Онлайн экспресс - конкурс «Воспитание в классе-2022»

Муниципальное автономное учреждение
средняя общеобразовательная школ № 99
имени дважды Героя Советского Союза Бориса Сафонова

Методическая разработка

"КИБЕРБЕЗОПАСНОСТЬ – ЦИФРОВАЯ ГИГИЕНА ДЕТЕЙ"

Автор:
Воронина Ольга Александровна
учитель начальных классов
классный руководитель 4 "А

Краснодар 2022

Пояснительная записка

Номинация конкурса "Работа с родителями".

Тема воспитательного мероприятия:

Родительское собрание "Кибербезопасность - цифровая гигиена детей".

Целевая аудитория - родители учащихся 4 "А" класса МАОУ СОШ № 99.

Цель родительского собрания: сформировать правильное поведение родителей по вопросу кибербезопасности детей.

Задачи:

- ознакомить родителей с возможными рисками при использовании интернета детьми,
- дать рекомендации по предотвращению рисков при использовании интернета детьми,
- подобрать методическую продукцию в помощь родителям по вопросу кибербезопасности детей.

Необходимое оборудование:

- мультимедийный комплекс
- презентация
- памятки для родителей

Наши дети – главная ценность в жизни. В наше время защищать детей от различных неприятностей становится непросто. Современные телефоны и планшеты становятся все сложнее. В связи с этим родителям необходимо постоянно совершенствовать свои знания технологий, чтобы помогать детям правильно использовать гаджеты.

Чем старше становятся дети, тем больше новых проблем появляется. Родители учат своих детей и учатся сами. Нынешние подростки родились буквально со смартфоном в руках, в то время как многие взрослые познакомились с мобильными устройствами уже в сознательном возрасте. Но это не делает ребенка главным техническим специалистом в доме. Даже если ребенок умеет пользоваться интернетом, это не означает, что он осознает последствия каждого действия в Глобальной компьютерной сети Интернет.

В современном мире все большую роль играет киберпространство, постепенно проникающее во все сферы человеческой жизни. Образование, межличностное взаимодействие, работа – эти и другие области все активнее переходят в виртуальное измерение, требуя от людей адаптации под новые, постоянно изменяющиеся условия, а также подразумевающие наличие ряда

специфических знаний об обеспечении собственной безопасности, так как риски виртуальности многие склонны недооценивать.

Особенную группу риска в этой связи представляют школьники разного возраста, которые в силу различных причин относятся к предостережениям достаточно пренебрежительно, а также воспринимают кибер-взаимодействие как нечто естественное и очевидное, так как значительная часть их сознательной жизни с самого начала была связано с кибер-реальностью. По этой причине перед педагогом возникает необходимость не только обучать школьников своему предмету, но и прививать им основы безопасного взаимодействия в виртуальной реальности.

Актуальность заключается в том, что, в связи с вынужденным переходом на дистанционное обучение, очень остро встал вопрос о необходимости защиты интересов детей в онлайн-пространстве, усвоения учениками школы правил кибербезопасности, формированием у них адекватного представления о возможностях и рисках виртуальности, что особенно значимо в период дистанционного обучения.

«Кибербезопасность» определяется как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В рамках нашей работы мы будем рассматривать это явление несколько уже, как совокупность условий, при которых участники взаимодействия в виртуальном пространстве защищены от максимального количества угроз, а также обладают достаточной компетентностью для эффективного и несущего минимальное количество негативных последствий взаимодействия в сети интернет.

Роль данного фактора особенно возрастает в период дистанционного обучения, в который возрастает количество проводимого онлайн времени, а также возникает ряд новых, непривычных ситуаций в киберпространстве, связанных с обучением в виртуальности.

Для получения более объективных данных, на основе которых мы планировали разрабатывать план формирования у школьников представлений о кибербезопасности и развития необходимых навыков, нами было проведено анкетирование учеников школы.

Целью нашего исследования было определить, насколько сформировано представление о кибербезопасности у учащихся школы и на основе полученной информации разработать стратегию совершенствования компетентности учащихся в этой сфере. Для сбора информации о имеющихся у школьников знаниях и получении представления о стратегии их поведения в виртуальной реальность нами была составлена анкета, состоящая из нескольких блоков, включающих в

себя вопросы, касающиеся различных аспектов активности учащихся в киберпространстве:

- общая информация о имеющихся дома устройствах для выхода в сеть,
- базовое понимание существующих в киберпространстве рисков и угроз,
- знание основ кибербезопасности,
- активность в социальных сетях,
- безопасность личной информации,
- значимость активности на страницах в социальных сетях (подписчики, комментарии и т.д.).

