Министерство образования и молодежной политики Свердловской области
Государственное автономное образовательное учреждение
дополнительного профессионального образования Свердловской области
«Институт развития образования»

Рекомендации для родителей в рамках проведения Единого урока безопасности в сети «Интернет»

Методические рекомендации

Екатеринбург
2019

ББК 74.200.5я81
Р 37

Авторы-составители:
О. А. Богословская, кандидат сельскохозяйственных наук, заведующий учебно-методическим кабинетом ГАОУ ДПО СО «ИРО»;
М. А. Герасимова, кандидат педагогических наук, заведующий кафедрой педагогики профессионального образования ГАОУ ДПО СО «ИРО»;
Н. Ю. Сероштанова, старший преподаватель кафедры прикладной информатики МБОУ ВО ЕАСИ (институт), г. Екатеринбург; руководитель проектов ООО «Р2Р Технологии».

Р 37 Рекомендации для родителей в рамках проведения Единого урока безопасности в сети «Интернет»: методические рекомендации / Министерство образования и молодежной политики Свердловской области, Государственное автономное образовательное учреждение дополнительного профессионального образования Свердловской области «Институт развития образования»; авт.-сост. О. А. Богословская, М. А. Герасимова, Н. Ю. Сероштанова. – Екатеринбург: ГАОУ ДПО СО «ИРО», 2019. – 47 с.

Данное издание включает рекомендации по проведению ежегодного Единого урока безопасности в информационно-телекоммуникационной сети Интернет, проводимого в рамках плана мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы. В издании использованы материалы ГАОУ ДПО СО «ИРО» по формированию информационно-безопасной среды в образовательных организациях, разработанные для педагогов Свердловской области и используемые в процессе реализации дополнительных профессиональных программ.

Методические рекомендации ориентированы на родителей (законных представителей) детей, педагогов образовательных организаций.

ББК 74.200.5я81

Содержание

Введение

Уважаемые родители!

Согласно российскому законодательству информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию [1].

Проблема информационной безопасности для школьников в интернете приобретает все большую актуальность для здоровья и интеллектуального, нравственного развития молодого поколения. Сегодня педагогическая общественность, все активнее используя средства информационных и коммуникационных технологий, ресурсы и услуги интернета, осознает, что глобальные сети наряду с уникальными возможностями, которые с их помощью открываются для системы образования, таят в себе и чрезвычайную опасность.

Важно понимать, что информационная безопасность детей – это забота не только школы, педагогов, но и родителей.

Ведь наши российские дети регулярно посещают сеть Интернет: и в то время, когда находятся в школе, и находясь дома. Зачастую это происходит без контроля и присмотра педагогов и родителей.

Проблемы, к которым это приводит, известны. Это:

– издевательство ровесниками и незнакомцами в сети над ребенком, травля (буллинг);

– воровством его аккаунтов, денег и личных данных;

– втягивание ребенка в асоциальную деятельность (группы смерти, группы с рекламой наркотиков и т.д.);

– прочтение детьми информации, вредящих их мировоззрению и психотическому состоянию.

Тревожен факт усиления угроз и рисков, связанных с поведением детей в сети Интернет. По данным исследования «Образ жизни российских подростков в сети» у 87% процентов детей возникали различные проблемы в сети «Интернет» только за последний год, и, к сожалению, только 17% детей рассказали о них своим родителям.

Причины этого различны:

– дети часто уверены в том, что родители не знают, как решить их проблемы;

– дети испытывают страх перед родителями;

– дети не имеют возможности рассказать и поделиться с родителями своими проблемами [2,3].

Родители и дети – два разных поколения, кардиально отличающиеся друг от друга.

Современные школьники – это дети XXI века. Согласно теории поколений, разработанной американскими учеными Нейлом Хоувом и Вильямом Штраусом в 1991 году, нынешние дети являются поколением Z. Они абсолютно уникальны, потому что на их развитие с самых ранних лет влияет такой мощный инструмент, как цифровая реальность [4]. Их рождение совпало с цифровой революцией и

появлением первого смартфона, они живут в совершенно другом мире, мире Интернета. Интернет – это новая среда обитания и источник развития ребенка. Конечно, такая ситуация влияет на формирование личности детей, на их взаимоотношения с окружающим миром.

Сегодняшние родители, выросшие в другое время, сами должны учиться существованию в сети Интернет, овладевать «цифровой компетентностью».

Цифровая компетентность – это не только сумма общепользовательских и профессиональных знаний и умений, но и ценностная установка на эффективную деятельность и личное отношение к ней, основанное на чувстве ответственности. Цифровая компетентность – это личностный компонент для каждого современного человека.

Иными словами, овладение цифровой компетентностью сегодня – это необходимость и для родителей, и для детей. Поэтому каждому родителю сегодня важно выстроить свое общение с ребенком именно как взаимодействие по совместному с ребенком овладению цифровой компетентностью.

Вместе с тем, выполняя родительские функции, родитель должен стать тем, кто напрямую будет обеспечивать информационную безопасность своего ребенка в сети Интернет [9].

При подготовке методических рекомендаций были использованы материалы ГАОУ ДПО СО «ИРО», разработанные для педагогов Свердловской области и используемые в процессе реализации дополнительных профессиональных программ (авт. Л. И. Долинер, Г. А. Бутакова, Е. В. Ахлестина, Т. А. Сундукова, Д. Е. Щипанова, Н.В. Шпарута, Н.Ю. Сероштанова,), а также материалы И.А. Волковой И.А. (МАОУ Лицей № 130, г. Екатеринбург).

Особенности поведения детей в сети Интернет (что нужно знать родителю о среде, в которой общаются их дети)

Возможности сети Интернет в большой мере позволяют оказывать мощное влияние на эмоциональную сферу подростка, поскольку Интернет является площадкой информационного обмена и общения.

Особенно это касается социальных сетей. Различные приемы предоставления информации, анонимность, правила участия в сети и другие особенности существования сетей являются инструментарием психологической поддержки участия человека (в нашем случае – ребенка, подростка) в виртуальном общении. Примером влияния на эмоциональную сферу человека является прием «вбрасывания» в сеть эмоционально окрашенных текстов.

Сеть как средство виртуального общения не имеет ни направленности, ни контекста разговора. В Сети как в любом контексте существования все задается людьми. Как любая площадка общения Интернет, площадка общения подростков, молодых людей отражает их особенности, потребности, интересы. Направленность может быть различной, в том числе и асоциальной. Подростки и молодые люди сами создают свой виртуальный социум, в котором действуют лишь ими же придуманные законы. Таковы особенности создания, развития социальных сетей и их влияния на процесс социализации подростков.

Несмотря на то, что в настоящее время в дружеских отношениях увеличивается доля общения, опосредованного современными техническими средствами (в виде электронной почты, интернет-сообщества, сотового телефона и т. п.), цели дружбы сохраняются прежними: эмоциональная поддержка, взаимопонимание, взаимная помощь. Поэтому общение в социальных сетях может оказывать и положительное воздействие на ребёнка. У детей в результате общения в сети накапливается психологический опыт, у ребенка получает развитие социальная компетентность. Немаловажно, что при этом реализуются такие важные потребности подростков как желание, с одной стороны, выделяться из толпы, оказаться замеченным и узнаваемым, а, с другой стороны, добавиться к общей группе, скрыться и раствориться в ней, поделив групповые ценности и став чувствовать себя защищённым, социализироваться.

