



ГБУ «Институт оценки качества
образования Республики Тыва»

Күрүнениң бюджеттен
хандырылгалыг албан чери
«Тыва Республиканың
өөредилгезиниң шынарын
үнелээр институт»

667011, г. Кызыл, ул. Ленина, д.39
тел., факс:8(39422)5-62-27, 5-61-26
e-mail: gu_ioko@mail.ru

Руководителям муниципальных
органов управлений образованием

Руководителям образовательных
организаций

от 22.09.2021 № 571

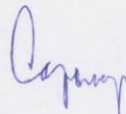
Уважаемые руководители!

Во исполнения письма №12/7327 от 30.07.2021 г о направлении решения Правительственной комиссии по профилактике правонарушений от Министерства внутренних дел, в целях расширения практики информирования родителей (законных представителей) учащихся методам блокирования нежелательного контента в сети Интернет по распространению информационных буклетов «Безопасность детей в сети интернет (Советы родителям)» разработанных Министерством образования и науки РТ в соответствии с методическими рекомендациями Министерства просвещения РФ (письмо № 03-393 от 29.03.2019 года), направляем вам информационные буклеты для размещения на официальных сайтах, а также для распространения родителям в бумажном виде и раздать во время родительских собраний, а также выложить на социальных сетях (вайбер, вконтакте, инстаграм). Просим проинформировать родителей (законных представителей) к применению защитных функций интернет-браузеров, в том числе специальных программных фильтров («родительский контроль»), позволяющих блокировать «всплывающие окна», а также интернет-сайтов с негативным контентом. Дополнительно сообщаем вам, что в октябре 2021-2022 учебного года, в целях

проверки знаний родителей по безопасному интернету, будет проводиться дистанционное онлайн-тестирование.

Приложение на 6 л., в 1 экз.

С уважением,
и.о. директора



Ш.М.Монгалбии

Исп: Кыргыз Н.В.. 8(394-22) 5-62-27

Обмен информацией между пользователями:

В данную категорию входят Интернет-ресурсы и технические программные решения, направленные на предоставление возможности двум и более пользователям в сети "Интернет" обмениваться информацией в любой форме, например, социальные сети, мессенджеры, сервисы электронной почты и другие, которым рекомендуется реализовать следующие меры:

Родителям следует установить родительский контроль, предоставляющий возможность родителям отслеживать список друзей ребенка, его местонахождение и его активности;

Ограничить доступ детей в возрасте до 12 лет до клубов и сообществ, содержащих нежелательный контент для детей, по возможности установить механизмы предупреждения о нежелательном контенте для остальных возрастных групп до 18 лет в соответствии с возрастной классификацией информации, предусмотренной Федеральным законом от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

Поисковые системы:

В данную группу входят Интернет-ресурсы и технические программные решения, направленные на организацию поиска по запросу пользователя информации в сети "Интернет" и (или) информации в рамках Интернет-ресурса или технического программного решения, на котором организован поиск информации, например, поисковые системы, системы поиска для сайтов и другие, которым рекомендуется реализовать следующие меры:

1. Найти пути предупреждения (антивирусы, фильтры и т.д.) о нежелательном для детей контенте, выдающемся в результатах поиска;

2. Найти пути решения безопасного поиска, предназначенного для родителей (законных представителей) и позволяющего при включении ограничить доступ несовершеннолетних пользователей к нежелательному контенту;

3. Исключить из результатов поиска персональные данные детей в форме ссылок на аккаунты в социальных сетях;

4. Использовать средства контентной фильтрации для выявления запрещенной для детей информации.

Информационные сайты:

В данную категорию входят Интернет-ресурсы и технические программные решения, представляющие пользователям сети "Интернет" в одностороннем порядке информацию общественного, политического, либо другого характера, которым рекомендуется реализовать следующие меры:

До просмотра мультимедиа (видео, фотографии, комментарии другого контента) в котором может содержаться запрещенная для детей информация, разместить текстовый или графический знак информационной продукции для предупреждения о недопустимости просмотра данного контента детьми;

При наличии функций, позволяющих пользователям обсуждать и комментировать контент, рядом с каждым сообщением должна быть предусмотрена функция жалобы в администрацию ресурса о нарушении законодательства в сфере информационной защиты детей.

