КИБЕРБЕЗОПАСНОСТЬ

ПРОФИЛАКТИКА
федеральный центр

БЕЗОПАСНОСТЬ ПАРОЛЕЙ: ЧТО НУЖНО ЗНАТЬ

Пароль — это ключ ко всей личной информации вашего ребенка в сети. Если злоумышленник получит доступ к аккаунтам, он сможет украсть личные данные, фотографии, переписки, деньги и даже воспользоваться именем вашего ребенка для мошеннических действий.

- Используйте длинные пароли от 8 символов.
  Пример: «NekotoryySlOzhnyParol123»
- Создавайте уникальные комбинации с буквами разного регистра (заглавные и строчные), цифрами и специальными символами (!@#$%^&*).
  Пример: «7mYpAsSwOrDwItHSpEcIaLSymBoL$»
- Не используйте имена, фамилии, даты рождения, номера телефонов или любые легкоугадываемые слова и последовательности («qwerty», «password»).
- Меняйте пароли регулярно (минимум раз в полгода).
- Не записывайте пароли на бумаге или в незашифрованных файлах на компьютере. Используйте специализированные менеджеры паролей.
- Используйте двухфакторную аутентификацию.
- Объясните опасность фишинга. Расскажите детям о рисках перехода по подозрительным ссылкам и ввода персональных данных на незнакомых сайтах.
- Ограничьте доступ к публичным сетям Wi-Fi.

Важно регулярно напоминать эти советы своим детям, ведь безопасность — дело первостепенной важности!

ПРОФИЛАКТИКА
федеральный центр

ИНТЕРНЕТ-ЗАВИСИМОСТЬ: ЧТО ЭТО ТАКОЕ И ПОЧЕМУ ВОЗНИКАЕТ?

Интернет-зависимость – это патологическое состояние, характеризующееся неконтролируемым желанием проводить большое количество времени в сети.

Признаки интернет-зависимости:

- потребность постоянно проверять уведомления и обновления социальных сетей,
- раздражительность и агрессия при попытке ограничить доступ к гаджетам,
- снижение интереса к учебе, хобби и общению вне интернета,
- трудности засыпания и бессонница,
- проблемы с концентрацией внимания и памятью.

Причины возникновения интернет-зависимости

- Недостаточная социализация.
- Потребность в самовыражении.
- Отсутствие самоконтроля.
- Эмоциональная неудовлетворенность.
- Низкая самооценка. Для некоторых подростков виртуальное пространство становится

Рекомендации родителям:

- организуйте онлайн-досуг ребенка: развивающие занятия, видеоуроки на проверенных цифровых платформах; фильмы, каналы с видеоконтентом;
- для детей до 14 лет установите соответствующие настройки («семейные», «детские»), минимизирующие встречи с деструктивным контентом;
- способствуйте вовлечению ребенка в реальные группы сверстников (кружки, секции, лагеря и т. д.);
- обратите внимание подростков на опасность общения в Интернете с незнакомцами;
- договоритесь с ребенком о доступном количестве сетевой активности в сутки;
- развивайте цифровую грамотность ребенка;
- расскажите, что в случае встречи в Интернете с неприятным и пугающим контентом, он может поделиться этими фактами с родителями;
- при обнаружении признаков деструктивного поведения ребенка обратитесь за помощью к специалистам (психологи, службы горячей линии).

ПРОФИЛАКТИКА
федеральный центр

КАК ЗАЩИТИТЬ РЕБЁНКА ОТ НЕЖЕЛАТЕЛЬНОГО КОНТЕНТА В ИНТЕРНЕТЕ?

Для защиты детей от вредоносного контента в Интернете можно использовать встроенные функции различных цифровых платформ и устройств.

СЕМЕЙНЫЕ АККАУНТЫ

Многие популярные сервисы предлагают возможность создания семейных аккаунтов, объединяющих взрослых и детей в одну группу пользователей. Это позволяет взрослым контролировать доступ детей к контенту и приложениям.

ДЕТСКИЙ РЕЖИМ

Некоторые устройства и браузеры имеют специальные детские режимы, которые фильтруют результаты поиска, ограничивают доступ к нежелательным сайтам и позволяют выбирать категории просматриваемого контента.

РОДИТЕЛЬСКИЙ КОНТРОЛЬ

Большинство смартфонов и планшетов поддерживают инструменты родительского контроля, которые позволяют ограничивать доступ к определённым приложениям, играм, покупкам и медиаконтенту.