Благодаря участию в общении в сети у детей появляются неограниченные возможности самопрезентации; возникает возможность экспериментирования со своей идентичностью и проигрывания различных ролей, что можно рассматривать в виде своеобразного психологического тренинга.

У детей, подростков появляются перспективы преодоления коммуникативного дефицита и расширения круга общения, увеличения информированности в обсуждаемых вопросах, обмен разными ситуативными эмоциональными состояниями и настроениями.

Активность подростков в социальных сетях реализуется в создании и оценке текстов, общении (обмен текстами), поиске друзей и новых знакомств, поиске информации, организации досуга: просмотр видеофильмов, фотогалерей, рекламных роликов и обмен мнениями.

Социальная сеть создает условия открытости и свободы осмысления социальных событий. Вместе с тем, как и любое техническое средство, сеть уже используется людьми в различных целях. Ее наполнение – индикатор развития общества. Она средство информационных войн, манипуляций людьми, социализации, самообразования, воспитания детей, подростков и молодежи, распространения опыта разных видов поведения.

Свобода – альтернатива запрету. Запрет в условиях доступа к информации, предоставленной Интернетом, мотивирует ее поиск, побуждает к конструированию неадекватного поведения и реализации его уже не в виртуальном мире, в жизни. Заимствуя в виртуальной среде такого рода опыт, подросток копирует его, а затем переносит на другие виды деятельности. Опыт поведения и деятельности сознателен и потому он может быть перенесен в реальность.

По данным проекта «ПроСММ» (2016) было установлено, что социальные сети занимают значительное место в жизни подростков, молодые люди практически все свободное и учебное время, проводят в социальных сетях. Выявлено, что основной целью посещения социальных сетей являются: просмотр видео, скачивание музыки и т. д., общение с друзьями и поиск новых знакомств. Оказалось, что подростки предпочитают виртуальное общение реальному.

Особенно тревожным оказался факт освоения подростками опыта троллинга. Троллинг – это написание на форумах, в комментариях к сообщениям и других местах неприватного общения пользователей Интернета провокационных сообщений, зачастую с оскорбительным содержанием, с целью вызвать конфликт. Человека, который постоянно занимается троллингом, называется троллем. Тролли осуществляют свою деятельность любыми доступными им способами: от примитивного размещения нарочито оскорбительных сообщений до плодотворной целенаправленной работы в команде себе подобных с целью внесения хаоса в группе тем выбранного сайта/форума в качестве жертвы.

Ребенок, увлекаясь новыми возможностями, которые предоставляет Интернет подчас не в силах контролировать негативный контент, который в той или иной степени «атакует» его аккаунт.

Отмеченное убеждает, что бесконтрольное пребывание подростков в виртуальном пространстве, не подвергнутое рефлексивному анализу, несет в себе значительные риски их социализации. Поэтому требуется техническая и ценностно-смысловая готовность подростков в применения Интернета и социальных сетей в жизнедеятельности и образовании [5].

Роль родителей в организации безопасного информационного пространства ребенка

Чтобы организовать безопасную среду для работы ребенка в Интернете, родителю необходимо: знать основные правила по использованию Интернета ребенком в зависимости от возраста, какое программное обеспечение нужно установить на компьютер и мобильные устройства, какие договоренности достичь с ребенком.

Из-за того, что дети и подростки более «продвинуты» в техническом плане, они легко могут обойти запреты родителей и устранить некоторые средства родительского контроля. Поэтому взрослым сначала необходимо освоить базовые навыки работы в Интернете, а затем научить правилам общения в Интернете и компьютерной безопасности своего ребёнка, сделать это в той форме, которая соответствует возрасту ребенка и кругу его интересов.

Ребенка нельзя оставлять наедине с компьютером, родителям необходимо организовать безопасное образовательное пространство в Интернете с помощью настройки программных средств, вместе с ребенком сформулировать правила и установить определенные договоренности. Системную работу по формированию осознанного отношения ребенка к безопасному использованию Интернета, должны вести и родители, и педагоги [3].

Вопросы информационной безопасности детей для родителей или законных представителей детей имеют свою специфику, отражающую необходимые им знания для обеспечения защиты детей в информационном пространстве с учетом специфики каждого возраста.

Общие советы для родителей:

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку – главный метод защиты.
2. Если ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
3. Проверьте, с какими другими сайтами связан социальный сервис вашего ребенка. Странички вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт или сайт, на котором друг упоминает номер сотового телефона вашего ребенка или ваш домашний адрес).
4. Стимулируйте ваших детей сообщать обо всем странном или отталкивающем.
5. Реагируйте, когда они этого не делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).

6. Будьте в курсе сетевой жизни вашего ребенка. Интересуйтесь, кто его друзья в Интернете так же, как интересуетесь реальными друзьями.

Советы родителям детей 7 – 8 лет

В Интернете ребенок 7-8 лет старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т.е. родительский контроль или то, что вы сможете увидеть во временных файлах. В результате у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7 – 8 лет могут быть следующими:

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
4. Используйте специальные детские поисковые машины.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.
6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
8. Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
9. Научите детей не загружать файлы, программы или музыку без вашего согласия.
10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
11. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
13. Не делайте «табу» из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».

14. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Советы родителям детей 9 – 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств родительского контроля. Желательно придерживаться следующих правил:

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от вашего ребенка соблюдения норм нахождения за компьютером.
3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.
4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.
6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.
7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
8. Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
10. Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
11. Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.
12. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.
13. Расскажите детям о порнографии в Интернете.
14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Советы родителям детей 13 – 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете. Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей. Советы по безопасности в этом возрасте от 13 до 17 лет:

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).
2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.
3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.
5. Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
8. Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
9. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

11. Приучите себя знакомиться с сайтами, которые посещают подростки.

12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

13. Объясните детям, что ни в коем случае нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

15. Постоянно контролируйте использование Интернета вашим ребенком. Это не нарушение его личного пространства, а мера предосторожности и проявление вашей родительской ответственности и заботы.

Интернет дает возможность анонимного общения. К сожалению, часто это выливается в чувство безнаказанности и вседозволенности. Подростки с обусловленной возрастом нестабильной психикой и индивидуальными психологическими проблемами (неуверенность, страхи) подвержены развитию вседозволенности, распущенности в Интернете, которая позже переходит в реальную жизнь. Кроме того, в Интернете очень просто приукрасить свою жизнь, соответственно, можно нарваться на мошенников.

Как определить, что вас пытаются обмануть или ввести в заблуждение:

– Сопоставляйте ответы на ваши вопросы. Если у вас возникли сомнения в правдивости, повторите свой вопрос через какое-то время. Вопросы могут касаться места учебы, работы и т. д. Любопытно, что вруны действительно не помнят, что они говорили ранее, они заговариваются.
– Предложите встретиться. Если ваш собеседник под разными предлогами отказывается от очной встречи, это должно насторожить. Если ваш собеседник все же решил встретиться, то назначайте ее в людном месте.
– Излишняя навязчивость собеседника может говорить о подозрительных намерениях. В любом случае, если у вас возникает хоть какое-то подозрение, что перед вами мошенник, необходимо прекратить «общение» [6].

