, когда стало популярным дистанционное обучение. Поскольку занятия, задания и отчёты всё чаще проводятся в сети Интернет, учащиеся вынуждены проводить в нём гораздо больше времени, что приводит к росту числа случаев кибербуллинга.

Трудно распознать и противостоять кибербуллингу, поскольку он происходит в интернете. Поскольку киберпространство даёт анонимность, хулиганы могут использовать его для повторных действий, не опасаясь последствий. Это также создаёт серьёзные проблемы для педагогов, поскольку они не могут быть свидетелями агрессивного поведения и не могут противостоять ему. Тем не менее, есть несколько стратегий, которые педагоги могут использовать, чтобы остановить кибербуллинг.

Многие предупреждающие признаки того, что происходит кибербуллинг, связаны с использованием ребёнком своего устройства. Поскольку дети проводят много времени со своими устройствами, увеличение или уменьшение использования может быть менее заметным. Важно обращать внимание на внезапные изменения в цифровом и социальном поведении ребёнка. Вот некоторые из предупреждающих признаков того, что ребёнок может быть вовлечён в кибербуллинг:

1. Заметное, быстрое увеличение или уменьшение использования устройств, включая текстовые сообщения.
2. Ребёнок проявляет эмоциональные реакции (смех, гнев, огорчение) на происходящее на его устройстве.
3. Ребёнок прячет свой экран или устройство, когда другие находятся рядом, и избегает обсуждения того, что он делает на своём устройстве.
4. Аккаунты в социальных сетях закрываются или появляются новые.
5. Ребёнок начинает избегать социальных ситуаций, даже тех, которые доставляли ему удовольствие в прошлом.
6. Ребёнок замыкается в себе, впадает в депрессию, теряет интерес к людям и занятиям.

РЕКОМЕНДАЦИИ ДЛЯ ПЕДАГОГОВ ПО РАБОТЕ С РОДИТЕЛЯМИ ПО ОБЕСПЕЧЕНИЮ КИБЕРГИГИЕНЫ

Воспитывая будущих цифровых граждан, важно научить детей осознанно и ответственно относиться к использованию информации в интернете, научить их правилам сетевого этикета и возможностям для защиты собственного творчества в сети.

Информационная безопасность в отношении детей обеспечивается комплексом мер и включает в себя государственное регулирование (Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»), процесс воспитания и обучения в образовательной организации и дома, а также набор основных правил технического и организационного характера для саморегулирования цифрового поведения пользователей.

Родителям рекомендуется своевременно обращать внимание и не допускать просмотра ребёнком медиапродукции с информацией, причиняющей вред его психическому здоровью и нормальному возрастному развитию. Осуществление родительского контроля за информационной безопасностью ребёнка поможет избежать причинения его здоровью физического, психического и морального вреда.

В процессе обучения и воспитания детей рекомендуется:

1. Формировать основы информационной компетентности, а именно:

- умение искать и анализировать информацию в интернете,
- подвергать её критической оценке, сопоставлять различные факты и данные;
- навыки создания информационных объектов с использованием цифровых ресурсов: сетевых, текстовых, изобразительных, аудио и видео.

2. Обучать правилам «компьютерной гигиены»: проводить зарядку для глаз, физкультминутки, контролировать время пребывания за компьютером, информировать о правилах безопасного использования интернета.

3. Научить выстраивать личное пространство при коммуникации в интернете:

- презентовать себя в интернете;
- выстраивать социальную сеть взаимоотношений в интернете (друзья, знакомые);
- взаимодействовать с другими пользователями в сообществах;
- соблюдать этические правила и социальные нормы в отношениях;
- использовать различные модели общения в зависимости от вида ресурса, цели и аудитории;

- научить избегать и справляться с основными коммуникационными рисками (общение с незнакомцами, агрессия и сексуальные домогательства).

4. Формировать основы экономической грамотности при использовании интернета в потребительских целях:

- осознавать собственные потребности и возможности их удовлетворения с помощью различных интернет-технологий;
- оценивать основные риски, связанные с приобретением и потреблением товаров и услуг в интернете (например, распознавать интернет-мошенничество, недобросовестную торговлю и т. д.).

Основные правила для саморегулирования цифрового поведения пользователей

1. Установите антивирусное программное обеспечение.

2. Используйте средства контентной фильтрации. К контентным фильтрам может относиться как специализированное программное обеспечение, которое блокирует доступ к сайту полностью, так и расширения для браузеров, которые блокируют нежелательный контент.

3. Подключите дополнительную услугу от поставщика интернета. У большинства поставщиков интернета (как мобильного, так и домашнего) есть специальная услуга по блокировке нежелательного контента и сайтов, например: опция «Ребёнок в доме» для домашнего интернета от ПАО «Ростелеком», услуга «Родительский контроль» от МТС и «Билайн», услуга «Детский интернет» от «Мегафон».

4. Создавайте резервные копии. Реалии сегодняшнего дня таковы, что файлы можно легко «потерять», например, случайно удалить или «поймать» вирус, который преобразует все файлы без возможности восстановления, или устройство, на котором вы храните файлы, может выйти из строя. Чтобы избежать подобных ситуаций создавайте резервные копии Ваших документов. Самым оптимальным вариантом решения будет хранение Ваших файлов на нескольких различных устройствах, таких как жёсткий диск компьютера, CD или DVD диски, внешние переносные устройства (флэшка или внешний жёсткий диск), облачные файловые хранилища.

5. Используйте безопасные пароли. Нельзя использовать в качестве паролей даты рождения, номера телефонов, имена и фамилии. Лучше использовать абстрактные пароли, состоящие из различных цифр и букв. При создании паролей используйте сочетание прописных и строчных букв, цифр и знаков препинания. Не храните логины и пароли в записной книжке или на видном месте. Используйте для этого специальные программы, например, KeePass Password Safe. Можно использовать программы для генерации паролей, например, KeePass Password Safe.

6. Установите семейные правила работы за компьютером, например, отвечающие на следующие вопросы:

- Какие сайты могут посещать дети и что они могут там делать?
- Сколько времени дети могут проводить в сети?
- Что делать, если детей что-то беспокоит при посещении интернета?
- Как защитить личные данные?
- Как следить за безопасностью?
- Как вести себя вежливо?
- Как правильно общаться в интернете?

7. Изучите основы сетевого этикета вместе с детьми. Необходимо придерживаться тех же правил вежливого общения, что и в реальной жизни. Также необходимо помнить о своей репутации при публикации материалов в интернете, уважать чужое мнение и право на личную переписку, не использовать сеть для хулиганства, распространения сплетен и угроз.

8. Расскажите детям об угрозах в сети:

- угроза заражения вредоносным программным обеспечением;
- доступ к незаконному и нежелательному содержимому;
- контакты с незнакомыми людьми в социальных сетях и мессенджерах;
- раскрытие личных данных;
- азартные игры в интернете;
- неконтролируемые покупки, в том числе в онлайн-играх.

9. Научите детей общению в сети. Беседуйте с детьми об их друзьях и случайных знакомых в интернете. Настаивайте, чтобы дети никогда не соглашались на личные встречи с виртуальными друзьями. Приучите вашего ребёнка сообщать вам о любых угрозах или тревогах, связанных с интернетом, спрашивать совета родителей.

10. Научите ребёнка безопасному просмотру страниц и загрузке файлов:

- не переходить по ссылкам от незнакомых людей, не нажимать всплывающие окна;
- не игнорировать предупреждения антивируса о зараженных страницах;
- не открывать вложенные файлы из сообщений, если отправитель не известен;
- при копировании информации с интернет-страниц обязательно давать ссылку на источник, не нарушать закон об авторском праве;
- разрешённое для скачивания программное обеспечение скачивать только с официального сайта производителя;
- все скачиваемые файлы обязательно сканировать с помощью антивируса.

