# Методические рекомендации для родителей по профилактике информационной безопасности и усилению контроля за нахождением обучающихся в интернет-пространстве в условиях дистанционного обучения в период самоизоляции

учитель будущего

Центр непрерывного повышения профессионального мастерства
педагогических работников – «Педагог 13.ру»

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ ПО ПРОФИЛАКТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УСИЛЕНИЮ КОНТРОЛЯ ЗА НАХОЖДЕНИЕМ ОБУЧАЮЩИХСЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ В УСЛОВИЯХ ДИСТАНЦИОННОГО ОБУЧЕНИЯ В ПЕРИОД САМОИЗОЛЯЦИИ

Саранск
2020

ББК 373.167.1:004
М54

**Рецензенты:**

Э. Н. Азоркина, секретарь Комиссии по делам несовершеннолетних и защите их прав Республики Мордовия

Ю. Г. Чиндяйкин, заведующий лабораторией проектной деятельности ГБУ ДПО РМ «ЦНППМ «Педагог 13.ру», кандидат исторических наук, доцент

М54 **Методические** рекомендации для родителей по профилактике информационной безопасности и усилению контроля за нахождением обучающихся в интернет-пространстве в условиях дистанционного обучения в период самоизоляции / сост.: О. Г. Литяйкина. – Саранск : ЦНППМ «Педагог 13.ру», 2020. – 12 с.

Методические рекомендации раскрывают способы контроля за поведением детей и подростков в интернет-пространстве в условиях дистанционного обучения, методы профилактики кибербуллинга и кибермошенничества.

Рекомендовано к печати редакционно-издательским советом
ГБУ ДПО РМ «ЦНППМ «Педагог 13.ру»

**ББК 373.167.1:004**

## ОТ СОСТАВИТЕЛЯ

Интернет-пространство в условиях дистанционного обучения детей и подростков в период самоизоляции имеет огромное образовательное значение. Обеспечение безопасности интернет-пространства во много зависит от компетентности и ответственности, в первую очередь, родителей (законных представителей) обучающихся. Родители (законные представители) наряду с педагогами являются участниками формирования безопасной виртуальной обучающей среды, способствующей реализации образовательных целей и задач, обеспечивающей доступность конструктивной коммуникации участников образовательного процесса.

## 1. ПЕРВООЧЕРЕДНЫЕ МЕРЫ ПО УСИЛЕНИЮ КОНТРОЛЯ ЗА НАХОЖДЕНИЕМ ДЕТЕЙ И ПОДРОСТКОВ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Поскольку современная информационная среда характеризуется не только достоинствами, но и факторами риска, родителям необходимо принять меры по усилению контроля нахождения детей и подростков в интернет-пространстве. В связи с этим родителям (законным представителям) обучающихся рекомендуется принять следующие меры:

1. Формировать у детей и подростков представление о безопасной интернет-среде. Важно, расположив ребенка к доверительному диалогу по вопросам интернет-безопасности, объяснить ему, что Интернет является не только надежным источником информации, но и источником опасности, рассказать о видах угроз и правилах соблюдения информационной безопасности.

2. Обсудить с ребенком регламент работы с компьютером и другими гаджетами, временные ограничения, определить интернет-ресурсы, которые можно и нужно посещать. Объяснить, что Интернет, в первую очередь, является средством развития и обучения и только потом средством развлечения и общения. Необходимо договориться с ребенком о том, что новые игры и программы будут устанавливаться совместно с родителями.

3. Учебные занятия и самоподготовка с использованием сети Интернет в условиях дистанционного обучения в период самоизоляции, независимо от возраста обучающихся, должны проводиться в присутствии одного из родителей (законных представителей). Доступ к данному информационному ресурсу должен быть эффективным и безопасным.