Понимая, что не все учащиеся имеют равные возможности в плане доступа в киберпространство, как и неодинаковую заинтересованность в данном процессе, мы постарались отобрать наиболее близкие для различных категорий вопросы, которые позволили бы охватить максимальное количество деталей. При этом мы старались сформулировать их таким образом, чтобы получить представление не только об имеющихся у школьников знаниях и навыках, но и определить основные мотивы их активности в киберпространстве.

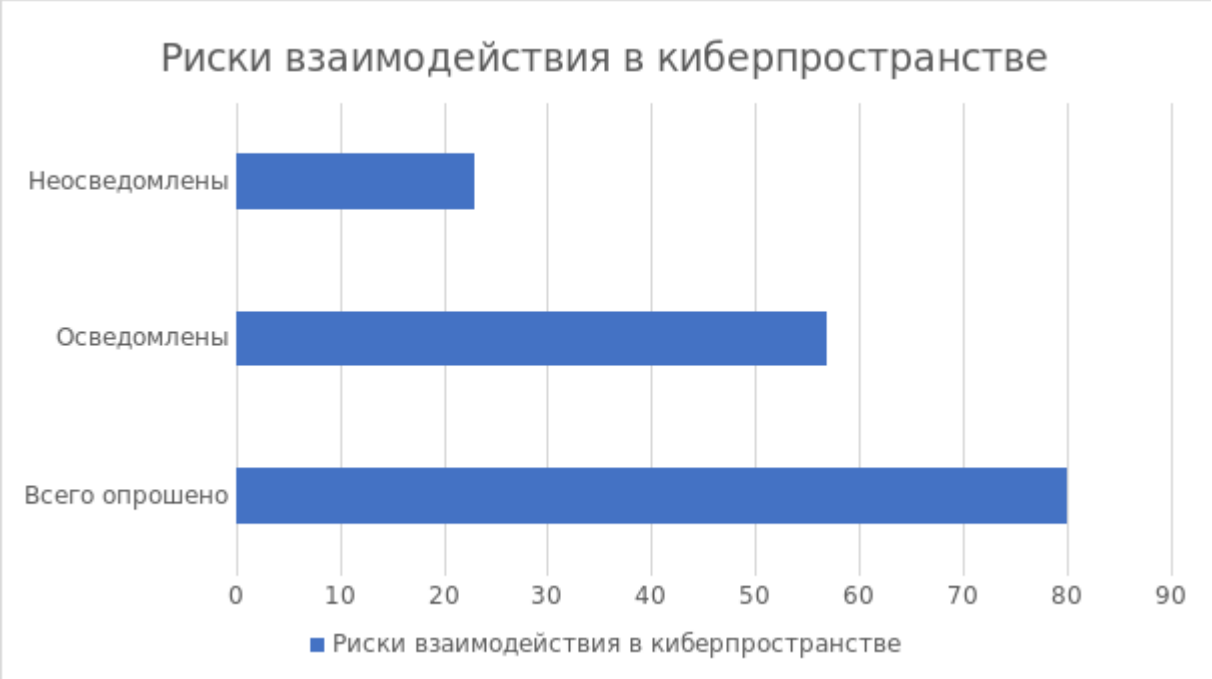
Нами были опрошены учащиеся параллели 4-х классов МАОУ СОШ № 99, в количестве 90 человек, так как именно эта группа учеников осуществляет наиболее активную коммуникацию в интернет пространстве, а также действует в нем с минимальным контролем со стороны взрослых или вовсе без него. Кроме того, эти дети, являются крайне подверженной психологическому воздействию возрастной группой, так как их эмоциональные потребности и потребности в самоутверждении в значительной степени влияют на мотивы их поступков, а также на способность критически воспринимать получаемую информацию и имеют потребность в копировании действий, не всегда правоправных и безопасных, людей, которые для них являются авторитетом. Что включает представителей этой возрастной категории в группу риска.

Рассматривая ответы учащихся на вопросы анкеты, считаем целесообразным проанализировать каждый блок анкеты отдельно.