РОДИТЕЛЬСКИЙ КОНТРОЛЬ НА МОБИЛЬНОМ УСТРОЙСТВЕ

Родительский контроль — это ограждение ребёнка от нежелательного контента в интернете, на который чадо может наткнуться даже совершенно случайно, а также защита от слишком большого количества времени, проведённого в сети и в смартфоне (или планшете).

Родительский контроль осуществляется установкой специализированных мобильных приложений, которые могут работать как на Android, так и на iOS. Эти мобильные приложения обычно позволяют управлять настройками и просматривать отчёты с самого телефона или планшета.

Для того, чтобы не вызвать у ребёнка внутренний протест против контроля и ограничения, рекомендуется использовать приложение родительского контроля в качестве системы слежения, которая только контролирует действия ребёнка в мобильном устройстве, но не ограничивает их. В то же время родитель получает полный отчёт об активности ребёнка, может его проанализировать, сделать выводы и применить методы педагогического воздействия.

На что необходимо обратить внимание при выборе мобильного приложения родительского контроля

1. **Наличие веб-фильтрации.** Особенностью контроля детей является способность предотвращать доступ к неуместным или опасным веб-сайтам.

2. **Возможность блокировки приложений**. Одна из областей — способность предотвращать использование детьми выбранных приложений, например, программа автоматически блокирует новые приложения, которые ребёнок устанавливает, пока родители их не одобрят.

3. **Возможность ограничения времени**. Некоторые сервисы позволяют указать, сколько часов (или минут) в день ребёнок может потратить на какое-либо устройство, а также график, когда это можно делать.

4. **Отслеживание местоположения.** Приложение мобильного родительского контроля должно иметь возможность отслеживать текущее местоположение ребёнка и сохранять данные о местоположении в истории. Также важно, чтобы был уровень контроля над уведомлениями и частотой отчётов о местоположении.

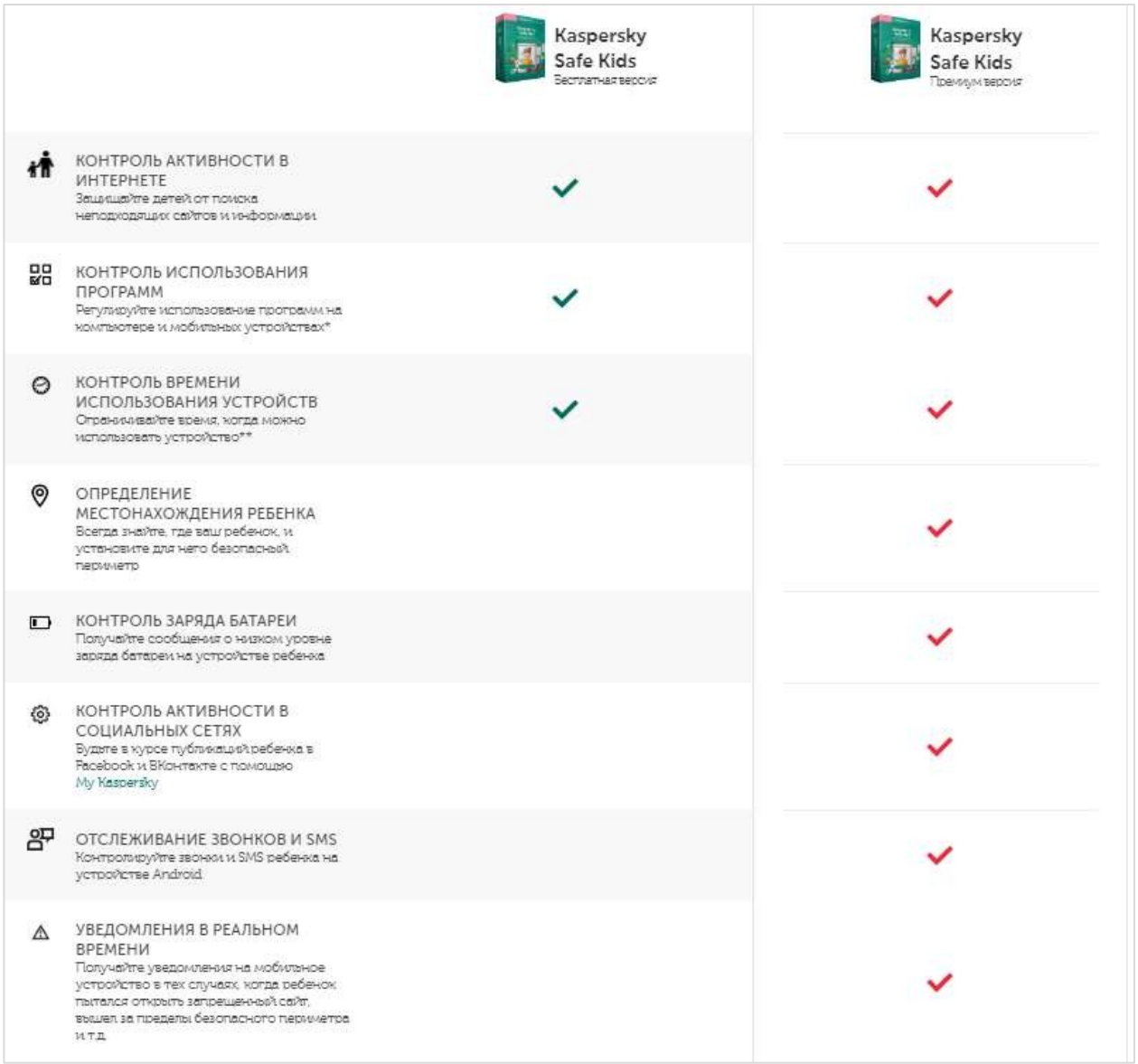
5. **Связь и дополнительные услуги.** Некоторые приложения для родительского контроля позволяют записывать и отслеживать, с кем и о чём общается ваш ребёнок.

6. **Рейтинг и отзывы реальных пользователей.**

Обзор мобильных приложений родительского контроля

1. **Родительский контроль и GPS: Kaspersky SafeKids.** Оценка «Отлично» в независимом обзоре PC Mag.

Также доступно для устройств на базе Mac, Windows и др.



Скачать приложение можно в GooglePlay | AppGallery | AppStore

Сайт: https://www.kaspersky.ru

2. Norton Family parental control.

Удостоенное наград программное обеспечение для родительскогоконтроля

Возможности продукта	Norton Family Premier	Norton Security Premium
+ Контроль веб-сайтов	✓	✓
+ Контроль времени	✓	✓
+ Контроль поиска	✓	✓
+ Контроль социальных сетей	✓	✓
+ Защита личной информации	✓	✓
+ Оповещения по эл. почте	✓	✓
+ Запрос доступа	✓	✓
+ Журнал действий	Последние 30 дней	Последние 30 дней
+ Удобный веб-портал	✓	✓
+ Мобильное приложение для родителей[2]	✓	✓
+ Контроль расположения[1,2]	✓	✓
+ Контроль мобильных приложений[2]	✓	✓
+ Контроль SMS-сообщений[2,3]	✓	✓
+ Контроль просмотра видео[4]	✓	✓
+ Мгновенная блокировка	✓	✓
+ Ежемесячные или еженедельные отчеты	✓	✓
+ Лучшая защита от вирусов и вредоносных программ[5]	×	✓
+ 100% защита от вирусов[6]	×	✓
+ Защита идентификационных данных	×	✓
+ Поддержка 10 устройств	×	✓
+ Автоматическое резервное копирование	×	✓
+ Облачное хранилище на 25 ГБ	×	✓
+ Лучший в своем классе продукт для защиты[5]	×	✓
+ Глобальное обнаружение угроз	×	✓