Интернет сервисы:

В данную группу входят Интернет-ресурсы и технические программные решения, направленные на предоставление своим пользователям различных товаров и (или) услуг, например, интернет-магазины, приложении, игры и другие, которым рекомендуется реализовать следующие меры:

1. При продаже товаров и услуг, которые включают информационный контент, запрещенный для детей и отдельных возрастных категорий в соответствии с Федеральным законом от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" администрация интернет-сервиса обязана запросить дополнительную информацию о покупателе (ФИО, возраст; телефон) и, в случае не достижения пользователем возраста продажи, либо непредоставления данной информации, отказать в продаже товара или оказания услуг;

2. При предоставлении товаров и услуг, ориентированных на взрослых, подробная информация о них должна быть недоступна. Краткая информация должна содержать возрастную маркировку, текстовое предупреждение о недопустимости просмотра данного товара или услуги до момента согласия пользователя об ответственности за последствия просмотра подробной информации;

3. Разработать методы родительского контроля, позволяющие родителям ознакомиться с историей оказанных их ребенку услуг или приобретенных им товаров, настроить доступные ребенку категории товаров и услуг и ограничить возможность ребенка по получению ими возмездных или безвозмездных товаров или услуг.



Министерство
образования и науки РФ

Безопасность детей в сети Интернет (советы родителям)



ГБУ «Институт оценки
качества образования РФ»

СОВЕТЫ ДЛЯ РОДИТЕЛЕЙ «ПРАВИЛА БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ

Если ваш ребёнок в возрасте от 7 до 9 лет

1. Компьютер должен находиться в общей комнате, чтобы родители в любой момент могли проконтролировать ребенка.
2. Просматривая вместе сайты, постепенно приучайте ребенка делиться с вами увиденным.
3. Если ребенок решит воспользоваться электронной почтой, научите его пользоваться семейным электронным ящиком.
4. Вместе с ребенком найдите сайты, которые ему интересны в этом возрасте и сохраните их в разделе браузера «Избранное». Для просмотра достаточно будет щелкнуть мышкой на нужном названии.
5. Для уверенности в безопасности, установите фильтры.
6. Учите ребенка тот факт, что ребенок может просматривать Интернету кого-то из друзей без разрешения родителей.
7. Объясните ребёнку, с чем он может столкнуться в Интернете, и подскажите, как найти выход из подобной ситуации.
8. Согласуйте с ребенком время пользования интернетом.

Если ваш ребёнок в возрасте от 10 до 12 лет

1. Вместе с детьми обсуждайте надежность сайтов, заинтересуйте их в поисках полезной и качественной информации.
2. Решайте с ребенком вопросы, касающиеся семьи. Например, выбор места поездки на отдых или приобретение новой вещи через Интернет. Пусть ребенок самостоятельно попытается найти несколько вариантов.
3. Поговорите с ним о разрешенных и запрещенных действиях в Интернете.
4. Объясните, какую информацию, и в каких случаях можно разглашать, о способах взаимодействия с пользователям и о связанных с этим рисках, и как можно защитить свою личность.
5. Предупредите детей, что несовершеннолетние не могут воспользоваться услугами интернет-магазинов в соответствии с Федеральным законом от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

С кем общается ваш ребенок?



Будьте бдительны online!