АНТИВИРУСНЫЕ ПРОГРАММЫ

Антивирусные решения с функцией защиты детей не только защищают устройство от вредоносного программного обеспечения и фишинга, но и предоставляют отчёты о действиях ребёнка в интернете.

! Важно помнить, что ни одна программа не способна заменить активное участие взрослого в формировании культуры безопасного поведения ребёнка в цифровом пространстве.

ПРОФИЛАКТИКА
федеральный центр

КАК ЗАЩИТИТЬ РЕБЕНКА ОТ ПРОВОКАТОРОВ В ИНТЕРНЕТЕ?

- Обсудите с ребенком активизацию деятельности по вербовке в террористические организации. Расскажите, какую опасность жизни и здоровью людей несут такие организации. Предупредите об уголовной ответственности.
- Сообщите ребенку, что необходимо игнорировать сомнительные предложения и сообщения. Если поступят такие сообщения, необходимо сообщить взрослому. Если сообщения уже поступили, успокойте и поддержите ребенка.
- Вместе изучите настройки социальных сетей и мессенджеров. Поставьте запрет на входящие звонки и сообщения с неизвестных номеров.
- При поступлении информации о призывах к террористической деятельности – сообщите в правоохранительные органы (номер 102).

Помните: лучшая защита вашего ребенка — это ваша осведомленность, поддержка и доверие!

ПРОФИЛАКТИКА
федеральный центр

КАК ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ РЕБЕНКА В ИНТЕРНЕТЕ?

ОБУЧЕНИЕ ОСНОВАМ ЦИФРОВОЙ ГРАМОТНОСТИ

Рассказывайте детям правила безопасного поведения в интернете, объясняйте последствия необдуманных действий.

ИСПОЛЬЗОВАНИЕ АНТИВИРУСНЫХ ПРОГРАММ И ФИЛЬТРОВ

Установите специальные программы, блокирующие доступ к нежелательным сайтам и защищающие устройства от вирусов.

КОНТРОЛЬ ПРИВАТНОСТИ АККАУНТА

Настройте ограничения видимости профилей и публикаций в социальных сетях, убедитесь, что ребенок правильно настраивает уровень конфиденциальности.

ОГРАНИЧЕНИЕ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Следите за количеством времени, которое ребенок проводит онлайн, помогайте организовывать режим отдыха и занятий вне интернета.

СОЗДАНИЕ ДОВЕРИТЕЛЬНЫХ ОТНОШЕНИЙ

Поддерживайте открытый диалог с ребенком, позволяйте ему делиться своими переживаниями и сомнениями относительно взаимодействия в сети.

ПРОФИЛАКТИКА
федеральный центр

КАК ПРОТИВОСТОЯТЬ ВОВЛЕЧЕНИЮ РЕБЕНКА В ПРОТИВОПРАВНУЮ ДЕЯТЕЛЬНОСТЬ?

Вовлечение – это склонение, вербовка или иное завлечение ребенка путем уговоров, предложений, обещаний, обмана, угроз или иным способом в совершение преступления или антиобщественных действий.

Это могут быть:

- участие в экстремистских или террористических группировках;
- участие в несанкционированных акциях и митингах;
- сбор информации или выполнение задач в интересах злоумышленников и т. д.

Основные признаки возможного риска

- резкое изменение поведения подростка, изоляция от семьи и друзей, замкнутость;
- частое посещение закрытых групп и чатов, закрытие экрана компьютера или телефона при появлении взрослых;
- появление новых знакомых в социальных сетях, общение с незнакомцами;
- повышенный интерес к радикальным идеям, агрессивная риторика, отрицательное отношение к другим людям и обществу;
- скрытность в финансовых вопросах, появление непонятных источников дохода.

ПРОФИЛАКТИКА
федеральный центр

Что должно насторожить ребенка

- собеседник задает много вопросов о личной жизни;
- просит об одолжении взамен на что-либо;
- задает вопросы о том, кто из родителей, родственников, друзей имеет доступ к телефону или аккаунту;
- просит держать общение в секрете;
- задает вопросы личного и интимного характера;
- заставляет чувствовать себя виноватым или угрожает;
- настаивает на личной встрече;
- лестно говорит о внешнем виде.