Первый блок касался рисков взаимодействия в киберпространстве. Необходимо констатировать, что подростки осведомлены о существующих в интернете угрозах школьники независимо от возраста. Положительный ответ дал 75% опрошенных. Согласно полученным результатам, они имеют представление о достаточно широком спектре виртуальных угроз, однако к некоторым из них продолжат относиться достаточно несерьезно, что будет подробно описано далее в статье. Среди широко известных им рисков виртуальности, школьники называют:

- кражу личной информации,
- взлом страниц в социальных сетях,
- вирусы.

Диаграмма №1



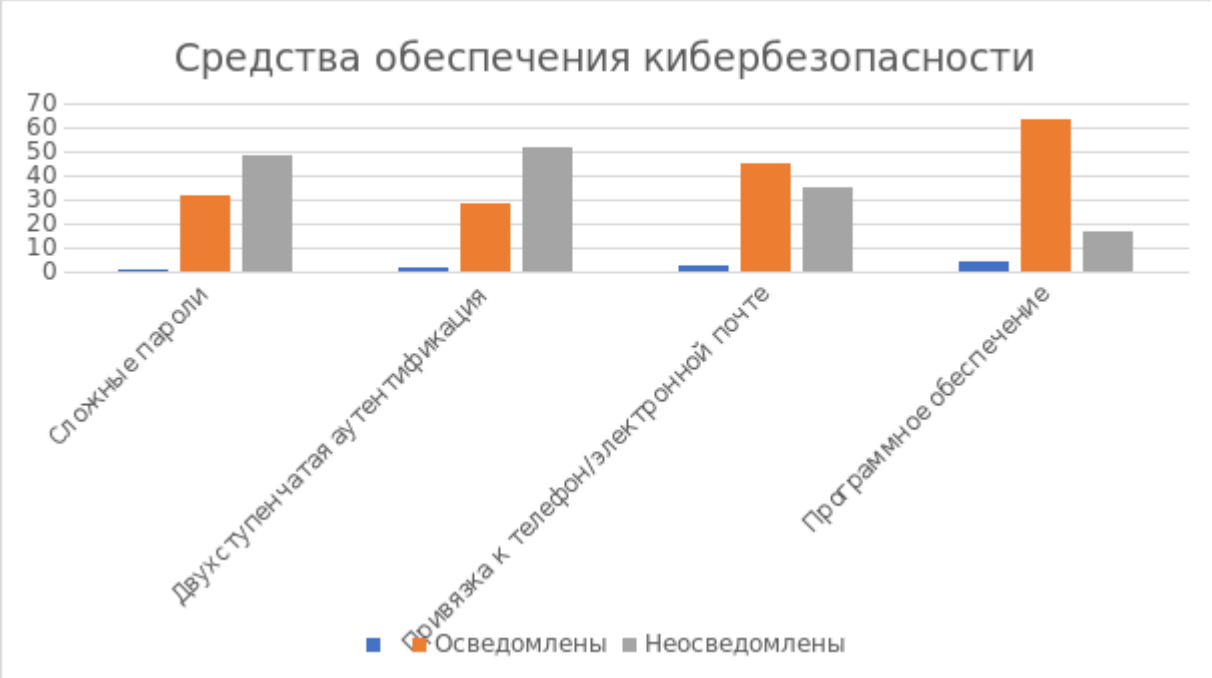
При этом такие явления, как кибербуллинг и вредоносная информация (а также манипулирование с преступными целями) названы не были. Делаем вывод, что школьники не рассматривают их как риски, при том, что проблема травли в сети интернет достаточно активно обсуждается на всех уровнях, также, как и вопрос о так называемых «группах смерти», а также манипулирование и вовлечение подростков в преступные схемы. Предположительно, это может быть обусловлено отсутствием таких случаев в опыте самих школьников и их окружения, а также низким уровнем заинтересованности в сообщениях СМИ и недоверием к ним.

Отвечая на вопросы о способах защиты от кражи личной информации, участники опроса показали низкий процент осведомлённости. Хотя 40% (32 человека) понимают значение соблюдения правил кибербезопасности для своей активности в виртуальности. Для этого ими используются:

- сложные пароли,
- двухступенчатая аутентификация,

- привязка аккаунта к номеру телефона или адресу электронной почты,
- программное обеспечение (антивирусы).