4. Необходимо исключить (блокировать) доступ детей к интернет-ресурсам, содержание которых противоречит законодательству Российской Федерации, может оказать негативное влияние на несовершеннолетних (информацию, пропагандирующую порнографию, культ насилия и жестокости, суицид, наркоманию, токсикоманию, антиобщественное поведение, сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.). С целью ограничения доступа детей к «вредным» материалам родители и

другие члены семьи могут установить на любом гаджете программу «Kaspersky Internet Security» с встроенным родительским контролем. С этой целью в настройках программы применить вкладку «Родительский контроль», при этом произойдет блокировка информации, связанной с порнографическими сюжетами, жестокостью, нецензурной лексикой и др., оказывающей негативное влияние на детей и подростков. Помимо опции «Родительский контроль» рекомендуется использовать дополнительные средства блокирования нежелательного контента, в частности контент-фильтрацию, обеспечиваемую следующими способами:

использование на персональном компьютере программного обеспечения, реализующего фильтрацию;

использование внешнего фильтрующего сервера, в том числе DNS-сервера и (или) прокси-сервера;

получение услуг фильтрации через оператора связи либо специализированную организацию, обеспечивающую доступ в Интернет для частных физических лиц.

5. О характере и объеме информации, полученной детьми в интернет-ресурсах, необходимо систематически узнавать в «Журнале обозревателя» программы «Internet Explorer».

## 2. ДОПОЛНИТЕЛЬНЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ С УЧЕТОМ ВОЗРАСТНЫХ ОСОБЕННОСТЕЙ

Помимо перечисленных выше общих мер усиления родителями контроля за деятельностью детей в интернет-пространстве, рекомендуются дополнительные меры обеспечения информационной безопасности детей, имеющие свою специфику с учетом возрастных особенностей.

**Родителям (законным представителям) обучающихся 7 – 9 лет необходимо:**

1. Создать совместно с ребенком список домашних правил пользования Интернетом и контролировать их выполнение.

2. Убедить ребенка, что родители (законные представители) наблюдают за ним потому, что беспокоятся о его безопасности и всегда готовы ему помочь.

3. Создать «белый» список интернет-сайтов, разрешенных для посещения детьми, применив для этого опцию«Родительский контроль».

4. Создать ребенку ограниченную учетную запись для работы на компьютере.

5. Использовать специальные детские поисковые «машины», типа MSN Kids Search.

6. Создать семейный электронный ящик в целях контроля переписки.

7. Блокировать с помощью соответствующего программного обеспечения доступ к сайтам с бесплатными почтовыми ящиками.

8. Использовать фильтры электронной почты для блокирования сообщений от конкретных людей или блокирования сообщений, содержащих определенные слова или фразы.

9. Приучить ребенка согласовывать с родителями (законными представителями) передачу какой-либо информации средствами электронной почты, чатов в мессенджерах, регистрационных форм и профилей.

10. Убедить ребенка никогда не соглашаться на личные встречи с незнакомыми лицами, от которых ребенок получил сетевое сообщение.

11. Приучить ребенка рассказывать обо всем, что вызывает у него неприятные чувства или дискомфорт при работе с интернет-ресурсами, сообщать родителям (законным представителям) о любых угрозах или тревогах, связанных с деятельностью в интернет-пространстве.

**Родителям (законным представителям) обучающихся 10 – 12 лет необходимо:**

1. Создать совместно с ребенком список домашних правил пользования Интернетом и контролировать их выполнение.

2. Убедить ребенка, что родители (законные представители) наблюдают за ним потому, что беспокоятся о его безопасности и всегда готовы ему помочь.

3. Создать ребенку ограниченную учетную запись для работы на компьютере.

4. Контролировать использование ребенком только сайтов из «белого» списка, созданного совместно с ним.

5. Обсудить с ребенком важность периодического предоставления доступа к его личной электронной почте; помочь защититься от спама; научить не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

6. Обговорить с ребенком важность согласования с родителями (законными представителями) передачу какой-либо информации (в том числе, личных данных) средствами электронной почты, чатов в мессенджерах, систем быстрого обмена сообщениями, регистрационных форм, личных профилей, регистрации на интернет-конкурсы, интернет-олимпиады и др.