Скачать приложение можно в GooglePlay | AppGallery

Сайт: https://family.norton.com/web/

3. **Kid security — Родительский контроль — Трекер**

Родителю доступна информация:

- Звук вокруг: чтобы удостовериться, что с ребёнком всё в порядке, можно прослушать звук вокруг него.
- Местоположение ребёнка, отслеживаемое в режиме реального времени.
- Статистика использования приложений на устройстве ребёнка.
- Заряд батареи смартфона / планшета ребёнка.
- Режим звука, включенный в настоящий момент на мобильномустройстве ребенка (Без звука / Вибрация/ Звук).
- Мониторинг всех входящих и исходящих вызовов.
- Родитель может удалённо включить громкость мобильного устройства ребёнка, чтобы связаться с ним, в случае, если звук выключен.
- Управление уведомлениями, которые вы хотели бы получить в случае изменений на мобильном устройстве ребёнка.

Скачать приложение можно в GooglePlay | AppGallery | AppStore

4. **Родительский контроль Screen Time.**

Возможности в бесплатной версии:

- Отслеживать со своего смартфона, сколько времени дети проводят перед экранами мобильных устройств.
- Просматривать, какие приложения используются и в течение какого времени.
- Получать уведомления, когда дети пытаются установить новое приложение.
- Следить, какие веб-сайты посещаются с детских устройств.
- Просматривать, какие поисковые запросы вводятся с детского устройства.

Скачать приложение можно в GooglePlay | AppStore

РОДИТЕЛЬСКИЙ КОНТРОЛЬ НА СТАЦИОНАРНОМ УСТРОЙСТВЕ (ОС WINDOWS)

Родительский контроль в Windows — это встроенная функция всех операционных систем от Microsoft, с помощью которой родители могут организовать работу ребёнка за компьютером, запретить использование определённых программ или сайтов и просматривать статистику активности ПК. Функция пригодится в любой семье, ведь вы всегда будете в курсе, сколько времени ребёнок проводит за компьютером, какие сайты он просматривает и в какие игры играет. Одна из основных опций родительского контроля — настройка времени включения ПК. Вы можете запретить ребёнку включать компьютер, к примеру, после шести вечера. В результате, он никак не сможет войти в свою учётную запись.

С помощью стандартной опции контроля родители будут иметь возможность отслеживать все действия, которые выполнял ребёнок за компьютером, видеть какие программы он запускал и сколько времени они работали. Система предоставляет учётной записи администратора ПК детальный отчёт о детских учётных записях. Таким образом, можно получить наиболее полную картину о взаимодействии ребёнка и компьютера на протяжении недели или месяца.

Родительский контроль на компьютере Windows позволяет инсталлировать программы и игры, учитывая их возрастное ограничение. Ребёнок даже не будет подозревать о наличии активной функции контроля. В процессе установки игр система автоматически проверит цифровую подпись инсталлятора, которая содержит название игры, компанию разработчика и возрастной ценз. Если возраст выше разрешённого вами, приложение не установится под видом ошибки системы.

Опция родительского контроля в ОС Windows осуществляет полный контроль над работой с браузером, поисковыми системами и различными веб-ресурсами. Отслеживайте историю активности ребёнка в интернете, ограничивайте использование сайтов, в описании которых есть указанные вами ключевые слова; устанавливайте ограничение времени работы за компьютером, выставляйте временной промежуток, во время которого ребёнок сможет включить компьютер. По истечении нужного времени работа устройства будет автоматически завершена. Такая опция позволит ребёнку организовать своё дневное расписание и поможет привыкнуть к ограниченному сидению за компьютером без постоянных просьб родителей выключить компьютер.

Настройка функции родительского контроля в ОС Windows

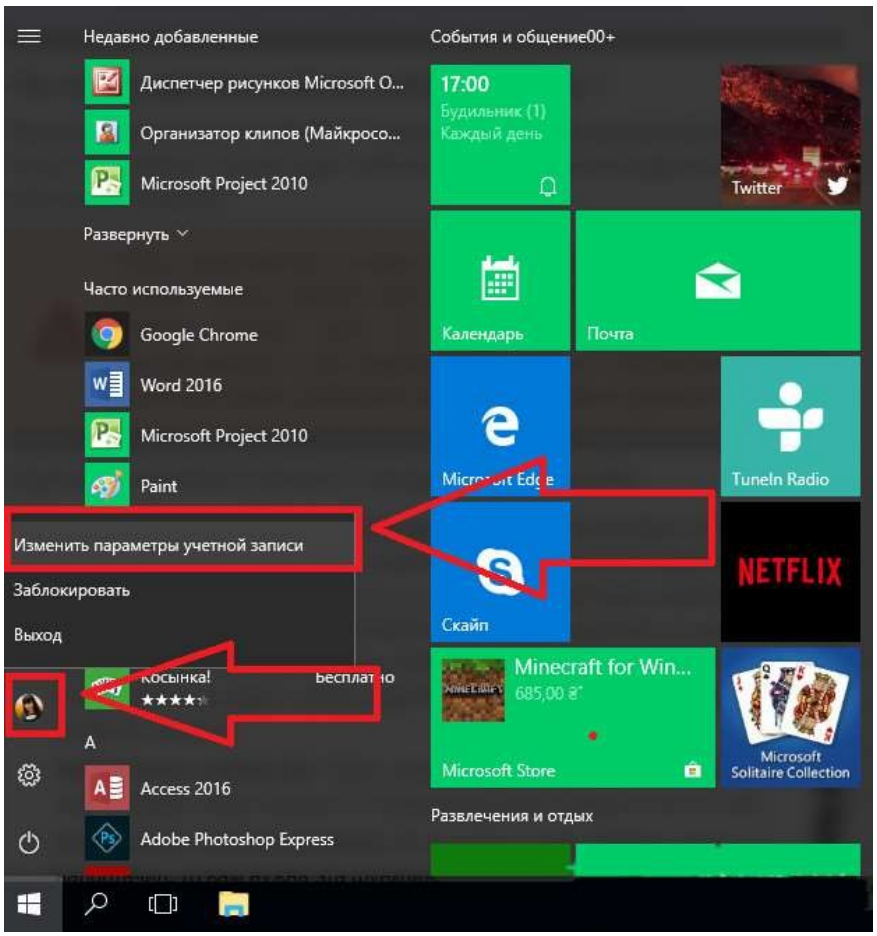
Перед настройкой родительского контроля в любой из версий Windows, необходимо создать на компьютере две учётные записи — для вас и ребёнка. Если же учётная запись родителей будет без пароля, ребёнок сможет без проблем обойти все выставленные ограничения, авторизовавшись под записью администратора.