Рекомендации родителям по применению технологических средств обеспечения информационной безопасности

Блокировка «нежелательных собеседников» на персональном компьютере в социальных сетях

Facebook

web.facebook.com

1. Зайдите в свой аккаунт[1].
2. Социальная сеть ФБ позволяет настроить конфиденциальность вашего профиля. Для этого необходимо выбрать в личном кабинете меню «Настройки».
3. В разделе «Настройки» можно задать параметры безопасности под личный профиль (рис. 1).

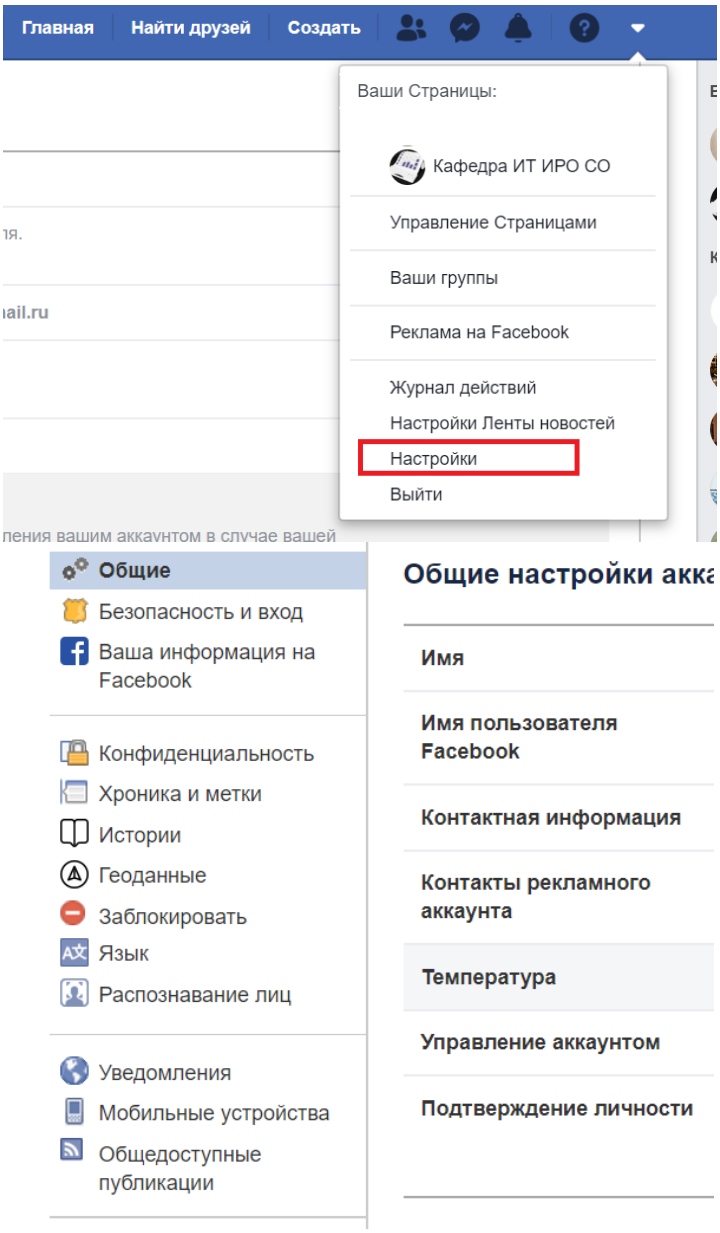

Рис. 1. Параметры безопасности раздела «Настройки» Facebook

[1] Учетная запись (аккаунт) – хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам

Параметры, которые можно настроить:

Предупреждение о входе – Facebook сохраняет список компьютеров, гаджетов[2] и браузеров[3], которыми вы обычно пользуетесь при входе в соцсеть. Если соцсеть зарегистрирует вход с незнакомого устройства или браузера, вам придет оповещение на электронную почту.

Подтверждение входа, или двухфакторная аутентификация[4]. При входе в соцсеть приходит SMS-сообщение с коротким кодом, который нужно ввести вместе с паролем. Также можно получить список из 10 «запасных» одноразовых кодов на тот случай, если необходимо входить при таких обстоятельствах, когда SMS невозможно получить, например, украли смартфон.

Генератор кода – эта функция позволяет вместо SMS использовать коды, которые генерирует мобильное приложение Facebook, или привязать проверку безопасности к другому, стороннему приложению.

Открытый ключ – это публичный ключ, который будет отображаться в информации вашего аккаунта. Зачем это нужно: с помощью публичного ключа ваши друзья могут отправлять вам письма в зашифрованном виде, так что, даже если это письмо попадет не в те руки, злоумышленники не смогут его прочитать. Заводится два ключа – публичный и секретный. Публичный используется для шифрования, его знают все. А вот для расшифровки нужен секретный ключ, который есть только у вас. Это называется «асимметричное шифрование»: шифруем одним ключом, расшифровываем другим.

Признанные устройства – это список доверенных браузеров и приложений на различных устройствах, которыми вы постоянно пользуетесь для входа в Facebook.

Откуда вы вошли – очень удобная функция, которая позволяет посмотреть, на каких устройствах сейчас зашли в Facebook (рис. 2). Это поможет, если вы заходили в соцсеть с компьютера другого человека и забыли выйти. Если вы увидите в списке подключений подозрительную сессию[5], которая не имеет к вам никакого отношения, можно ее закрыть и, если нужно, поменять пароль.

---

[2] Гаджет – (англ. gadget – штуковина, приспособление, устройство, безделушка) – небольшое устройство, предназначенное для облегчения и усовершенствования жизни человека (здесь и далее определение взяты с сайта «Википедии» – ru.wikipedia.org)

[3] Бра́узер, или веб-обозреватель (от англ. web browser – просмотрщик) – прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов

[4] Метод контроля доступа к компьютеру, в котором пользователю для получения доступа к информации необходимо предъявить более одного «доказательства»

[5] Промежуток работы на компьютере

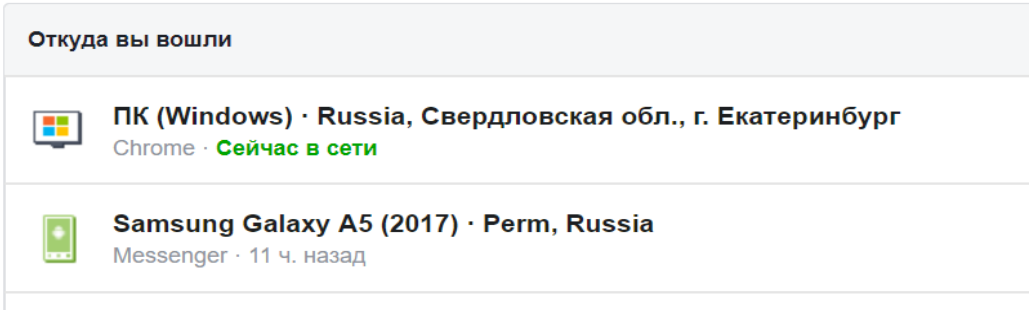

Рис. 2 Функция «Откуда вы вошли»

Деактивировать аккаунт – можно деактивировать учетную запись. Записи перестанут быть видны, но вы всегда можете вернуться.