Если ваш ребёнок в возрасте от 13 до 15 лет



1. Родители должны принимать участия в дискуссиях и чаще общаются с ребенком, чем ребенок общается в Интернете.
2. Ребенок должен понимать, что в любой момент он может поговорить с родителями, если столкнется в Интернете с чем-то неприятным.
3. Если он захочет поместить свою фотографию и личную информацию на веб-сайте, помогите ему. Подскажите ему, как создать персональный пароль, не предоставляя никакой информации о себе (почтовый адрес, телефон, школу, спортивную секцию и т. д.). Никому не сообщайте пароль и регулярно его меняйте.
4. Заблокируйте параметры электронной почты, чтобы ребенок получал почту только от указанных адресатов.
5. Договоритесь с ребенком о выборе веб-сайтов, которые он будет посещать и о времени пользования.
6. С помощью фильтров блокируйте сайты, содержащие опасную информацию, ограничьте список собеседников.



Интернет один из лучших источников знания, если его правильно использовать!

Интернет – вещь классная,
Но чересчур опасная.
Много всякого в нём хлама:
Вирусов коварных, спама ...
Чтоб ничего не зацепить,
Надо осторожным быть.
Вот пришёл домой из школы
И, отбросив все дела,
Открываешь блоги, сайты,
Ищешь нужные слова,
Сочинения, ответы ...

Стоп! Всё подряд не открывай,
Куда не надо, не «влезай»!

Ничего тебе не нужно
Ни прогулки, ни обед,
Ни родные папа с мамой
Только был бы Интернет.

Интернет совсем не прост,
До добра не доведёт!

Интернет – вещь классная!
И быть может безопасная.
Если в меру там «бродить»,

То здоровью
не вредит!



ПРОВЕРЬ СЕБЯ!

Пройди тест на знание об интернете и правил поведения в интернете

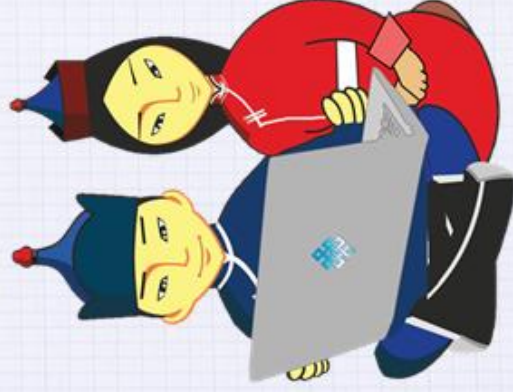
1. В какой стране впервые появился Интернет?
А. Япония
Б. США
В. Франция
2. Почему нельзя открывать неизвестные файлы, пришедшие на электронную почту?
А. Они могут быть большие по размеру
Б. Отправлены не вам
В. В них могут быть вирусы
3. Что такое спам в Интернете?
А. Непрошенное письмо или сообщение
Б. Ложная статья на сайте
В. Тип вируса
4. Где нельзя хранить свои файлы в Интернете?
А. В облачных сервисах
Б. В социальной сети
В. На torrent-ресурсах
5. Что такое смайлик?
А. Название социальной сети
Б. Псевдоним пользователя
В. Картинка в виде рожицы, выражающая эмоции

1Б, 2В, 3А, 4В, 5В



Министерство
образования и науки РТ

БЕЗОПАСНЫЙ ИНТЕРНЕТ И ТЕЛЕФОН ДЕТЯМ!



ПОЛЕЗНЫЕ СОВЕТЫ ДЛЯ
ШКОЛЬНИКОВ



ГБУ «ИОКО РТ»

ВИРТУАЛЬНЫЕ МОШЕННИКИ И ДРУГИЕ ПРЕСТУПНИКИ

Ты знаешь, что вне дома и школы есть вероятность столкнуться с людьми, которые могут причинить тебе вред или ограбить.

@ В Интернете также есть злоумышленники – ты должен помнить об этом и вести себя так же осторожно, как и на улице или в незнакомых местах.

@ Не сообщай свой адрес или телефон незнакомым людям и никогда не выкладывай в Интернете.

@ Никогда не высылай свои фотографии без родительского разрешения. Помни, что преступники могут использовать эту информацию против тебя или твоих родных.