Диаграмма №2



Осведомленность учащихся о средствах обеспечения кибербезопасности

В тоже время ученики концентрируют своё внимание скорее на технических и программных способах обеспечения собственной кибербезопасности, забывая о правилах поведения и коммуникации в виртуальном пространстве, что подтверждают их дальнейшие ответы.

Можем сделать вывод, что, находясь в сети интернет, школьники не до конца осознают риски, связанные с общением, особенно с общением с незнакомцами. Согласно результатам анкетирования, многие школьники (половина от опрошенных) размещают на страничке личные фото достаточно редко, но обмениваются ими в личных переписках. Однако, мы должны заметить, что метками геолокации ученики не пользуются (90% учащихся отрицают их использование).

В личной переписке они стараются не распространяться о деталях своей жизни, но 28% учащихся иногда передают личные данные вроде номеров телефон и адресов, как правило только близким и хорошим друзьям. Но стоит отметить, что были ученики, говорившие, что интернет-друзьям после долгого общения могут предоставить эту информацию. На просьбу уточнить, как именно они решают, кому дать эти данные, школьники использовали формулировку «чувствую, что этому человеку можно доверять», что сохраняет наличие рисков со

стороны виртуальных знакомых, поскольку многим из них в силу возраста не хватает жизненного опыта и понимания окружающих, чтобы определить настоящие намерения собеседника.

Как должны родители и взрослые помочь детям избежать все возможные неприятности, чтобы сделать их пребывание в интернете более безопасным, научить их ориентироваться во всемирной сети? Конечно же, отказ от использования этих современных технологий не является решением проблемы защиты детей в онлайн-пространстве. Это все равно что запретить ездить автотранспорту по улицам и придворовым территориям, чтобы дети не попадали в ДТП. Во избежание несчастных случаев нужно лишь научить ребенка быть осторожным, соблюдать определенные правила, быть ответственным пешеходом, следовать положительному примеру взрослых. Аналогично наиболее важной задачей взрослых является предупреждение детей об опасностях Интернета, чтобы они вели себя осторожно, обдуманно. Кроме того, необходимо обсуждать с детьми все те вопросы, которые могут у них возникнуть при использовании Интернета.

Представим советы родителям для кибербезопасности детей:

Постоянно наблюдайте за поведением детей. Не забывайте, что любые попытки приблизиться к ребенку он будет обсуждать со своими идеологами в соцсетях. Ему будут пояснять примерно так: «не слушай родителей, слушай нас».

Постарайтесь вернуть ребенка в семью. Родительская любовь и тепло могут в этом помочь.

Рекомендации по техническому контролю.

1. Используйте инструменты родительского контроля. Функции родительского контроля можно использовать как в браузерах, так и в антивирусных программах. Например, в ESET NOD32 SmartSecurity, KasperskyInternetSecurity предусмотрен модуль «Родительский контроль». Кроме того, вы можете выбрать специальное мобильное приложение – ESET NOD32 ParentalControl для Android.

Существуют подобные инструменты для игровых приставок, таких как NintendoWii, Playstation и Xbox 360. Особенно полезны будут те отчеты, которые вам предоставит Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary InternetFiles в операционной системе).

2. Не разрешайте детям публиковать в интернете личную информацию. Запомните и объясните детям, что конфиденциальная информация никогда не запрашивается по электронной почте или в чате.

3. Не удаляйте сообщения агрессора, история сообщений послужит доказательством акта воздействия.

4. Объясните ребенку, что далеко не вся информация в интернете достойна доверия.

5. Ведите с ребенком открытый диалог. Ключевую роль в обеспечении безопасности детей играет общение с ними. Разговоры о безопасности, страхах и проблемах намного эффективнее наказаний. Доброжелательная атмосфера в семье и открытый диалог способствуют успешному развитию ребенка.

6. Все, что попало в интернет, останется там навсегда. Объясните детям, что информация, проиндексированная поисковыми системами, навсегда останется в Сети. Хуже того, после публикации пользователь теряет контроль над своими данными, любой может использовать и распространять эту информацию. Пусть дети возьмут за правило никогда не публиковать фотографии, статусы и другой контент, который они не хотели бы показывать родителям или родственникам. Это распространяется на соцсети, мессенджеры, блоги и другие сервисы.