Создание учётных записей с паролем

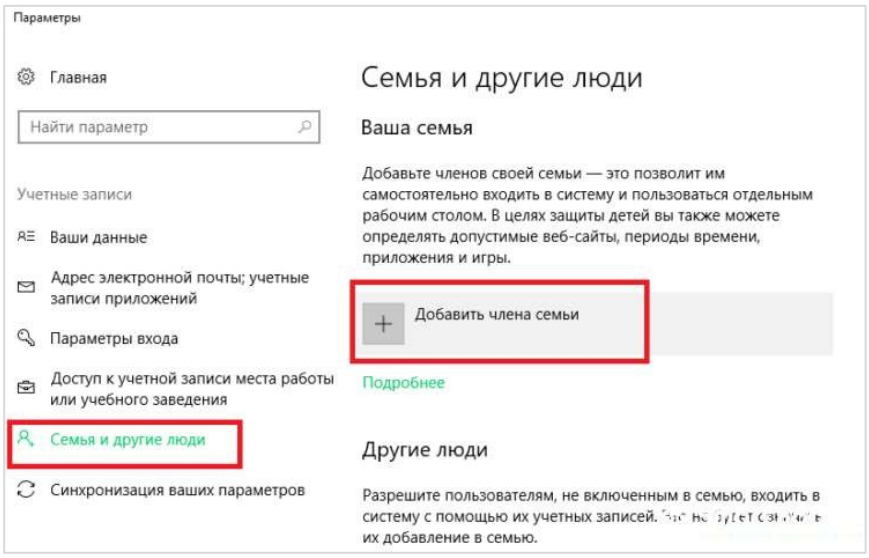
Аккаунт ребёнка не обязательно защищать паролем. Без ввода кодового слова владельцу учётной записи будет проще начать работу с компьютером. Достаточно просто кликнуть на фотографию профиля и дождаться загрузки рабочего стола.

Следуйте инструкции, чтобы создать несколько пользователей системы в Windows 8/10:

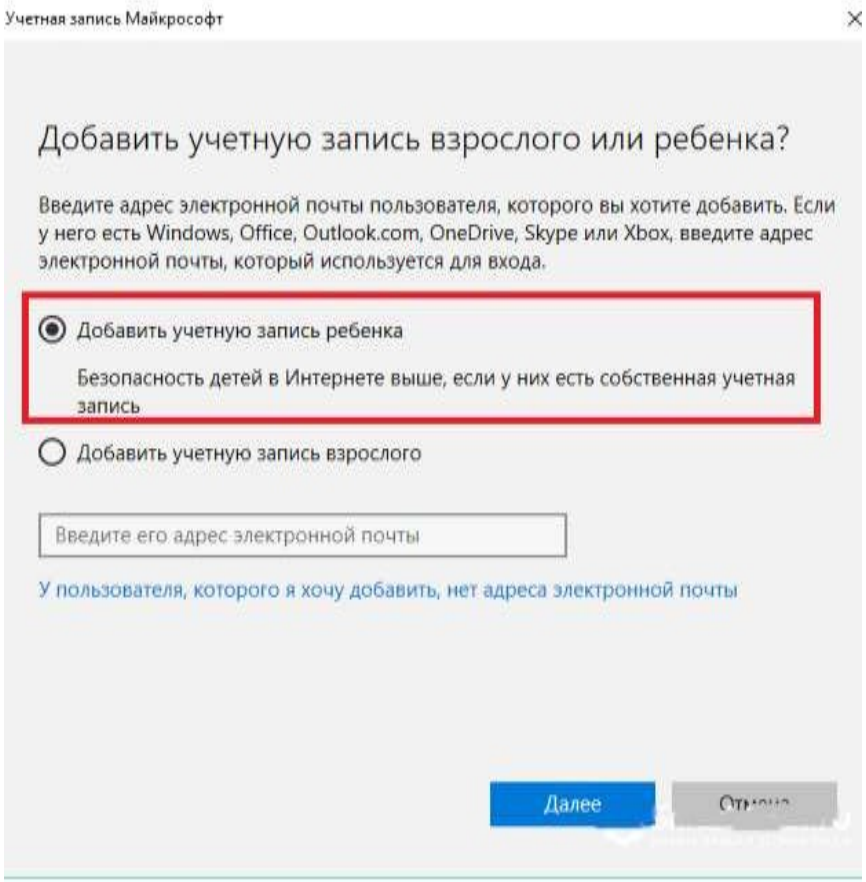
- откройте меню «Пуск» и кликните на фотографию Вашего профиля;
- затем в выпадающем списке нажмите на поле «Изменить параметры учётной записи»;



- в появившемся окне перейдите в раздел «Семья и другие люди»;
- кликните на кнопку «Добавить члена семьи»;



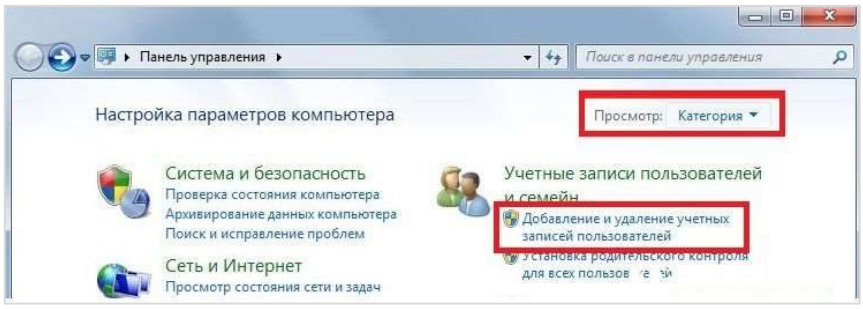
- затем зайдите в режим добавления учётной записи ребёнка и следуйте инструкциям мастера установки. После завершения процедуры, на компьютере появятся две учётных записи: Ваша и ребёнка;



- чтобы задать пароль для записи пользователя, кликните на его фото и в списке выберите «Пароль доступа». Если запись администратора привязана к службе Microsoft Online, то пароль доступа — это пароль привязанной к аккаунтуэлектронной почты.

Инструкция для пользователей Windows 7

- Зайдите в панель управления и выберите режим просмотра «Категория».
- Кликните на поле «Учётные записи», а затем на кнопку добавления нового профиля.
- Задайте пароль для своей учётной записи и для страницы ребёнка. В Windows 7 это делается с помощью простого нажатия на фотографию пользователя и ввода кодового слова в настройках. Привязка к службе Microsoft Onlline отсутствует.



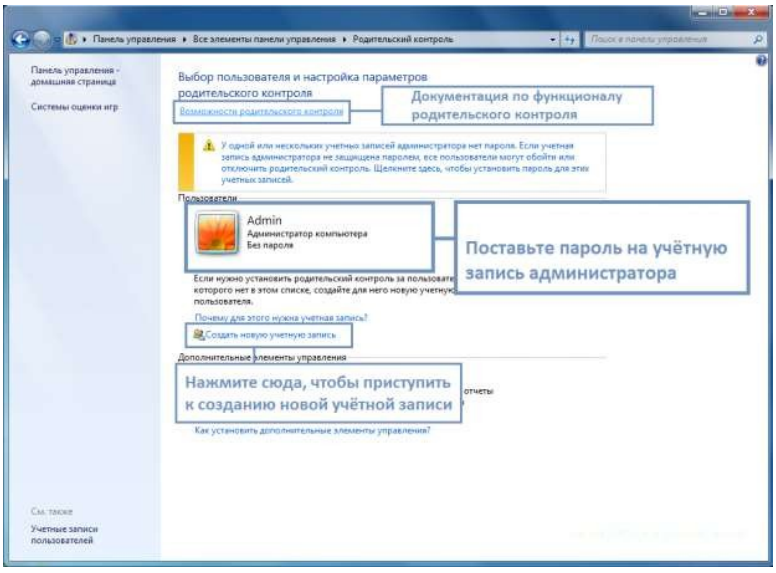
Настройка функции в Windows 7

Родительский контроль в Windows 7 поддерживает следующие опции:

- ограничение времени включения компьютера;
- настройка списка разрешённых программ;
- ограничение на время работы игр.