Виды опасных сообщений

- призывы к совершению противоправных действий, самоубийству, причинению себе телесных повреждений;
- инструкции по изготовлению взрывных устройств и оружия;
- распространение экстремистских идей (материалов) и пропаганды;
- угрозы, шантаж;
- подозрительные тематические подборки

ПРОФИЛАКТИКА
федеральный центр

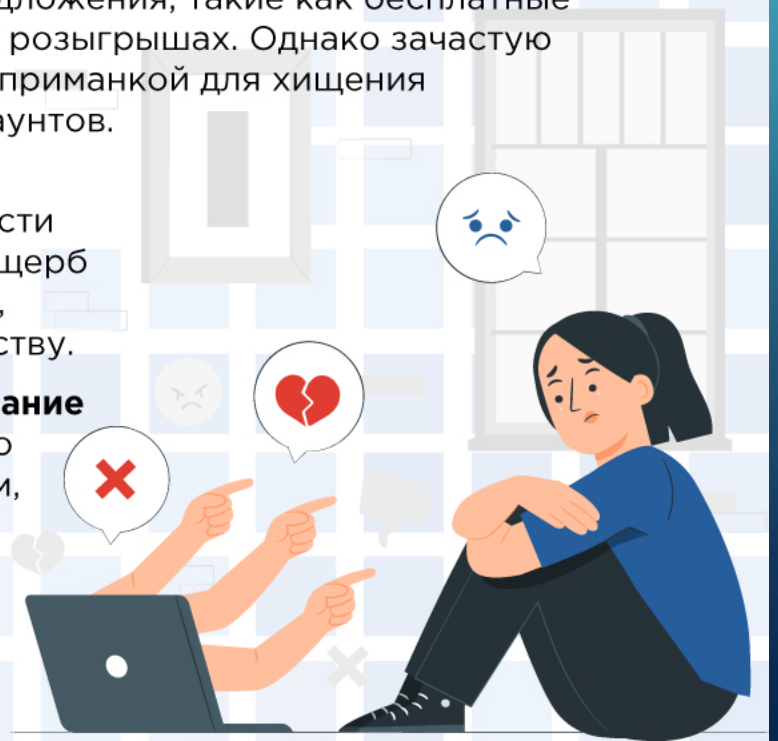
ЧТО ВАЖНО СДЕЛАТЬ РОДИТЕЛЯМ?

- Поддерживайте открытый диалог с ребенком.
- Установите правила пользования интернетом совместно с ребенком, обсудив последствия нарушения правил.
- Регулярно проверяйте историю посещений, устройства и приложения, которыми пользуется ребенок.
- Изучите основные методы вербовки, используемые злоумышленниками.
- Предупредите ребенка о рисках публикации личной информации, фотографий, местоположения. Обучите правилам защиты персональных данных, использованию надежных паролей.
- Подавайте личный пример. Соблюдайте принципы безопасной цифровой гигиены.

ПРОФИЛАКТИКА
федеральный центр

КАКИЕ РИСКИ ЕСТЬ В ИНТЕРНЕТЕ?

- **Фишинговые атаки.** Фишеры маскируются под официальные ресурсы и службы, пытаясь обмануть пользователей и украсть личные данные, пароли и финансовую информацию.
- **Кража персональных данных.** Утечка персональной информации может привести к финансовым потерям, шантажу или другим негативным последствиям.
- **Интернет-мошенничество.** Детей привлекают яркие рекламные объявления и заманчивые предложения, такие как бесплатные подарки, скидки или участие в розыгрышах. Однако зачастую подобные акции оказываются приманкой для хищения денег или компрометации аккаунтов.
- **Буллинг и травля в сети.** Онлайн-травля способна нанести серьезный психологический ущерб ребенку, приводя к депрессии, замкнутости и даже самоубийству.
- **Нецелесообразное использование Интернета.** Подростки нередко теряют контроль над временем, проводимым онлайн, что негативно сказывается на учебе, здоровье и социальной активности.



ПРОФИЛАКТИКА
федеральный центр

СОВРЕМЕННЫЕ ОПАСНОСТИ ОНЛАЙН-КОММУНИКАЦИЙ: КИБЕР-ГРУМИНГ

Груминг (англ. grooming – «ухаживание») – долговременное установление взрослым близких, доверительных отношений с ребёнком (а также с членами его семьи) с целью завоевания доверия и последующего совращения.

Методы манипуляции:

- длительное «ухаживание»;
- привлечение ребёнка тёплой дружбой или романтичными отношениями;
- принятие роли наставника;
- постепенное дистанцирование жертвы от её окружения;
- постепенная «нормализация» прикосновений, нарушение личных границ и представление недопустимого поведения как нормального явления;
- давление и манипулирование чувством вины и ответственности жертвы.