7. Не рекомендуется создавать для ребенка учетную запись с правами администратора.

8. Настройте использование https. Убедитесь в том, что ваш ребенок открывает сайты с защищенным протоколом https (наименование протокола отображается в адресной строке браузера). Это позволит избежать перехвата информации – данные передаются в зашифрованном формате, который не распознают вредоносные программы. Посоветуйте детям-подросткам использовать эти настройки и при доступе к соцсетям через публичный Wi-Fi.

9. Используйте надежные пароли. Напомните детям, что пароли нельзя передавать или давать на время даже лучшим друзьям.

10. Настройте параметры безопасности для социальных сетей. Параметры безопасности в соцсетях, установленные по умолчанию, не гарантируют безопасности. Рекомендуется посвятить немного времени их правильной настройке и проверить, какая информация находится под угрозой утечки.

Тактические подсказки для родителей

1. Создайте для ребенка учетную запись с правами обычного пользователя – это позволит вам эффективно контролировать его онлайн-активность. Учетная запись с правами администратора должна использоваться только взрослым.

2. Не забывайте регулярно обновлять антивирус и программу родительского контроля.

3. Просматривайте историю посещения сайтов ребенком. Если вы обнаружите, что история подчищена, найдите повод, чтобы с ребенком поговорить.

4. Проверьте настройки веб-камеры и убедитесь, что она отключена или закрыта, если в данный момент не используется.

5. Проверьте настройки профиля ребенка в соцсетях. Открытый доступ к профилю может подвергнуть ребенка риску.

6. Не переходите по подозрительным ссылкам

7. Скачивайте программы и мобильные приложения только из официальных источников

8. Используйте комплексные антивирусные продукты и решения.

9. Избегайте заполнения сомнительных форм с персональными данными в Сети.

10. Не открывайте файлы от неизвестных отправителей.

КИБЕРБЕЗОПАСНОСТЬ

=

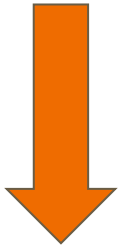
ЦИФРОВАЯ ГИГИЕНА

Родительский контроль

ДОЗИРОВАТЬ ВРЕМЯ

ЗАЩИТА ИНФОРМАЦИИ

КУЛЬТУРА МЕДИАПОТРЕБЛЕНИЯ В СЕМЬЕ



МЕДИА-ИНФОРМАЦИОННАЯ ГРАМОТНОСТЬ

Медиа-информационная грамотность

Формирование у молодого поколения следующих компетенций:

- техническая компетенция (защита компьютера и гаджетов, каналов связи, программного обеспечения);
- информационная компетенция (защита от информационного перегруза, оценка достоверности источников информации и новостей, поиск информации в сети);
- коммуникативная компетенция (защита от буллинга, навыки позитивного общения в сети, киберкультура);
- коммерческая компетенция (защита своих прав потребителя).