@ Если ты хочешь участвовать в каком-нибудь конкурсе, где нужно указывать свои данные, посоветуйся с родителями.

@ Никогда не соглашайся прийти в гости к человеку, с которым ты познакомился в Интернете.

@ Если назначается встреча, она должна проходить в людном месте и желательно с присутствием родителей. Помни, что под маской твоего ровесника может скрываться взрослый человек с преступными намерениями



НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Обман по телефону: требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.

SMS-просьба о помощи: требование перевести определенную сумму на указанный номер, используется обращение «мама», «друг», «сын» и т. п.

Телефонный номер «грабитель»: платный номер, за один звонок на который со счёта списывается денежная сумма.

Выигрыш в лотерею: которую якобы проводит радиостанция или оператор связи. Вас просят приобрести карты экспресс-оплаты и сообщить коды либо перевести крупную сумму на свой счет, а потом ввести специальный код.

Простой код от оператора связи: предложение услуги или другой выгоды—достаточно ввести код, который на самом деле спишет средства с Вашего счёта.

Штрафные санкции и угроза отключения номера: якобы за нарушение договора с оператором Вашей мобильной связи.

Ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку.



ГРУБИЯНЫ И ХУЛИГАНЫ В ИНТЕРНЕТЕ: КАК СЕБЯ ВЕСТИ?

Кроме преступников в Интернете есть просто злые и невоспитанные люди. Ради собственного развлечения они могут обидеть тебя, прислать неприятную картинку или устроить травлю. Ты можешь

столкнуться с такими людьми на самых разных сайтах, форумах и чатах.

ПОМНИ: ты не виноват, если получил оскорбительное сообщение. Не нужно реагировать на грубых людей – просто прекратить общение.

Если тебе угрожают по Интернету, не стесняйся сообщить об этом родителям. Помни, что цель угрозы испугать тебя и обидеть. Но подобные люди боятся ответственности.

Коллективное преследование – это крайнее проявление жестокости. Жертву забрасывают оскорблениями и угрозами, его фотография искажают и все данные публикуют. Никогда не участвуй в травле и не общайся с людьми, которые обижают других.

Всегда советуйся с родителями во всех указанных случаях.



Какие есть способы контролировать телефон и компьютер ребенка

1. Установить приложение контролирующее устройство (готовый телефон) ребенка
2. Установить контент-фильтрацию на компьютер (список разрешённых и запрещённых сайтов)
3. Способы дистанционного управления за устройством ребенка.

Почему нужно обезопасить детей от сети Интернет

10 причин:

1. Недостаток реального общения
2. Отсутствие творчества
3. Кибермошенничество
4. Потеря времени, низкое качество образования
5. Нежелательный контент
6. Потеря конфиденциальности персональных данных
7. Бессонница
9. Интернет-зависимость
10. Потеря авторитета родителей и учителей

Программы для контентной фильтрации трафика Интернета



- SkyDNS
- NetPolice Pro
- Интернет-Цензор
- Установить Семейный фильтр для поисковых браузеров (Яндекс, Google Chrome, Mozilla Firefox, Opera)

УСТАНОВКА СЕМЕЙНОГО ФИЛЬТРА В БРАУЗЕРАХ

Google Chrome.

1. Войдите в настройки браузера: Верхний правый значок из трёх горизонтальных линий -> Настройки.
2. Выберите: Начальная группа -> Следующие страницы.
3. Нажмите Добавить, в поле Добавить страницу впишите <http://family.yandex.ru>
4. Нажмите OK

Mozilla Firefox.

1. Войдите в настройки браузера: Правка -> Настройки.
2. Во вкладке Основные выберите: При запуске Firefox Показать домашнюю страницу.
3. В поле Домашняя страница укажите: <http://family.yandex.ru>

Opera.

1. Войдите в настройки браузера: Opera -> Настройки -> Общие настройки.
2. Во вкладке Основные выберите: При запуске Начать с домашней страницы.
3. В поле Домашняя укажите: <http://family.yandex.ru>
4. Нажмите OK.