7. Объяснить ребенку опасность самостоятельной загрузки программ или приложений, аргументируя тем, что они могут случайно загрузить вирусы или нелицензионное программное обеспечение, которое отрицательно скажется на работе устройства.

8. Завести личный аккаунт в той социальной сети, где имеет аккаунт ребенок, отправить запрос на подписку и войти в круг его сетевых «друзей» (или подписчиков). Систематически анализировать контакты ребенка, публикации, комментарии к ним. Беседовать с ребенком о его друзьях из интернет-пространства так же, как если бы речь шла о друзьях из реальной жизни. Убедить ребенка никогда не соглашаться на личные встречи с ними.

9. Контролировать переписку ребенка через социальные сети с помощью функции «Родительский контроль», что позволит сформировать списки контактов, переписка с которыми может быть разрешена или запрещена следующими способами:

а) задать ключевые слова, наличие которых будет проверяться в сообщениях;

б) указать личную информацию, пересылка которой будет запрещена.

10. Рассказать ребенку о таких угрозах интернет-пространства, как кибербуллинг, кибермошенничество.

11. Обсуждать с ребенком всё, что вызывает у него неприятные чувства или дискомфорт при работе с интернет-ресурсами, убедить его сообщать о любых угрозах или тревогах, связанных с деятельностью в интернет-пространстве.

12. Объяснить ребенку меру ответственности за использование сети для хулиганства, распространения непроверенной информации или угроз.

**Родителям обучающихся 13 – 17 лет необходимо:**

1. Создать совместно с подростком список домашних правил пользования Интернетом, договориться об их выполнении, контролируя ситуацию.

2. Составить список запрещенных сайтов («черный список»), часы работы в Интернете.

3. Использовать средства блокирования нежелательного контента как дополнение к стандартному «Родительскому контролю».

4. Знакомиться с сайтами, которые посещает подросток.

5. Знать, какими чатами пользуется подросток, ориентировать на использование модерируемых чатов.

6. Напомнить подростку риски работы с личной электронной почтой, способы защиты от спама, использование специальных почтовых фильтров.

7. Актуализировать важность согласования с родителями (законными представителями) передачу какой-либо информации (в том числе, личных данных) средствами электронной почты, чатов в мессенджерах, систем быстрого обмена сообщениями, регистрационных форм, личных профилей, регистрации на интернет-конкурсы, интернет-олимпиады и др.

8. Завести личный аккаунт в тех социальных сетях, где имеет аккаунты подросток, отправить запросы на подписку и войти в круг его сетевых «друзей» (или подписчиков). Систематически анализировать контакты подростка, публикации и комментарии к ним, фиксировать время его пребывания в сети. Беседовать с подростком о его друзьях из интернет-пространства так же, как если бы речь шла о друзьях из реальной жизни. Убедить подростка никогда не соглашаться на личные встречи с ними.

9. Контролировать переписку подростка через социальные сети с помощью функции «Родительский контроль», что позволит сформировать списки контактов, переписка с которыми может быть разрешена или запрещена.

10. Рассказать подростку о таких угрозах интернет-пространства, как кибербуллинг, кибермошенничество, порнография.

11. Объяснить подростку меру ответственности за использование сети для хулиганства, распространения непроверенной информации или угроз.

12. Обсудить с подростком проблемы сетевых азартных игр и их психические, психологические, социальные, материальные и правовые последствия.

Если на компьютере и мобильном устройстве подростка не установлен «Родительский контроль», следует обратить внимание на следующие тревожные факторы:

подросток не высыпается, даже если рано ложится спать; возможно, он не спит в ранние утренние часы;

рисует китов, бабочек, единорогов;

состоит в социальных сетях в группах, содержащих в названии следующее: «Киты плывут вверх», «Разбуди меня в 4.20», «f57», «f58», «Тихий дом», «Рина», «Ня пока», «Море китов», «50 дней до моего...», «Дом китов», «Млечный путь», «150 звёзд», «ff33», «d28», «Хочу в игру»;

закрыл ВКонтакте доступ к подробной информации в своем профиле, в переписке с друзьями (на личной стене) есть фразы «разбуди меня в 4.20», «я в игре», цифры, начиная от 50 и меньше;

переписывается в мессенджерах с незнакомыми людьми, которые дают странные распоряжения.