СРЕДСТВА РОДИТЕЛЬ-СКОГО КОНТРОЛЯ

https://www.kaspersky.ru/safe-kids

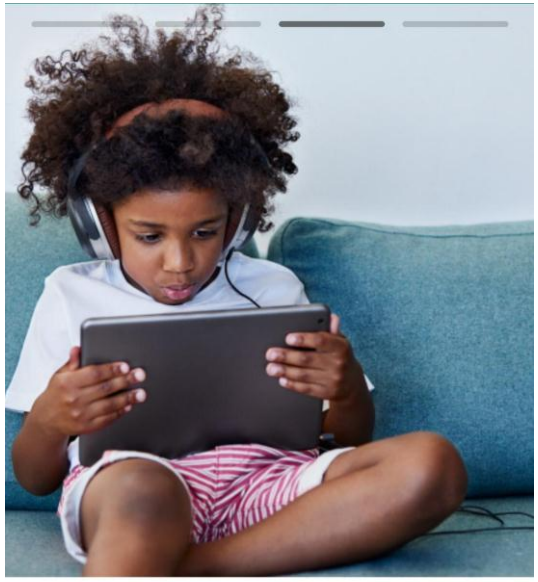
Kaspersky
Safe Kids

GPS ТРЕКЕР

Kaspersky Safe Kids

Учите детей здоровым привычкам — задавайте график использования устройств

Всегда знайте, где ваш ребенок. Используйте GPS



Разрешайте только подходящие по возрасту сайты и приложения

Контроль времени использования устройства

Данные о местонахождении ребенка и заряде батареи устройства

Блокирование нежелательных запросов в YouTube

НОВИНКА

Выберите нужную версию решения

GPS ТРЕКЕР

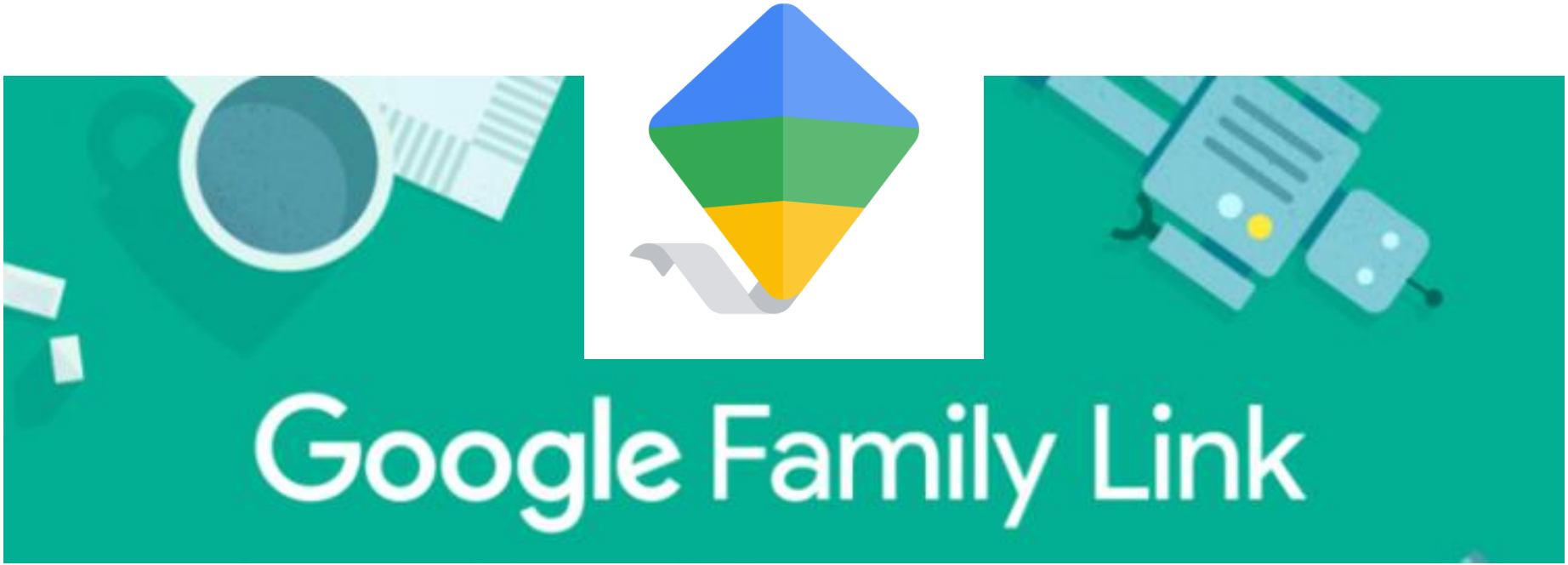
Kaspersky Safe Kids

	Kaspersky Safe Kids Бесплатная версия	Рекомендуем Kaspersky Safe Kids Премиум версия
КОНТРОЛЬ АКТИВНОСТИ В ИНТЕРНЕТЕ Защищайте детей от поиска неподходящих сайтов и информации*	✓	✓
БЕЗОПАСНЫЙ ПОИСК В YOUTUBE НОВИНКА Блокируйте нежелательные запросы ребенка в YouTube**	✓	✓
КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ПРОГРАММ Регулируйте использование программ на компьютере и мобильных устройствах*	✓	✓
КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ УСТРОЙСТВ Контролируйте время ежедневного использования устройств*	✓	✓