VK

vk.com

1. Зайдите в свой аккаунт.
2. Социальная сеть «ВКонтакте» настроена так, что вы можете задать параметры настройки и таким образом принимать или отклонять предложения «дружить». Также можно задать параметры конфиденциальности таким образом, что ваш профиль будет закрытым.
3. Настройте параметры безопасности, выбрав меню «Настройки» (рис. 3).

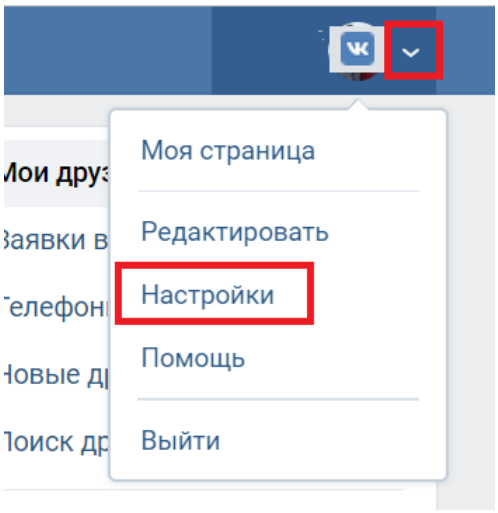

Рис. 3 Настройка параметров безопасности социальной сети «ВКонтакте»

4. Выберите меню «Приватность». В этом разделе можно настроить различные параметры безопасности, в т. ч. выбрать тип профиля (открытый/закрытый, кто видит фотографии, кто может подписываться на обновления и т. д.).

Недавно в соцсети «ВКонтакте» добавили запрет поиска профиля по номеру телефона.

Instagram

instagram.com

1. Если ваш аккаунт открытый, то любой пользователь может подписаться на обновления вашей страницы. Если на вас подписался «нежелательный собеседник», то необходимо зайти в свой аккаунт.

2. Зайдите в личный кабинет (нажмите ), выберите список подписчиков (рис. 4,5).

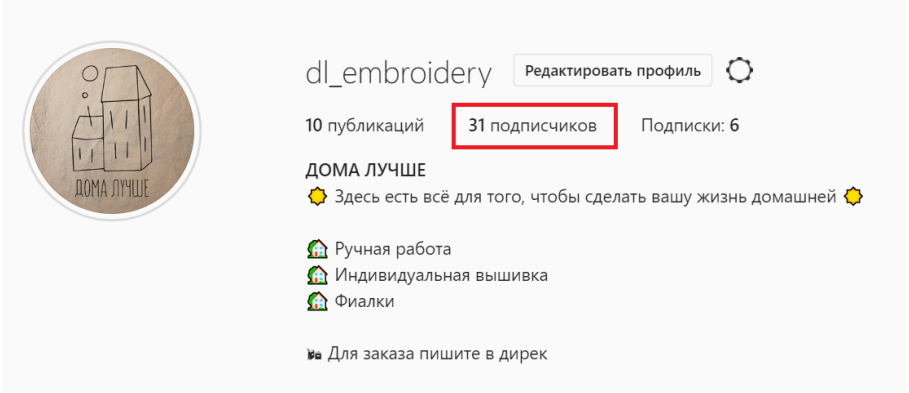

Рис. 4 Настройки списка подписчиков instagram.com

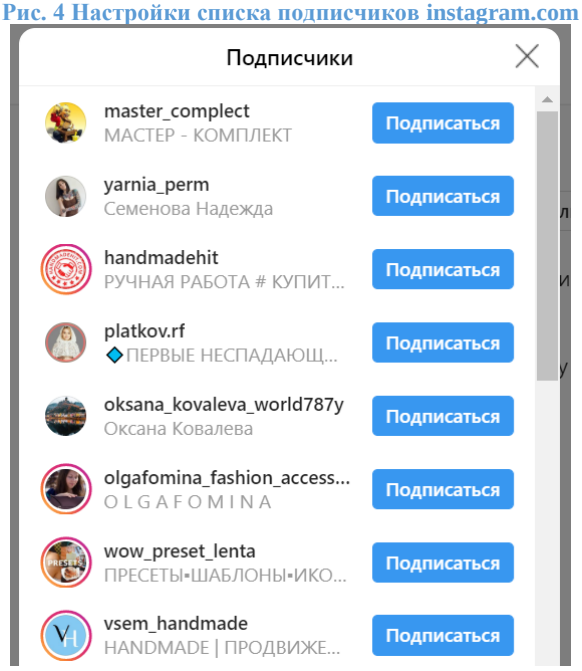

Рис. 5 Настройки списка подписчиков instagram.com

3. Выберите того пользователя, которого вы желаете заблокировать. Нажмите меню справа от пользователя (рис. 6).

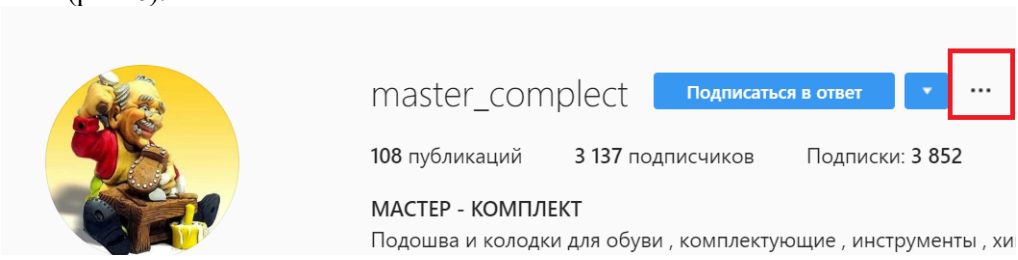

Рис. 6 Настройки списка подписчиков instagram.com

4. В открывшемся окне выберите необходимый вариант – заблокировать или пожаловаться на пользователя. Настройки безопасности аккаунта можно также сделать при редактировании профиля (рис. 7).

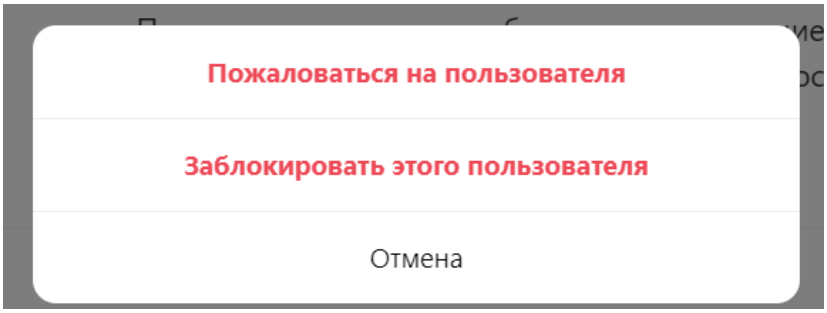

Рис. 7 Настройки списка подписчиков instagram.com

Для обеспечения безопасности в Instagram может использоваться двухфакторная аутентификация. Необходимо ввести специальный код для входа или подтверждать вход при каждой попытке получить доступ к Instagram с неопознанного устройства. Это может быть SMS с кодами с мобильного телефона, коды для входа из стороннего приложения (подробнее об использовании кодов аутентификации можно прочитать на сайте поддержки: help.instagram.com/1372599552763476).