## 3. ЕСЛИ РЕБЕНОК СТАЛ ЖЕРТВОЙ ИНТЕРНЕТ-УГРОЗ

Чтобы своевременно заметить, что ребенок стал жертвой кибербуллинга (интернет-травли), родители должны **обратить внимание на следующие факторы:**

беспокойное поведение подростка (депрессия и нежелание идти в школу – явные признаки того, что ребенок подвергается агрессии);

неприязнь к Интернету (в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире);

нервозность при получении новых сообщений (негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя; ребенок регулярно получает сообщения, которые расстраивают его).

Кибермошенничество – один из рисков современного интернет-пространства, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.) с целью причинить материальный или иной ущерб.

**Рекомендации для родителей по предупреждению кибермошенничества:**

1. Проинформировать ребенка о самых распространенных методах мошенничества и научить его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете.

2. Установить на компьютер антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.

3. Прежде чем совершить покупку в интернет-магазине, удостовериться в его надежности. Если ребенок уже совершает онлайн-покупки самостоятельно, объяснить ему простые правила безопасности:

ознакомиться с отзывами покупателей;

проверить реквизиты и название юридического лица – владельца магазина;

уточнить, как долго существует интернет-магазин (по дате регистрации домена с помощью сервиса WhoIs);

выяснить, выдает ли магазин кассовый чек;

сравнить цены в разных интернет-магазинах;

позвоните в справочную службу магазина;

обратить внимание на правила интернет-магазина;

уточнить, какую сумму придется заплатить.

4. Обеспечить постоянный контроль расходов карманных денежных средств, переданных детям самими родителями, а также контроль и выяснение обстоятельств появления денежных средств, в суммах, превышающих «карманные» расходы.

**Если ребенок или подросток все-таки столкнулся с какими-либо угрозами интернет-пространства, родителям рекомендуется следующее:**

1. Установить положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Рассказать о своей обеспокоенности тем, что с ним происходит. Ребенок должен доверять родителям и понимать, что они хотят разобраться в ситуации и помочь ему, а не наказать.

2. Внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка.

3. Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он попал в неприятную ситуацию (потратил деньги в результате интернет-мошенничества и др.), необходимо его успокоить и вместе с ним разобраться в ситуации: что привело к данному результату, какие неверные действия совершил сам ребенок, а где допущена ошибка со стороны родителей.

4. Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать, были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.), жестко ограничить встречи с незнакомыми людьми, проверить все новые контакты ребенка за последнее время.

5. Собрать наиболее полную информацию о происшествии как со слов ребенка, так и с помощью социальных сетей (зайти на страницы сайтов, где был ребенок, изучить список его друзей, прочесть комментарии, сообщения). При необходимости, скопировать и сохранить эту информацию, например, для обращения в правоохранительные органы.

6. Если нет уверенности в серьезности произошедшего с ребенком, ребенок недостаточно откровенен, не готов идти на контакт или родители не знают, как поступить в той или иной ситуации, целесообразно обратиться к специалистам (телефон доверия, горячая линия, региональная служба поддержки семей, имеющих детей и др.), где будут даны рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций.

Для того чтобы интернет-пространство в условиях дистанционного обучения детей и подростков в период самоизоляции стало, действительно, мощным образовательным ресурсом и не принесло вреда обучающимся, современные родители, помимо выполнения функций контроля, должны быть сами носителями культуры поведения в IT-пространстве и формировать ее у детей и подростков в рамках систематического интернет-воспитания.