Кибер-груминг (онлайн-груминг) – привлечение ребёнка осуществляется посредством социальных сетей и интернет-мессенджеров. Этот вид чаще всего направлен на подростков 12–15 лет, причем большинство пострадавших составляют девушки: отправка интимных фотографий и видеозаписей.

ПРОФИЛАКТИКА
федеральный центр

Признаки кибер-груминга, которые должны настораживать родителей и педагогов:

- Резкое изменение поведения ребёнка: скрытность, нервозность;
- Интенсивное общение в сети преимущественно поздно вечером или ночью;
- Изоляция от семьи и реальных друзей;
- Чрезмерная привязанность к новому знакомству, желание поддерживать связь именно с ним;
- Появление необычных подарков или денег;
- Проблемы с учебой и поведением;
- Изменение стиля речи и манеры общения;
- Создание скрытых аккаунтов, установка приложений для анонимизации;
- Отсутствие желания говорить о личной жизни;
- Стремление закрыть экран смартфона или компьютера при появлении родителя.

Как действовать, если произошел случай кибер-груминга:

- немедленно обратитесь в правоохранительные органы с подробным описанием ситуации и всеми имеющимися доказательствами (переписки, профили преступников);
- удалите контакт злоумышленника и заблокируйте его аккаунты;
- подключите специалиста-психолога для оказания помощи;
- проверьте безопасность устройства ребенка (обновление антивирусных программ, смена паролей).

ПРОФИЛАКТИКА
федеральный центр

СОВРЕМЕННЫЕ ОПАСНОСТИ ОНЛАЙН-КОММУНИКАЦИЙ: СЕКСТИНГ

Секстинг – обмен откровенными сообщениями, изображениями или видеороликами сексуального характера с использованием цифровых устройств.

Формы проявления секстинга:

- обмен личными снимками/видео обнажённого тела или интимных частей тела;
- сообщения откровенно сексуального характера.

Формы проявления секстинга:

- психологическое давление и эмоциональные травмы;
- издевательства и травля в интернете (буллинг);
- нарушение чувства собственного достоинства и самооценки;
- угроза безопасности и возможные преследования;
- возможность нарушения закона, если фотографии распространяются без согласия или принадлежат лицам младше 18 лет.

Причины возникновения секстинга:

- давление сверстников и желание соответствовать ожиданиям группы;
- привычка демонстрировать свою привлекательность и уверенность;
- незнание последствий распространения подобной информации;
- манипуляции со стороны посторонних лиц, использующих угрозу или обман.

ПРОФИЛАКТИКА
федеральный центр

Основные меры защиты от кибер-груминга и секстинга

- Открыто говорите с детьми о последствиях обмена материалами личного, интимного характера, особенно в эпоху высоких технологий и быстрого распространения информации.
- Мониторьте использование соцсетей и обеспечьте установку защитных программ на устройствах.
- Помогите ребёнку развивать критическое мышление и умение оценивать риски.
- Поддерживайте открытый диалог и убедитесь, что ребёнок чувствует себя комфортно, обращаясь к вам за поддержкой.
- Покажите важность соблюдения приватности и ограничения круга лиц, которым доступна такая информация.

ПРОФИЛАКТИКА
федеральный центр

КОМПЬЮТЕРНЫЕ ИГРЫ: ПРОФИЛАКТИКА ЗАВИСИМОСТИ

Польза компьютерных игр

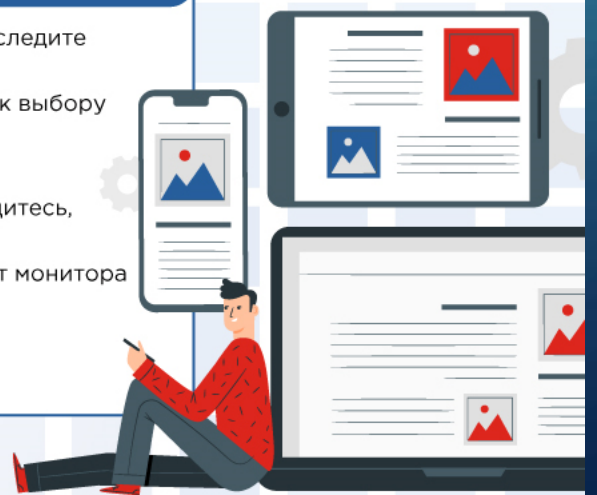
- Игры стимулируют мышление, память, реакцию и способность быстро принимать решения.
- Многопользовательские игры помогают развивать коммуникативные навыки и умение работать в команде.
- Некоторые исследования показывают, что умеренное игровое время помогает снять стресс и напряжение.
- Существуют образовательные игры, способствующие изучению иностранных языков, математики, физики и других дисциплин.