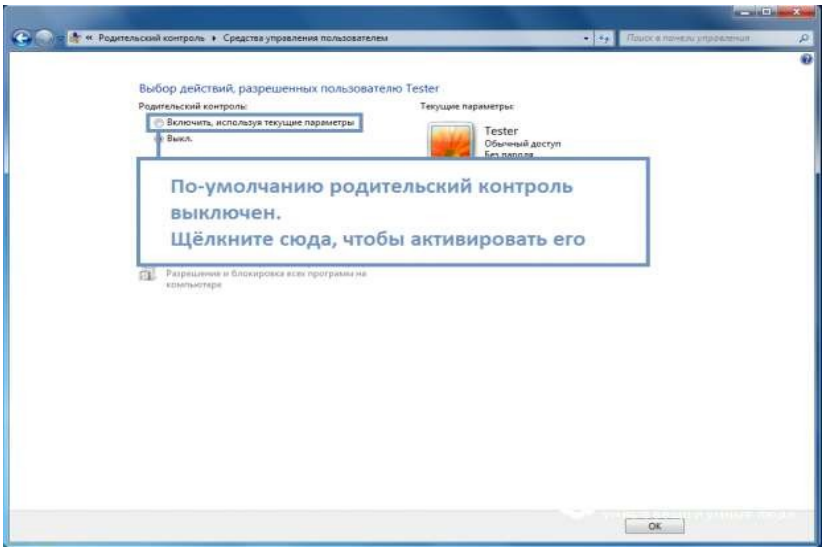
Для включения контроля убедитесь, что на компьютере создана детская учётная запись. Затем откройте Панель управления и выберите поле «Учётныезаписи пользователей». Выберите профиль администратора.

Проверьте, установлен ли пароль. Для ознакомления с документацией о родительском контроле от разработчика ОС кликните на указанном рисунке ниже поле.



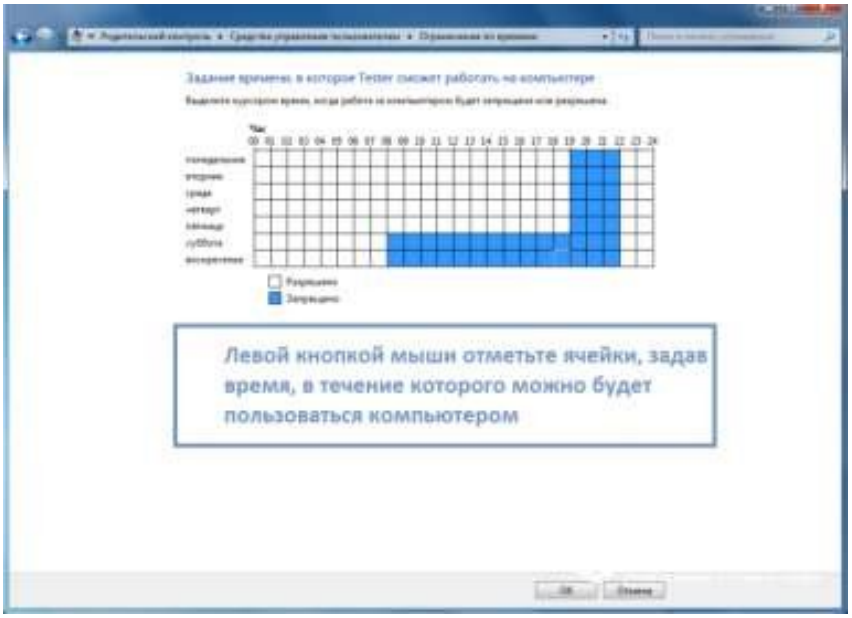
Все дополнительные профили будут отображены под записью администратора. Кликните на запись ребёнка, в данном случае это иконка Tester. Далее откроется окно с дополнительными сведениями.

В разделе «Выбор разрешённых действий» активируйте работу родительского контроля.



Теперь можно приступать к ограничению работы второго пользователя. В указанном выше окне отображается набор параметров, которые вы можете изменить. Первый из них — настройка времени работы компьютера. Вам нужно только отметить временной диапазон, в период которого будет разрешено использовать ПК. Выполнить настройку можно для каждого дня недели. Кликните мышкой на белый квадрат, чтобы изменить его цвет. Синий цвет означает, что в это время ребёнок сможет работать за компьютером.

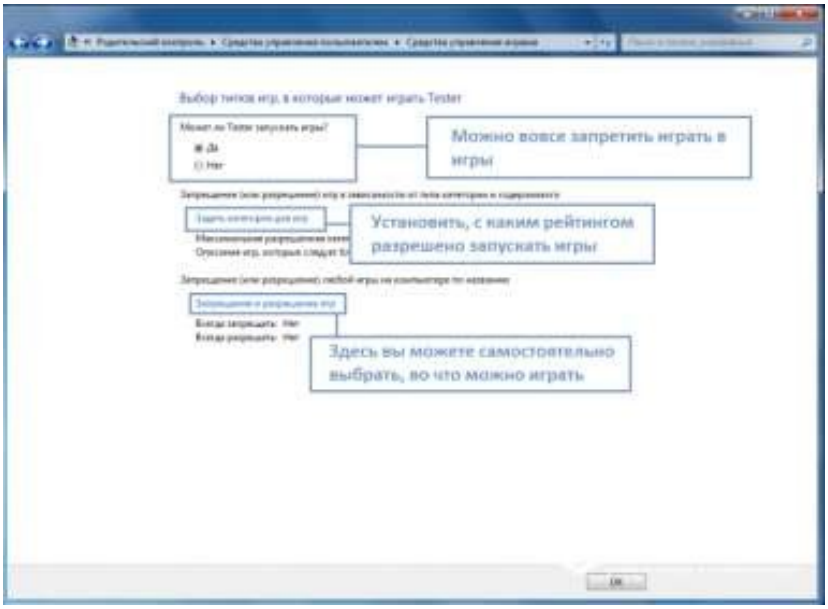
Чтобы выбрать одновременно несколько ячеек, удерживайте нажатой левую клавишу мышки и выделяйте нужный промежуток времени.



Следующая функция — настройка работы с установленными играми. Здесь Вы можете запретить или разрешить включать игровые приложения, задать разрешённый возрастной рейтинг или вручную выбрать среди установленных на компьютере игр те, которые ребёнок сможет включить.

Заметьте! Если приложение не указывает свой рейтинг, оно тоже будет заблокировано для второй учётной записи.

Для сохранения настроек нажмите на клавишу «ОК» внизу экрана.



Если на компьютере установлены пиратские игры, рекомендуется настраивать доступ к приложениям вручную, так как в окне выбора разрешённого возрастного ценза эти программы не будут отображаться. Чтобы проверить правильность всех настроек обязательно самостоятельно протестируйте работу всех функций. Попытайтесь включить запрещённую программу или игру. В случае необходимости ещё раз проверьте правильность выставленных параметров.

Настройка родительского контроля в Windows 10

Родительский контроль в Windows 10 поддерживает ещё больше функций и возможностей. Нововведение, которое запустил разработчик — это опция контроля покупок в магазине Microsoft. Родители могут выставлять максимальную сумму покупки и возрастной ценз. Таким образом, ребёнок не может купить игру, которая предназначена для определённого возраста.

Всего в магазине приложений есть 5 категорий ПО с разделением по возрасту:

- 6+ лет;
- 12+ лет;
- 16+ лет;
- 18+ лет.