Одноклассники

ok.ru

Блокировка нежелательных сообщений и рекламных рассылок

1. Переходите в раздел сообщений.

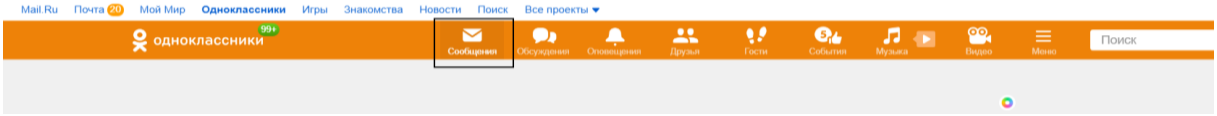

Рис. 8

2. Нажимаете на фото отправителя.

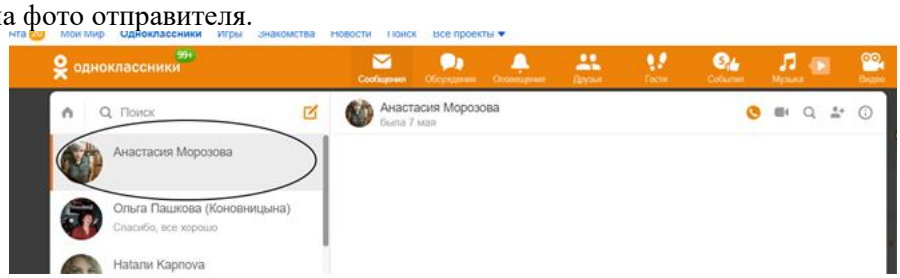

Рис. 9

3. Справа вверху нажимаете на «Настройки».

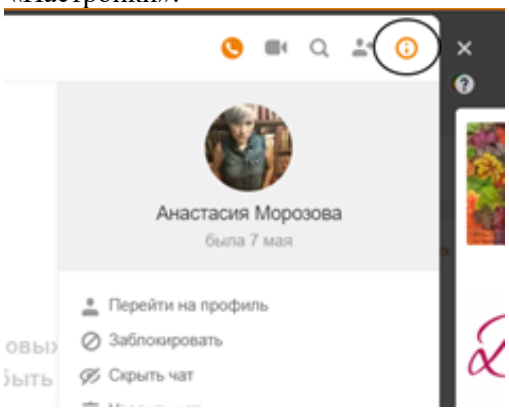

Рис. 10

4. Выбираете «Заблокировать».

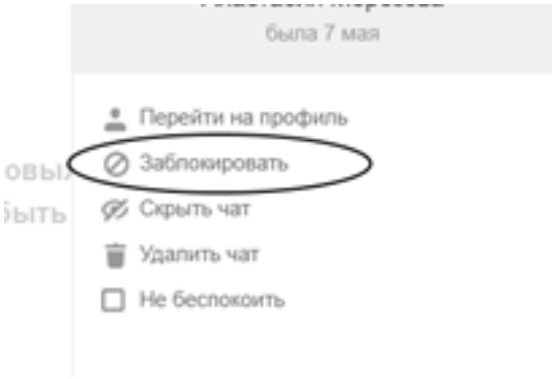

Рис. 11

5. Подтверждаете свое действие.

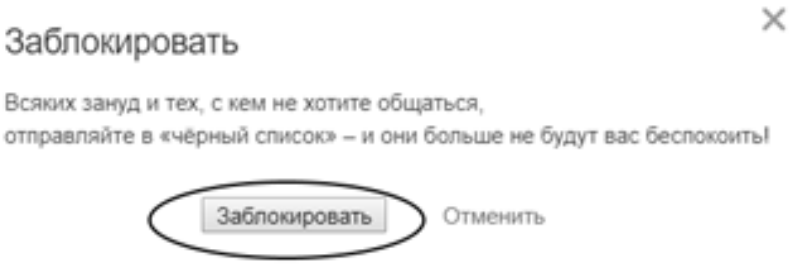

Рис. 12

Блокировка гостей (отключение возможности заходить на вашу страницу определенным пользователям)

1. Переходите в раздел «Гости».

Рис. 1

2. Наводите мышку на человека, которого не хотите видеть в гостях.
3. Во всплывающем окошке нажимаете «Заблокировать».

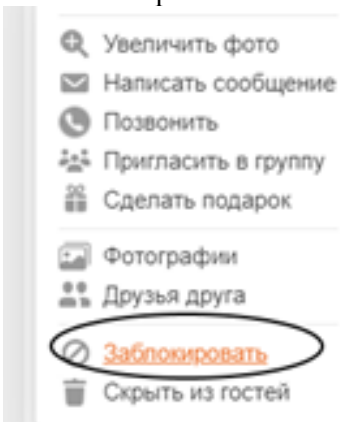

Рис. 2

4. Подтверждаете свое действие.

Как заблокировать друга в одноклассниках

1. Переходим в раздел «Друзья».

Рис. 3

2. Нажимаем на фото друга, которого хотим удалить (заблокировать).
3. Выбираем в открывшемся меню «Прекратить дружбу».

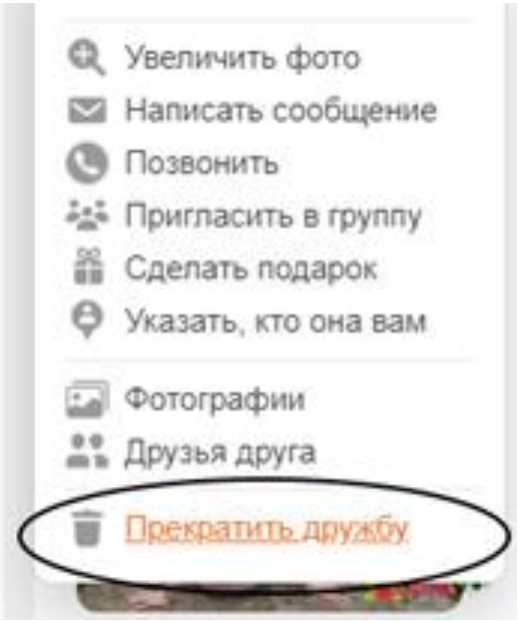

Рис. 4

4. Подтверждаете свое действие.

Обеспечение информационной безопасности на персональных компьютерах

Антивирусная защита

Антивирусная программа – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления зараженных (модифицированных) такими программами файлов и профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом[6].

В задачи антивирусного ПО входит обнаружение шпионских программ, вирусов, фишинговых[7] ресурсов, опасных серверов и подозрительного трафика.

[6] ru.wikipedia.org

[7] Фи́шинг (англ. phishing от fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов

Лучшие бесплатные антивирусы по версии журнала PC-magazine[8]

представлены на рисунке.