Потенциальный вред

- Чрезмерное увлечение компьютерными играми может стать причиной психологической зависимости, приводящей к проблемам с учёбой, общением и здоровьем.
- Долгое сидение за компьютером негативно влияет на зрение, осанку и общее физическое состояние организма.
- Агрессивные и жестокие игры могут способствовать повышению уровня агрессии и снижению эмпатии.
- Современные игры требуют вложений денег на покупку дополнительного оборудования, подписки и внутриигровые покупки.

Как предотвратить развитие игровой зависимости?

- Определите ежедневные лимиты игрового времени и строго следите за соблюдением этих ограничений.
- Обсудите пользу и вред, чтобы ребёнок осознанно подходил к выбору игровых занятий.
- Предлагайте альтернативные виды досуга.
- Просматривайте содержимое любимых игр ваших детей, убедитесь, что они соответствуют возрасту и интересам ребёнка.
- Создавайте семейные мероприятия, чтобы отвлечь ребёнка от монитора и укрепить семейную связь.
- Ограничьте собственное время, проведённое за гаджетами, демонстрируйте активный образ жизни.



ПРОФИЛАКТИКА
федеральный центр

ОСНОВНЫЕ ПРАВИЛА ОНЛАЙН-ПОКУПОК

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ РОДИТЕЛЯМ

- Объясните основы финансовой грамотности: познакомьте ребёнка с понятием бюджета, накопления, расходов и экономии.
- Учите сравнивать цены и выбирать качественные товары.
- Научите ребёнка проверять надежность сайта магазина и защиту платежей.
- Старайтесь ограничить импульсивные покупки ребёнка, поощряя размышления и взвешенный подход к приобретению вещей.
- Договоритесь заранее о совместных обсуждениях крупных покупок, чтобы оценить целесообразность приобретения.
- Включите ребёнка в процесс планирования семейных трат, позволяя ему видеть реальные финансовые потоки и учиться распределять бюджет.
- Исключить неограниченный доступ ребёнка к платёжным средствам.

ПОЧЕМУ КОНТРОЛИРОВАТЬ ОНЛАЙН-ПОКУПКИ ВАЖНО?

- Дети и подростки нередко совершают необдуманные покупки, соблазнившись яркой рекламой или скидками.
- Незрелость финансового сознания может привести к накоплению долгов, кредитов и микрозаймов.
- Погруженность в мир потребления снижает мотивацию к активному отдыху, творчеству и спорту.
- Множество рекламных предложений способно утомлять мозг и вызывать усталость от принятия решений.
- Желание обладать дорогими вещами иногда связано с неуверенностью в себе, чувством неполноценности и желанием привлечь внимание сверстников.

ПРОФИЛАКТИКА
федеральный центр

СКОЛЬКО ВРЕМЕНИ МОЖЕТ ПРОВОДИТЬ РЕБЁНОК У ЭКРАНА?

Суммарная ежедневная продолжительность работы с электронными устройствами, оборудованными экранами (компьютерами, планшетами, смартфонами и пр.)

ДЛЯ ДЕТЕЙ ДО 2–3 ЛЕТ

Максимально исключить гаджеты.
Заменить экранное время на сенсорную игру с реальными объектами (игрушки, природные элементы)