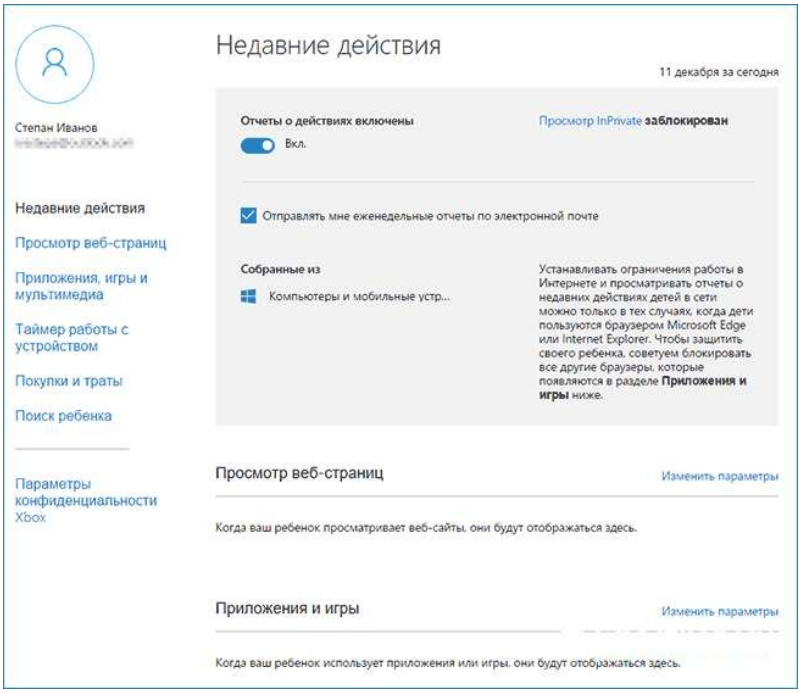
Создайте учётную запись ребёнка, как это было описано выше, и задайте пароль для странички администратора системы. Теперь можно начинать настройку родительского контроля.

Сразу после создания новой учётной записи авторизуйтесь под её именем и проверьте, действительно ли она создалась в категории «Ребёнок». Также вы сможете настроить оформление рабочего стола и добавить на него все необходимы для работы ребёнка ярлыки. Это позволит детям быстрее приступить к работе и не искать нужные программы по всем папкам системы.

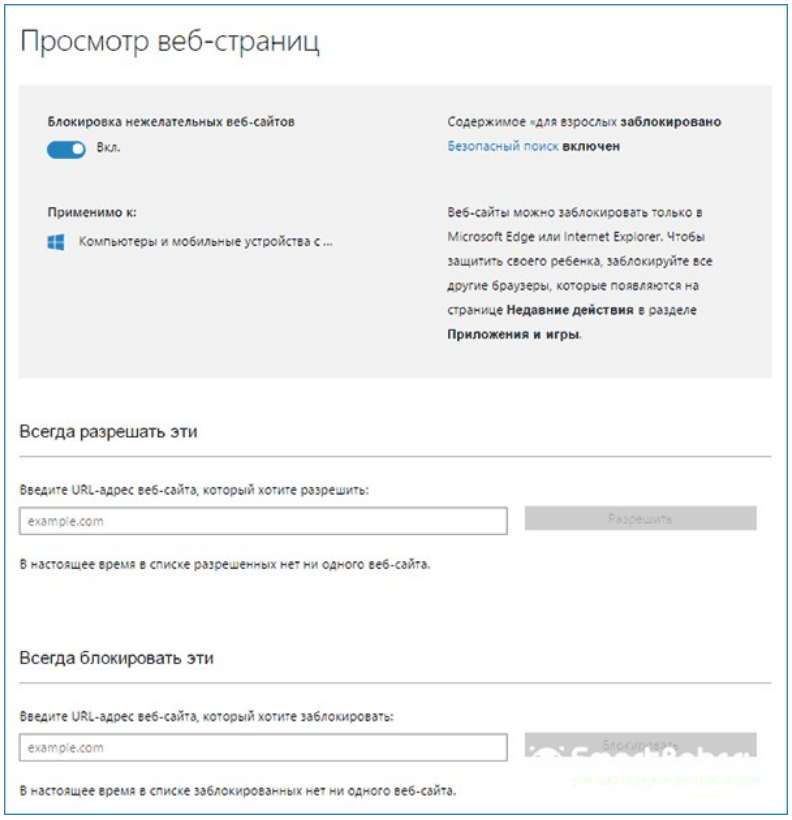
Для управления настройками записи ребёнка зайдите на страничку https://account.microsoft.com/account/ManageMyAccount?destrt=FamilyLandingPage
и авторизуйтесь с данными записи владельца (администратора) компьютера. Второй аккаунт уже привязан к Вашему. Для начала настройки достаточно кликнуть на значке дополнительного профиля.

Доступные настройки

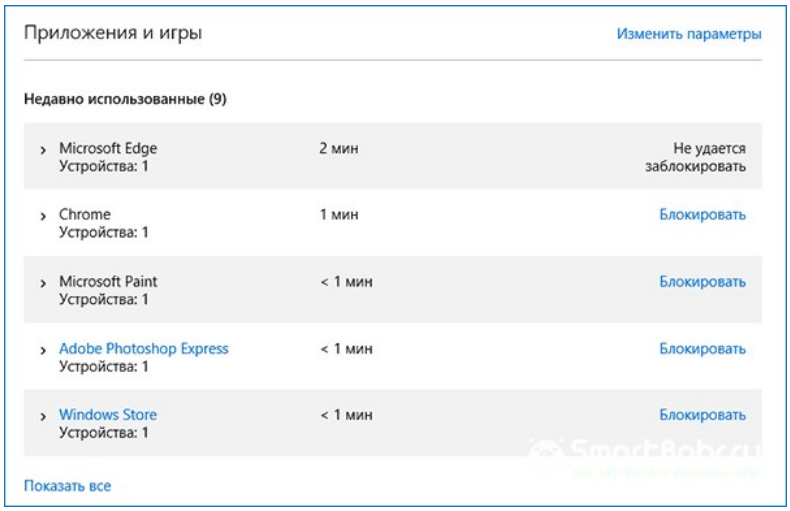
Отчёты о действиях. Активируйте эту опцию, чтобы получать детальные отчёты о том, сколько времени провёл ребёнок за компьютером и какие программы были запущены во время сеанса. Также в отчёт включается история браузера и поисковых запросов (даже если ребёнок их удалил).



Для регулирования разрешённых веб страниц кликните на «Изменить параметры» в указанном на рисунке ниже окне. Вы можете вручную ввести адреса разрешённых ресурсов и в то же время настроить автоматическую блокировку нежелательных страниц.



В окне настроек приложений и игр вы увидите, сколько времени ребёнок использовал каждую программу. Кликните на «Блокировать», чтобы запретить ПО.



Таймер работы. Для ограничения времени пребывания за компьютером выставьте разрешённый временной диапазон на каждый день недели.

Также в окне настроек родительского контроля есть опция **контроля местоположения ребёнка**. Если он использует переносной гаджет с Windows 10, родители всегда будут оставаться в курсе того, где сейчас ребёнок. Это возможно с помощью служб геолокации, работающих в режиме реального времени.

РЕКОМЕНДАЦИИ ПО ПРОФИЛАКТИКЕ КИБЕРБУЛЛИНГА СРЕДИ ОБУЧАЮЩИХСЯ

Рекомендации для педагогов

Памятка
«10 основных способов для педагогов, как остановить кибербуллинг»

- ***Относитесь к кибербуллингу серьёзно.***

Первый шаг для педагогов — признать, что проблема кибербуллинга серьёзна. Пренебрежение педагогов, несмотря на рост числа случаев киберзапугивания, является небрежным поведением, которое поощряет кибербуллинг. Только когда Вы, как педагог, серьёзно относитесь к кибербуллингу, Вы можете придумать способы противостоять ему.