## Список источников


*Федеральные законы РФ*

1. Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации».
2. Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе».
3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
5. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».
6. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

*Указы Президента РФ*

1. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации».
2. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

*Постановления и распоряжения Правительства РФ*

1. Концепция информационной безопасности детей. Утверждена распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р.
2. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
3. Постановление Правительства РФ от 21 марта 2012 г. № 211«Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами,

операторами, являющимися государственными или муниципальными органами».

4. СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях».

*Приказы Минкомсвязи России*

1. Приказ Минкомсвязи России от 16.06.2014 № 161«Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию».

2. Приказ Минкомсвязи России от 07.06.2019 № 261«Об утверждении требований к подключению и доступу, включая требования к передаче данных, образовательных организаций, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий к единой сети передачи данных».

*Рекомендации*

1. Письмо Департамента государственной политики в сфере оценки качества общего образования Минпросвещения России № 04-474 от 07.06.2019 «О методических рекомендациях».

2. Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования. Разработаны в рамках реализации пункта 7 приказа № 88 Минкомсвязи России 27 февраля 2018 года «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018 – 2020 годы» Временной комиссией Совета Федерации по развитию информационного общества, Министерством просвещения России, Министерством цифрового развития, связи и массовых коммуникаций России и Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

*Научно-методическая литература*

1. Бабаш, А. В. Информационная безопасность. Лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. – М. : КноРус, 2016. – 136 с.

2. Гафнер, В. В. Информационная безопасность : учебное пособие / В. В. Гафнер. – Ростов-н/Д. : Феникс, 2017. – 324 с.

3. Громов, Ю. Ю. Информационная безопасность и защита информации : учебное пособие / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова. – Ст. Оскол : ТНТ, 2017. – 384 с.

4. Ефимова, Л. Л. Информационная безопасность детей. Российский и зарубежный опыт : монография / Л. Л. Ефимова, С. А. Кочерга. – М. : ЮНИТИ-ДАНА, 2016. – 239 с.

5. Ефимова, Л. Л. Информационная безопасность детей. Российский и зарубежный опыт : монография / Л. Л. Ефимова, С. А. Кочерга. – М. : ЮНИТИ, 2016. – 239 с.

6. Запечников, С. В. Информационная безопасность открытых систем. В 2-х т. Т. 1 – Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников, Н. Г Милославская. – М. : ГЛТ, 2017. – 536 с.

7. Запечников, С. В. Информационная безопасность открытых систем. В 2-х т. Т. 2 – Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. – М. : ГЛТ, 2018. – 558 с.

8. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации / А. А. Малюк. – М. : ГЛТ, 2016. – 280 с.

9. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. – М. : Форум, 2016. – 432 с.

10. Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, И. П. Слинькова, В. В. Гафнер. – М. : АРТА, 2016. – 296 с.

11. Семененко, В. А. Информационная безопасность : учебное пособие / В. А. Семененко. – М. : МГИУ, 2017. – 277 с.

12. Чипига, А. Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. – М. : Гелиос АРВ, 2017. – 336 с.

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ ПО ПРОФИЛАКТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УСИЛЕНИЮ КОНТРОЛЯ ЗА НАХОЖДЕНИЕМ ОБУЧАЮЩИХСЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ В УСЛОВИЯХ ДИСТАНЦИОННОГО ОБУЧЕНИЯ В ПЕРИОД САМОИЗОЛЯЦИИ

**Составитель:**
О. Г. Литяйкина, начальник управления реализации
образовательных программ для детей
ГБУ ДПО РМ «ЦНППМ «Педагог 13.ру»,
кандидат педагогических наук, доцент

Редакторы-корректоры
*Л. Ломакина, М. Живова*

Печать способом ризографии
Тираж 500 экз.
Цена договорная

Отпечатано с оригинала-макета
в ГБУ ДПО РМ «ЦНППМ «Педагог 13.ру»
430027, г. Саранск, ул. Транспортная, 19