Рис. 5

Антивирус Kaspersky

Kaspersky Free (kaspersky.ru) – бесплатный антивирус Касперского с облачными технологиями Kaspersky Security Network, включающий несколько компонентов.

Файловый антивирус

Файловый антивирус Kaspersky Free Anti-Virus позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на вашем компьютере и на всех присоединенных дисках.

Почтовый антивирус

Почтовый антивирус проверяет входящие и исходящие почтовые сообщения на вашем компьютере. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов.

Веб-антивирус

Веб-антивирус перехватывает и блокирует выполнение скриптов[9], расположенных на веб-сайтах, если эти скрипты представляют угрозу безопасности компьютера. Веб-антивирус в Kaspersky Free Anti-Virus также контролирует весь веб-трафик и блокирует доступ к опасным веб-сайтам.

IM-антивирус

[8] comss.ru/page.php?id=5683

[9] Скрипт – это программа для Интернета. Ищет «слабые» места операционной системы и «заставляет» ее выполнять несвойственные ей действия

IM-антивирус обеспечивает безопасность работы с IM-клиентами[10], такими как WhatsApp, Viber, Facebook Messenger, Skype, ICQ, Google Hangouts.

Алгоритм установки антивируса:

1. Зайдите на сайт [kaspersky.ru.](kaspersky.ru)
2. Выберите в меню продукт для скачивания.

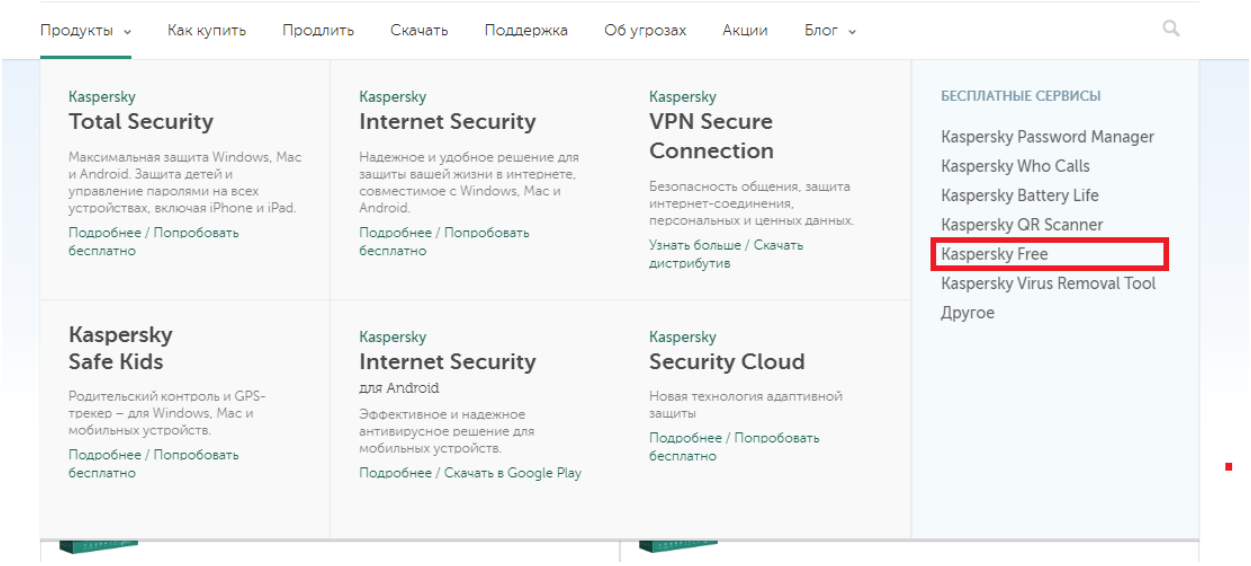

Рис. 6

3. Нажмите кнопку «Скачать».

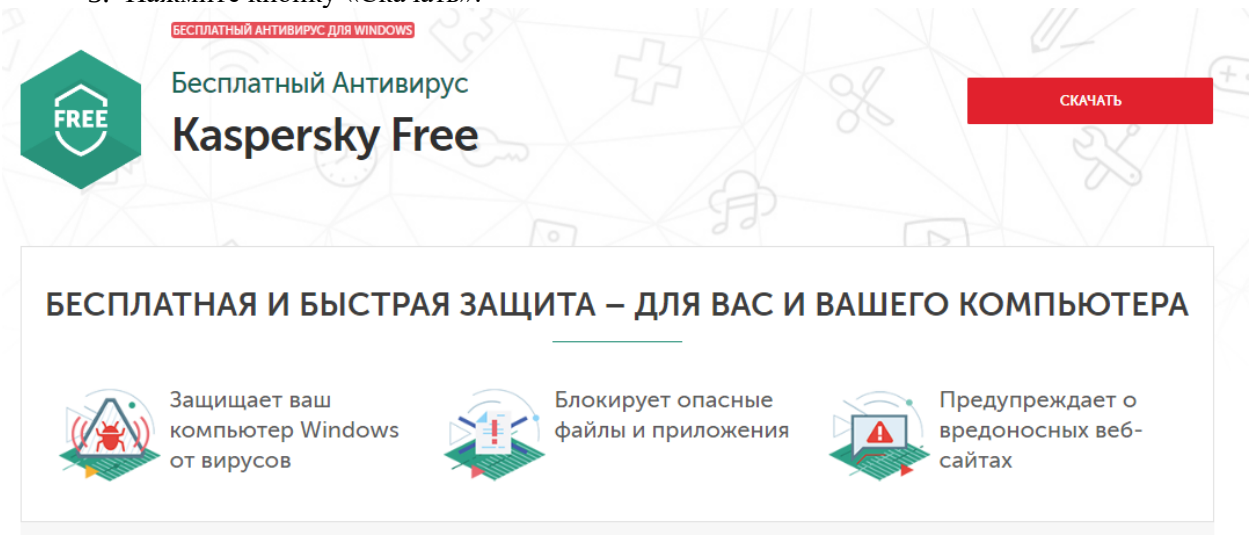

Рис. 7

4. После скачивания необходимо запустить файл. Для установки следуйте инструкциям.

Kaspersky Safe Kids

Kaspersky Safe Kids включает в себя приложения для ребенка и родителя, которые взаимодействуют через сервис My Kaspersky[11]. Приложение на устройстве ребенка помогает контролировать его онлайн-активность, позволяет родителям просматривать отчеты и менять настройки.

[10] IM – (англ. Instant Messaging, IM) – система мгновенного обмена сообщениями: службы мгновенных сообщений (Instant Messaging Service, IMS), программы – онлайн-консультанты

[11] my.kaspersky.com/

Решение Kaspersky Safe Kids успешно прошло сертификацию австрийской независимой организации AV-Comparatives и стало лучшим среди решений для детской онлайн-безопасности.

Для этого решения существует бесплатная версия, которая позволяет защитить детей от поиска неподходящих сайтов и информации, регулировать использование программ на компьютере и мобильных устройствах, ограничивать время, когда можно использовать устройство[12].

Платная версия позволяет определять местоположение ребенка, контролировать активность в соцсетях, а также получать уведомление в случае, если ребенок попытался зайти на запрещенный сайт, вышел за пределы безопасного периметра. Инструкция по установке расположена по адресу

Рис. 8

kaspersky.ru/safe-kids.