ДЛЯ ДЕТЕЙ ОТ 2–3 ЛЕТ

не более 20 минут в день

ДЛЯ ДЕТЕЙ ОТ 3–7 ЛЕТ

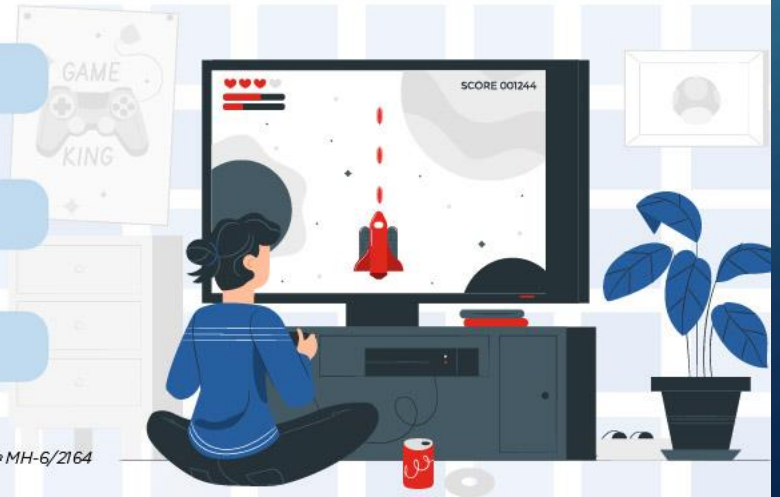
не более 1 часа в день

ДЛЯ ДЕТЕЙ ОТ 7 ДО 11 ЛЕТ

не более 1,5 часа в день

ДЛЯ ДЕТЕЙ ОТ 11 ДО 16 ЛЕТ

не более 2 часов в день



Согласно Письму Министерства образования и науки РФ от 24.07.2025 № МН-6/2164 «О направлении методических рекомендаций»

ПРОФИЛАКТИКА
федеральный центр

КАК ПОМОЧЬ ВЫЯВИТЬ ФЕЙКИ И БОТЫ СРЕДИ АККАУНТОВ В СОЦИАЛЬНЫХ СЕТЯХ?

- Мало публикаций.
- Отсутствие аватарки.
- Несоответствие имени профилю: странные имена типа набор букв, цифр или бессмысленных символов.
- Подозрительная активность: профиль подписан на большое число случайных сообществ или страниц, подписчики которого абсолютно разные тематики.
- Шаблонные комментарии.
- Минимальное взаимодействие: нет реакции на личные сообщения, отсутствие обсуждений с другими пользователями.
- Нереалистичные фото: в странных ракурсах, низкое качество, снимки знаменитостей, стоковые изображения.
- Круглосуточная активность.
- Использование коротких ссылок.
- Странная статистика: количество подписчиков значительно превышает количество опубликованных постов или лайков.

ПРОФИЛАКТИКА
федеральный центр

ЧТО ТАКОЕ КИБЕРБУЛЛИНГ И КАК С НИМ БОРОТЬСЯ?

Кибербуллинг – это форма травли, осуществляемая через интернет-ресурсы, соцсети, мессенджеры и другие средства коммуникации.

Цель – вызвать чувство унижения, страха, подавленности, изоляции жертвы путём угроз, распространения сплетен, оскорблений и преследования.

Признаки того, что ребёнок подвергается кибербуллингу.

- Избегает разговоров о своей онлайн-жизни.
- Часто испытывает плохое настроение после использования гаджетов.
- Теряет аппетит, плохо спит, проявляет апатию.
- Его популярность резко падает в кругу сверстников.
- Возникают трудности в учебе, ухудшается успеваемость.
- Постарался внезапно удалить свою страницу в соцсети или удалил старые посты.

ПРОФИЛАКТИКА
федеральный центр

РЕКОМЕНДАЦИИ РОДИТЕЛЯМ ПО БОРЬБЕ С КИБЕРБУЛЛИНГОМ

- Создайте атмосферу доверия между вами и вашим ребёнком, позволяющую свободно обсуждать любые темы, включая неприятные ситуации.
- Регулярно контролируйте цифровые устройства. Узнайте, какими приложениями пользуются ваши дети, периодически проверяя настройки конфиденциальности и безопасность аккаунтов.
- Настройка фильтров и блокировки. Помогите ребёнку настроить фильтры на нежелательную рекламу и спам, заблокировать подозрительных пользователей.
- Объясняйте детям особенности разных платформ и потенциальных опасностей каждой из них.
- Составьте договор с детьми относительно использования гаджетов, устанавливающий временные рамки и обязанности.
- Если ситуация выходит из-под контроля, обратитесь за консультацией к специалисту-психологу.
- Объясните ребёнку, что нельзя оставлять без внимания случаи оскорбления или издевательства над кем-либо в сети.
- Поддерживайте эмоциональное благополучие ребёнка. Чаще проводите время вместе, участвуйте в общих занятиях, обеспечивайте поддержку и понимание.

Сохраните психоэмоциональное здоровье вашего ребёнка и создайте благоприятную обстановку для его нормального роста и развития.