- ***Следите за любыми индикаторами кибербуллинга.***

Для педагогов, которые хотят предотвратить кибербуллинг, наблюдение является ключевым фактором. Как педагог, Вы должны наблюдать за поведением своего учащегося. Если учащийся внезапно начинает вести себя неустойчиво или необычно, возможно, он стал жертвой кибербуллинга. В этом случае поговорите с ними и узнайте, что происходит.

- ***Мотивируйте других сообщать об инциденте кибербуллинга.***

Как педагог, Вы не всегда можете быть свидетелем кибербуллинга. Однако есть кибер-прохожие, такие как одноклассники и друзья, которые могут видеть, как их одноклассники подвергаются кибербуллингу. Вы должны поощрять этих свидетелей сообщать о любом инциденте, который они увидят. Оперативное сообщение означает, что принимаются незамедлительные меры, которые помогают уменьшить последствия кибербуллинга для жертвы.

- ***Разработайте эффективный и действенный план реагирования на сообщения о кибербуллинге***.

У Вас должен быть план действий по обработке сообщений о кибербуллинге. Кто-то может сообщить вам в шутку, и некоторые сообщения могут быть серьёзными (например, киберпреследование), а некоторые могут быть менее серьёзными (например, исключение). Вам нужен надлежащий план реагирования на все эти случаи.

Как педагог, Вы должны убедиться, если учащийся сообщает об инциденте — это будет рассмотрено. Вы не можете создавать впечатление, будто никаких действий не предпринимается даже после того, как поступило сообщение о кибербуллинге.

- ***Действовать как мост между родителями, учащимися и администрацией школы.***

Как педагог, Вы можете преодолеть разрыв в общении между родителями, учениками и руководством школы. Вам необходимо регулярно консультироваться с родителями о присутствии их ребёнка в интернете и планировать сокращение любых негативных действий в интернете. Кроме того, Вы можете связаться с руководством школы если обнаружите, что ваш учащийся подвергается кибербуллингу.

- ***Поощряйте хорошее цифровое поведение среди учащихся.***

Поощрение учащихся к тому, чтобы они стали хорошими цифровыми гражданами, является частью обязанностей педагога. Вы должны научить своих учащихся не участвовать в онлайн-издевательствах или других неуместных действиях в интернете. Вы должны чётко объяснить последствия кибербуллинга и его вред.

Более того, научить своих ребят не делиться своей конфиденциальной личной информацией в интернете и серьёзно относиться к сетевой безопасности и конфиденциальности. Таким образом, поощряйте обучающихся вести себя хорошо в интернете. Вы можете хвалить и награждать за хорошее поведение в интернете, а также наказывать тех, кто занимается травлей в интернете.

- ***Спокойно выслушайте проблемы жертвы и вдумчиво ответьте.***

Вы должны терпеливо выслушивать проблемы ребёнка, подвергшегося кибербуллингу, и предлагать конструктивные решения для решения этих проблем. Поймите, что нет двух одинаковых случаев кибербуллинга. Таким образом, не существует универсального подхода при поиске ответа проблемному учащемуся, над которым часто издеваются.

Спокойно выслушайте учащегося и дайте ему понять, что он может поделиться с Вами своим опытом травли. Поддерживайте точку зрения ребёнка и давайте обдуманные ответы после тщательного обдумывания его проблем. Вы можете самостоятельно провести небольшое исследование в интернете, поговорить с другими педагогами или родителями и убедиться, что Вы нашли хорошее решение их проблем, а не вводите их в заблуждение.

- ***Попробуйте добавить принципы борьбы с кибербуллингом в учебную программу.***

К кибербуллингу нужно относиться серьёзно. Вы должны разъяснить этот момент родителям и учащимся. Создавайте проектные работы и задания, связанные с кибербуллингом, в своих программах обучения. Предложите ребятам провести небольшое исследование о кибербуллинге.

Вы также можете показать статистику о том, как кибербуллинг увеличился за эти годы и как защитить себя от него. Попробуйте добавить занятия по кибербуллингу в учебную программу.

Как только ребёнок подвергается кибербуллингу, ему становится очень трудно воссоединиться с другими детьми. Социальные тревоги, ненависть к себе, депрессия и т. д. вызывают антиобщественное поведение среди жертв кибербуллинга. Таким образом, Ваша работа как педагога будет заключаться в том, чтобы помочь этим детям реинтегрироваться в коллектив и заставить их чувствовать себя в безопасности во время занятий.

Помощь жертвам в возвращении в коллектив делает их более уверенными в себе и дружелюбными. Кроме того, нынешняя жертва может, в свою очередь, помогать другим жертвам в будущем. Это поощряет позитивное поведение учащихся и сводит к минимуму эффект кибербуллинга.

- ***Предложите учащимся стать лидерами, чтобы остановить кибербуллинг.***

Есть поговорка: вместо того, чтобы давать человеку рыбу, научите его ловить рыбу. Вы — педагог и не можете всегда присутствовать, когда учащийся становится жертвой онлайн. Так что отличным вариантом было бы сделать самих ребят лидерами в пресечении кибербуллинга.

Это лишь некоторые способы, с помощью которых педагог может остановить кибербуллинг. Как педагогу, поддерживать учащихся в подростковом возрасте может быть сложно, но знание того, когда нужно вмешаться и помочь, может спасти жизнь.

Рекомендации для родителей

Памятка
«Признаки, вовлеченности в кибербуллинг»

Кибербуллинг затрагивает по крайней мере одного из каждых пяти учащихся среднего и старшего возраста. Многие из тех, кто переживает это, никому не рассказывают.

Ребёнок может быть объектом кибербуллинга, если он или она:

- неожиданно прекращает пользоваться своим(и) устройством(ами);
- впадает в депрессию или испытывает разочарование после выхода в интернет (включая игры);
- слишком много спит или недосыпает;
- становится ненормально замкнутым в себе от друзей и членов семьи;
- показывает увеличение или уменьшение количества еды;

- кажется, регулярно подавленным;
- делает мимолетные заявления о самоубийстве или бессмысленности жизни;
- теряет интерес к тому, что для них важнее всего;
- избегает обсуждения того, что они делают в интернете;
- часто звонит или пишет смс с просьбой вернуться домой больной;
- желает проводить гораздо больше времени с родителями, а не со сверстниками;
- становится необычно скрытным, особенно когда дело касается онлайн-активностей.

Ребёнок может запугивать других, если он или она:

- быстро переключает экраны или прячет своё устройство, когда Вы рядом;
- использует своё устройство в любое время ночи;
- необычайно расстраивается, если не может использовать своё устройство;
- чрезмерно смеётся, используя своё устройство и не хочет показывать Вам, что смешного;
- избегает обсуждений того, что он делает в интернете;
- всё чаще замыкается в себе или изолируется от семьи;
- использует несколько учётных записей в интернете или одну учётную запись, но не собственное;
- имеет дело с повышенными поведенческими проблемами или дисциплинарными мерами;
- кажется чрезмерно озабоченным популярностью или постоянным присутствием в опредеёенном социальном кругу или статусе;
- демонстрирует растущую бесчувственность или чёрствость по отношению к другим подросткам;
- начинает общаться с «неправильной» тусовкой;
- демонстрирует склонность к насилию;
- выглядит чрезмерно тщеславным в отношении своих технологических навыков и способностей.