БЕСПЛАТНО

900 руб/год

ИСПОЛЬЗОВАНИЕ УСТРОЙСТВА ПО РАСПИСАНИЮ Задавайте интервалы времени, когда ребенок не может использовать устройство*	✓
ОПРЕДЕЛЕНИЕ МЕСТОНАХОЖДЕНИЯ РЕБЕНКА Всегда знайте, где ваш ребенок, и установите для него безопасный периметр	✓
КОНТРОЛЬ ЗАРЯДА БАТАРЕИ Получайте сообщения о низком уровне заряда батареи на устройстве ребенка	✓
КОНТРОЛЬ АКТИВНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ Будьте в курсе публикаций ребенка ВКонтакте с помощью My Kaspersky	✓
ИСТОРИЯ ПОИСКОВЫХ ЗАПРОСОВ В YOUTUBE новинка Будьте в курсе того, чем интересуется ваш ребенок**	✓
УВЕДОМЛЕНИЯ В РЕАЛЬНОМ ВРЕМЕНИ Получайте уведомления на мобильное устройство в тех случаях, когда ребенок пытался открыть запрещенный сайт, вышел за пределы безопасного периметра и т.д.	✓



https://families.google.com/familylink/

БЕСПЛАТНО

Безопасность и польза

Отслеживание действий

Управление приложениями

Приложения для детей

Ознакомьтесь со списком рекомендованного контента. Он составлен преподавателями и поможет вам выбрать приложения, которые будут полезны для вашего ребенка***.

Время использования

Установка ограничений

Решите, сколько времени ваш ребенок может использовать устройство в течение дня. С помощью Family Link можно устанавливать ограничения и блокировать устройство на ночь.

Блокировка устройства

Отслеживание местоположения

Теперь вы будете знать, где находится ваш ребенок. Просто откройте Family Link и посмотрите местоположение его мобильного устройства****.

Norton Family parental control

Родительский контроль Norton Family - один из главных конкурентов "Касперского". Приложение отмечено множеством профессиональных наград. По словам производителя, оно позволяет обучать детей правилам безопасного поведения в интернете и настраивать домашние правила.

Norton Family мало чем отличается по функциональности от "Касперского", имеет хорошие отзывы пользователей и экспертов. **Стоимость: 1240 рублей в год.** Совместимость: Android, iOS.

https://family.norton.com/web/

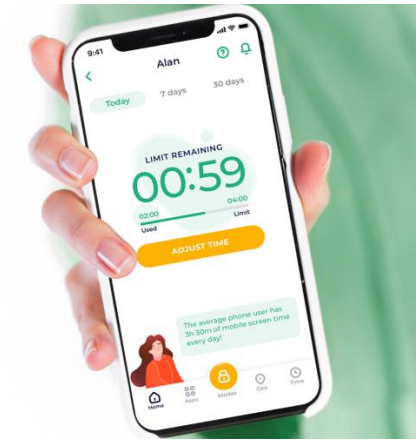
Kidslox

Приложение также одобрено экспертами Роскачества и имеет хорошие оценки пользователей.

В Kidslox можно контролировать до 10 аккаунтов одновременно на различных устройствах. Приложение позволяет настроить фильтр контента, установить расписание использования смартфона и удаленно блокировать доступ к камере.

Стоимость: 1240 рублей в год. Совместимость: Android, iOS.

KIDSLOX
Parental control app



https://kidslox.com/ru

Мониторинг социальных сетей

https://gerdabot.ru/

Бесплатно

- Проверка опасных групп

Расширенный

138 руб / месяц

- Проверка опасных групп
- Подписка на уведомления
- Лайки опасного контента
- Комментарии опасного контента
- Опасные группы друзей
- Подозрительные друзья
- Мат в соц. сетях
- Время проведенное онлайн

Школьная версия

Бесплатно - по запросу

- Добавление классов
- Массовая загрузка всех учеников
- Ежедневный мониторинг
- Отчеты на почту

Внимание родители!

Убедительная просьба, зайти на страницу в социальной сети «ВКонтакте», «Одноклассники», «**Fasebook**» к вашим детям и отследить подписаны ли они на «группы смерти»:

- Синий кит;
- Море китов;
- Мертвые души;
- Тихий дон;
- Я в игре;
- F 57
- Ff 33
- Море дельфинов;
- Беги или умри;
- 150 звезд;
- Разбуди меня в 4.20;
- f 57
- d 28

ОБРАТИТЕ ВНИМАНИЕ КАКИЕ ЗАПИСИ НАХОДЯТСЯ НА «СТЕНЕ» СТРАНИЦЫ ВАШЕГО РЕБЕНКА

Родители! Безопасность вашего ребенка в интернет пространстве это Вы!