ГБУ «Институт оценки качества образования РТ»

Памятка родителям «Как обезопасить детей в сети Интернет?»



1) Чтобы обезопасить своих детей в сети интернет, установите в мобильный телефон ребенка приложение



Family Link

1. Google Family Link для родителей (из Play Market или App Stor)
2. На телефоне ребенка установите детский аккаунт, а затем установите Google Family Link для детей.
3. На родительском устройстве откройте приложение Family Link нажмите ДАЛЕЕ и зайдите в свой Google аккаунт и выберите аккаунт ребенка который вы хотите контролировать.
4. Затем приложение попросит вас взять телефон ребёнка: на нём нажмите кнопку «Далее» чтобы получить код подключения.
5. На устройстве ребёнка откройте приложение Google Family Link и выберите опцию «Это устройство», далее выберите Google аккаунт ребёнка.
6. Устройство ребёнка запросит код соединения с Родительского устройства, введите код соединения с родительского устройства в устройство ребёнка.
7. На устройстве ребёнка проверьте почту ребёнка, если потребуется верификация.

Преимущества приложения

Family Link



Возможности приложения :

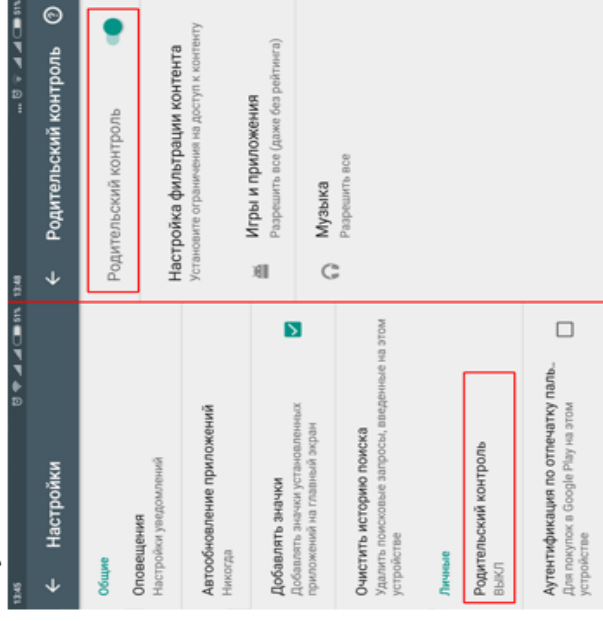
- Получение информации о местонахождении телефона вашего ребёнка;
- Одобрение загрузок и покупок вашего ребёнка на Google Play;
- Установка времени работы экрана телефона. Вы можете устанавливать лимит времени в день с Family Link, на протяжении которого ваш ребёнок может пользоваться своим гаджетом;
- Установка разрешений для приложений на ОС «Андроид» (доступ к микрофону, камере, определение местоположения, доступ к списку контактов);
- Ограничение доступности предлагаемых программ в Google Play, базирующееся на их возрастном рейтинге;
- Сброс пароля к аккаунту Google;
- Установка времени сна телефона ребёнка (например с 23 до 08 часов устройство будет недоступно, за исключением звонков);
- Работа с настройками активности в Google Аккаунт;
- Отдалённая блокировка телефона ребёнка

2) Установите родительский контроль на устройстве ребенка (Android)

Доступен в некоторых телефонах

Родительский контроль на телефоне Андроид — Android не предоставляет много возможностей по родительскому контролю. Создадим ограниченный профиль на телефоне ребенка. Для этого откройте настройки телефона родителя, перейдите в раздел пользователи и добавьте Google аккаунт ребенка и свяжите со своим аккаунтом .

Установите необходимые ограничения, приложения, контент и функции, которые будут доступны на этом аккаунте.



Ссылка на видео установка родительского контроля на телефоне ребенка

https://yandex.ru/efnr?stream_id=vDWDDeGgVGb1o