Рекомендации для подростков

Памятка
«Как противостоять кибербуллингу: десять лучших советов для подростков»

Эти десять советов дадут вам конкретные идеи о том, что вы можете сделать, когда вы стали свидетелем кибербуллинга.

1. **Отчёт в школу.** Если человек, подвергшийся кибербуллингу, является кем-то из вашей школы, сообщите об этом в свою школу. У многих есть системы анонимных сообщений, которые позволяют вам сообщить им о том, что вы видите, не раскрывая свою личность.
2. **Собирайте доказательства**. Сделайте снимок экрана, сохраните изображение или сообщение или запишите на экран то, что видите. Взрослому будет легче помочь, если он увидит и у него будет доказательство именно того, что было сказано.
3. **Отчёт на сайт/приложение/игру.** Все авторитетные онлайн-среды запрещают кибербуллинг и предоставляют простые инструменты для сообщения о нарушениях. Не стесняйтесь сообщать — эти сайты/приложения будут защищать вашу личность, а не «выбивать» вас.
4. **Поговорите с доверенным взрослым.** Развивайте отношения со взрослыми, которым вы можете доверять и рассчитывать на помощь, когда вы (или ваш друг) столкнётесь с чем-то негативным в Интернете. Это может быть родитель, учитель, консультант, тренер или друг семьи.
5. **Проявляйте внимательность.** Покажите человеку, подвергшемуся кибербуллингу, что он не одинок. Отправьте ему ободряющий текст или снимок. Отведите его в сторону в школе и дайте понять, что вы его поддерживаете.
6. **Работайте вместе.** Соберите других своих друзей и организуйте полноценный пресс позитива. Оставляйте добрые комментарии на его стене или под фотографиями, которые он разместил. Поощряйте других сообщать о вреде. Сила в количестве.
7. **Скажите ему остановиться**. Если вы знаете человека, который занимается кибербуллингом, попросите его прекратить это. Объясните, что так нехорошо поступать по отношению к другим. Но если вы промолчите — вы, по сути, скажете, что это нормально.
8. **Не поощряйте это.** Если вы видите, что происходит кибербуллинг, ни в коем случае не поддерживайте его. Не пересылайте, не добавляйте эмодзи в комментарии, не сплетничайте об этом с друзьями и не стойте в стороне.
9. **Оставайтесь в безопасности.** Не подвергайте себя опасности. Когда ваши эмоции зашкаливают, воздержитесь от публикации чего-то, что может обострить ситуацию. Не зависайте в интернете, где большинство людей жестоки. Никогда не угрожайте другим физически.
10. **Не сдавайтесь.** Подумайте творчески о том, что можно сделать, чтобы остановить кибербуллинг. Проведите мозговой штурм с другими и используйте таланты каждого, чтобы сделать что-то эпическое.

ЗАКЛЮЧЕНИЕ

Кибербуллинг превратился в эпидемию, ежегодно затрагивающую миллионы детей, подростков и взрослых. Это может быть особенно разрушительным для самооценки молодого человека, социальной жизни и успехов в учёбе.

Понимание кибербуллинга является ключом к выявлению и прекращению этого вредоносного поведения. Однако педагогам важно донести до учащихся важность прекращения киберзапугивания навсегда. По этим причинам крайне важно, чтобы педагоги были вовлечены, но положить конец такому поведению — непростая задача.

Данные методические материалы направлены на то, чтобы начать работу по выявлению инцидентов кибербуллинга, показать педагогам различные возможности предотвращения и вмешательства в ежедневную агрессию, которая происходит в образовательных организациях и изучить способы безопасного поведения в сети Интернет.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Андреева, А.О. Манипулирование в сети Интернет / А.О. Андреева // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи. – 2015. – С. 21–28.
2. Березина, О.С. Социальная профилактика кибербуллинга среди подростков / О.С. Березина // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи. – 2015. – С. 63–67.
3. Парфентьев, У. Кибер-агрессоры / У. Парфентьев // Дети в информационном обществе [Эл. рес.]. – 2009. – Вып. 2. – С. 66–67. Режим доступа: http://detionline.eom/assets/files/journal/2/threat2_2.pdf
4. Черкасенко, О.С. Феномен кибербуллинга в подростковом возрасте / О.С. Черкасенко // Личность, семья и общество: вопросы педагогики и психологии. – 2015. − № 6. – С. 52-54.

ПОЛЕЗНЫЕ ССЫЛКИ

- Рекомендации Управления «К» МВД России https://мвд.рф
- Дети России Онлайн http://detionline.com/
- Проект «Цифровая грамотность» http://цифроваяграмотность.рф
- Проект Роскомнадзора http://персональныеданные.дети
- Защита детей от Лаборатории Касперского https://kids.kaspersky.ru/
- Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт http://i-deti.org/
- Онлайн-площадка «Единый урок» https://www.единыйурок.рф
- Буклет для подростков https://drive.google.com/file/d/1qdNwczXeYybIrTfAjbt5jaY6Bk5ohm6I/view?usp=sharing
- Буклет для родителей https://drive.google.com/file/d/1m8tdx30oJRUFd6js9rQrqZNUwyPa_OsL/view?usp=sharing
- Буклет для педагогов https://drive.google.com/file/d/1MVIR77K2EqxXWZVVyAsBtLehQbmwgq9y/view?usp=sharing
- Набор памяток https://drive.google.com/drive/folders/1xXHR83zO_Gwy6FF9w9ZbcA8_kDThyxB7?usp=sharing
- https://cyberleninka.ru/article/v/kiberbulling-kak-novaya-forma-ugrozypsihologicheskomu-zdorovyu-lichnosti-podrostka
- http://files.runet-id.com/2017/riw/presentations/2nov.riw17-blue.11-00--soldatova.pdf
- http://mediasmarts.ca/
- http://detionline.com/helpline/rules/parents
- Памятка «Блокировка нежелательных писем» http://kcdod.khb.ru/files/documents/17038_pamyatka_blokirovka_negelatelnih_pisem.pdf
- Памятка «Двухэтапная аутентификация аккаунтов в социальных сетях» http://kcdod.khb.ru/files/documents/17039_pamyatka_dvuhetapnaya_autentifikatsiya.pdf
- Памятка «Как избавиться от следов своего существования в интернете» http://kcdod.khb.ru/files/documents/17040_pamyatka_kak_izbavitsya_ot_sledov.pdf
- Памятка «Лечение» компьютера после заражения вирусами» http://kcdod.khb.ru/files/documents/17041_pamyatka_lechenie_kompyutera_posle_zarageniya.pdf
- Памятка «Облачные сервисы безопасного хранения» http://kcdod.khb.ru/files/documents/17042_pamyatka_oblachnie_servisi_bezopasnogo_hraneniya.pdf
- Памятка «Создание надежных паролей» http://kcdod.khb.ru/files/documents/17044_pamyatka_sozdanie_nadegnih_paroley.pdf

Кибергигиена, как способ защиты от буллинга в сети Интернет. Методические материалы

Краевое государственное автономное образовательное учреждение дополнительного образования «Центр развития творчества детей (Региональный модельный центр дополнительного образования детей Хабаровского края)»

680000, г. Хабаровск, ул. Комсомольская, 87
тел. / факс: (4212) 30-57-13
Телеграм: @dopobrazovanie27
ВКонтакте: @dop.obrazovanie27
e-mail: rmc@edu.27.ru
http://www.kcdod.khb.ru

Подписано в печать: 27.03.2023
Тираж: 30 экз.

Методические материалы размещены на сайте КГАОУ ДО РМЦ

физкультурно-спортивная

туристско-краеведческая

художественная

естественнонаучная

техническая

социально-гуманитарная