Защитник Windows

В Windows 10 появился раздел «Безопасность Windows» (ранее Центр безопасности Защитника Windows), который упрощает управление добавленными пользователем средствами защиты, а также позволяет больше узнать о функциях безопасности, доступных в Windows 10 по умолчанию.

Основные компоненты раздела «Безопасность Windows»

Защита от вирусов и угроз – здесь отражается, какой антивирус используется для защиты. Это может быть Защитник Windows или любой сторонний антивирус. В этом разделе можно настроить сканирование.

Защита учетных записей – позволяет управлять безопасностью учетной записи и входа в нее. Можно настроить ввод PIN-кода или биометрической авторизации (распознавание лица, распознавание отпечатка пальца), графический пароль для более быстрого и безопасного входа в систему. Также доступна функция «Динамическая блокировка» – операционная система блокируется, если покинуть заданный периметр.

[12] Веб-контроль доступен только через браузер Kaspersky Safe Kids, а функционал контроля программ недоступен

Брандмауэр и безопасность сети – данный раздел предоставляет информацию о конфигурации брандмауэра[13] Windows и содержит ссылки для устранения проблем с сетевым подключением.

Безопасность устройства – предлагает общий статус безопасности: «обработчик безопасности» – дополнительное шифрование; «безопасная загрузка» – позволяет предупредить загрузку вредоносных программ во время запуска.

Параметры для семьи – раздел «Родительский контроль», который позволяет настроить время нахождения в сети, блокировать неподходящий контент, сообщение в случае, если дети хотят что-то купить в Microsoft Store (при создании учетной записи Microsoft).

Avast Free Antivirus 2019

Рис. 9

Основные функции антивируса Avast Free Antivirus

Комплексный антивирус содержит функцию интеллектуального сканирования, обнаружения уязвимостей, которые бы могли позволить вредоносному ПО проникнуть в систему.

Режим «Не беспокоить» – блокировка уведомлений во время игры, просмотра видео и проведения презентаций в полноэкранном режиме.

Веб-защита и защита от фишинга – защита от вредоносных сайтов, мошенников и предотвращение перехода на поддельные сайты без установки специального расширения для браузера.

Защита почты – предупреждает попадание зараженных писем в почтовый ящик на компьютере, а также не допускает отправки зараженных писем с учетной записи.

Анализ сети – автоматическое обнаружение слабых мест домашней сети Wi-Fi для защиты ее от злоумышленников.

Обновление программ – установка обновлений для другого программного обеспечения, которые избавят его от уязвимостей и улучшат производительность.

Менеджер паролей – защита всех учетных записей одним надежным паролем.

Очистка браузера – удаление из браузера ненужных панелей инструментов, надстроек и других расширений.

Диск аварийного восстановления – резервная копия для критических случаев.

Для установки программы на компьютер воспользуйтесь инструкцией, которая размещена на avast.ru

[13] Брандмауэр – в информатике программный и/или аппаратный барьер между двумя сетями, позволяющий устанавливать только разрешенные межсетевые соединения

Adblock Plus

Adblock Plus – блокировщик рекламы в браузерах, содержит защиту от слежения, блокировку опасных доменов, отключение кнопок социальных сетей.

Приложение блокирует надоедливые баннеры, объявления с вредной для психики информацией и всплывающую рекламу. А еще защищает конфиденциальность информации, позволяет сэкономить интернет-трафик и увеличить время работы телефона на 20 %. Для установки необходимо пройти по адресу adblockplus.org/ru/.

Сложные пароли

Сложность паролей напрямую определяет их надежность, поэтому рекомендуется использовать длинные случайные комбинации символов. Во-первых, их почти невозможно взломать перебором. Во-вторых, они не имеют привязки к личности пользователя.

Пароли в виде имени супруга или ребенка, даты рождения, клички собаки, названия любимой команды непосредственно связаны с вами. Это та информация, которую злоумышленники смогут подобрать, если получат доступ к социальной сети, почте или компьютеру.

Поэтому 17041991 – это плохой пароль. Masha17041991 или 1704masha1991 – тоже. А Vy0@$e6#Omx6 – сильный ☺ пароль. Его невозможно собрать исходя из данных о человеке, а найти перебором сложно технически.

Не используйте одинаковые пароли. В идеале для каждого случая должна быть своя комбинация. Применять для всех почтовых аккаунтов, соцсетей и банковских сервисов один и тот же код – опасно.

Все запомнить будет трудно. Поэтому установите для хранения менеджер паролей:

- KeePass Password Safe (keepass.ru/)
- LastPass Free (lastpass.com/ru)
- RoboForm (roboform.com/ru)
- Protect (yandex.ru/company/technologies/protect дополнение Яндекс.Браузера) – больше чем менеджер паролей, позволяет блокировать мошеннические сайты, защита в общественной сети.

Информационная безопасность при работе с почтой

Будьте аккуратны с файлами, приложенными к письмам в электронной почте. Никогда не открывайте и не запускайте их, если источник неизвестен. В противном случае убедитесь, что он действительно прислал вам важный документ. Не забудьте также проверить файл антивирусом – вдруг отправитель распространяет угрозы, но не подозревает об этом.

Правила работы с почтой:

1. По возможности надо иметь не менее 2 почтовых адресов – для рабочих и личных контактов.

2. Закрывайте окна веб-браузера после окончания работы, особенно если вы находитесь в библиотеках, интернет-кафе и т. п.
3. Не сохраняйте пароли в браузере и очищайте кеш браузера[14], историю посещенных сайтов, cookies[15] (это можно сделать, зайдя в настройки браузера и очистив историю).
4. Не открывайте письма с названием темы типа «наследство», «выигрыш в лотерею» («африканские» письма) и т. п.
5. Не отправляйте финансовую и частную информацию по электронной почте.
6. Не аннулируйте «подписку» на рассылки, на которые вы не подписывались: запросы на подтверждение подписки часто используют спамеры.
7. Не отключайте спам-фильтр. Пользуйтесь антивирусами с включенной возможностью сканирования вложений e-mail.

Своевременное обновление ПО

Преступники совершенствуют свои инструменты, а разработчики со «светлой» стороны – укрепляют оборону. Оба соперника изучают методы друг друга и стараются своевременно реагировать на изменения. Новые варианты взлома и слежки попадают в Сеть ежедневно, поэтому для снижения рисков до минимума надо регулярно обновлять программное обеспечение. К нему относится и антивирус, и операционная система, и браузер.

Безопасность среды

Угроза может проникнуть на компьютер не только напрямую из Сети или файла, полученного на почту. Источником способна послужить локальная сеть на работе, зараженное устройство одного из членов семьи, уязвимая точка Wi-Fi в общественном месте.

Старайтесь проверять степень защищенности всех устройств и сетей, к которым подключаетесь. А в общественных местах лучше вообще не использовать открытые сети для онлайн-оплаты или авторизации в веб-сервисах.

Общие правила пользования Интернетом

1. Проверьте настройки конфиденциальности в социальных сетях.
2. Не используйте общедоступные хранилища для личных данных. Случайно выдать лишнюю информацию можно не только через социальные сети. Например, не стоит хранить конфиденциальные данные в онлайн-службах, предназначенных для обмена информацией. Например, «Google Документы» не лучшее место для файла с паролями, а сканы паспорта не надо выкладывать на Dropbox.
3. Не сообщайте свою основную электронную почту и номер телефона всем подряд.

---

[14] Кэш, или кеш – промежуточный буфер памяти, с быстрым доступом к нему, содержащий информацию, которая может быть запрошена с наибольшей вероятностью (т. е. наиболее часто посещаемые сайты)

[15] Cookies (англ., буквально – печенье) – небольшой фрагмент данных, отправленный сервером и хранимый на компьютере пользователя.

4. Используйте мессенджеры со сквозным шифрованием (end-to-end), например WhatsApp. Обратите внимание, что Telegram, Facebook Messenger и Google Allo не используют сквозное шифрование по умолчанию. Чтобы включить его, необходимо вручную начать секретный чат.
5. Используйте надежные пароли.
6. Просматривайте разрешения мобильных приложений и расширений браузеров.
7. Защитите ваш телефон и компьютер паролями или кодами доступа.
8. Отключите уведомления на экране блокировки.
9. Соблюдайте осторожность в общедоступных сетях Wi-Fi.

Информационная безопасность на мобильных устройствах

Мобильные устройства – неотъемлемая часть нашей жизни. Основные черты этого сегмента: повсеместная распространенность и быстрый количественный рост. Они стремительно становятся основным способом нашего взаимодействия с окружающим миром: возможность постоянно оставаться на связи является неотъемлемой частью нашей сегодняшней жизни, телефоны и всевозможные носимые устройства расширяют наши возможности при покупке продуктов, получении банковских услуг, развлечениях, обучении, видеозаписи и фотографировании важных моментов нашей жизни и, разумеется, возможности общения.

Одновременно благодаря им и приложениям бренды получили принципиально новый способ заявить о себе, и это в свою очередь привело к феноменальным уровням роста мобильных технологий за последнее десятилетие. К сожалению, быстрый рост проникновения мобильных технологий приводит и к расширению возможностей для киберпреступников.

Сегодня через мобильные устройства пользователям доступно все больше весьма ценных сервисов, требующих внимательного отношения к безопасности (в числе которых, например, мобильный банкинг, платежи и мобильные идентификаторы). Хакеры прекрасно понимают, что, организовав утечку данных аутентификации через мобильное устройство, они смогут получить доступ к онлайн-ресурсам, представляющим собой высокую ценность. Злоумышленников привлекает, с одной стороны, прямая связь устройства с реальными деньгами (мобильный банкинг, счет мобильного), которые несложно обналичить, а с другой – различная информация, которая может принести не меньший доход.

Но как понять, какие меры безопасности следует принимать в том или ином случае?

Типичные угрозы и уязвимости мобильных устройств, выявленные «Лабораторией Касперского»:

1. Доступ к почте и почтовому ящику

Доступ к почтовым сервисам и синхронизация почты настраиваются на мобильном устройстве один раз, и в случае потери или хищения аппарата злоумышленники получают доступ ко всей переписке, а также ко всем сервисам, привязанным к данному почтовому ящику.

2. Интернет-пейджеры

Skype, ICQ, Jabber, WhatsApp, Viber и т. п. – все это не чуждо современным мобильным устройствам, в результате чего и вся переписка данного конкретного человека, и его контакт-листы могут быть под угрозой.

3. Документы, заметки

Dropbox, облачные хранилища для мобильных устройств вполне могут стать источником компрометации каких-либо документов, равно как и различные заметки и события в календаре. Емкость современных устройств достаточно велика, чтобы они могли заменить USB-накопители, а документы и файлы с них вполне способны порадовать злоумышленников. Нередко в смартфонах встречается использование заметок как универсального справочника паролей, также распространены хранящие пароли приложения, защищенные мастер-ключом.

4. Адресная книга

Иногда сведения об определенных людях стоят очень дорого.

5. Сетевые средства

Использование смартфона или планшета для удаленного доступа к рабочему месту посредством VNC, TeamViewer и прочих средств удаленного администрирования уже не редкость.

6. Мобильный банкинг

Основными путями компрометации информации с мобильных устройств являются их пропажа или хищение. Сообщения о громадных финансовых потерях из-за пропажи ноутбуков, смартфонов, планшетов службы банков получают регулярно.

Рис. 10

Средства защиты мобильных операционных систем (ОС)

Современные ОС для мобильных устройств имеют неплохой набор встроенных средств защиты, однако зачастую те или иные функции не используются или отключаются.

Современные мобильные ОС обладают неплохими средствами защиты – как встроенными, так и представленными на рынке. Основными проблемами являются несвоевременность или невозможность получения обновлений, обход защиты самим пользователем, отсутствие политики информационной безопасности (ИБ) для мобильных устройств. Рассмотрим, какие шаги необходимо предпринять для защиты устройств и что учесть при создании политики ИБ.

1. Блокировка устройства

Представьте, что ваш смартфон попал в руки к постороннему человеку. Для большинства пользователей это означает, что некто получит доступ сразу ко всему. Необходимо блокировать устройство паролем (стойким или с ограниченным количеством попыток ввода), после которых данные на устройстве затираются или устройство блокируется.

2. Использование криптографических средств

Необходимо использовать шифрование съемных носителей, карт памяти – всего, к чему может получить доступ злоумышленник.

3. Запрет на сохранение паролей в браузере мобильного устройства

Нельзя сохранять пароли в менеджерах паролей браузеров, даже мобильных. Желательно установить ограничение на доступ к переписке почтовой и SMS, использовать шифрование.

4. Запрет на установку ПО из непроверенных источников, осуществление «взломов» ОС

Желательно использовать ПО от крупных, известных разработчиков.

«Безопасный поиск» в Google включается через меню «Настройки поиска». В «Яндексе» в тех же настройках есть пункт «Фильтрация страниц». Ищите там «Семейный поиск» и помечайте его галочкой.

Если вам не хочется, чтобы ребенок скачивал в телефон все что угодно, заведите ему отдельный Google-аккаунт с ограниченными правами, а свой профиль сделайте основным.

На устройствах Apple родительский контроль можно использовать для блокирования или ограничения определенных программ и функций. Выберите «Настройки» > «Основные» > «Ограничения» и нажмите включить.

Также можно включить для вашего ребенка функцию «Попросить купить», тогда вы сможете утвердить или отклонить загрузку любого приложения, как платного, так и бесплатного.

5. Использование средств антивирусной и прочей защиты

Если это возможно, позволит избежать множества угроз (в том числе новых), а в случае потери или кражи устройства осуществить его блокировку и уничтожение данных на нем.

6. Ограничить список данных, которые можно передавать облачным сервисам

Современные мобильные устройства и приложения ориентированы на использование множества облачных сервисов. Необходимо следить, чтобы конфиденциальные данные и данные, относящиеся к коммерческой тайне, не были случайно синхронизированы или отправлены в один из таких сервисов.

Ответственность за безопасность детей в Интернете лежит на родителях. Во-первых, надо знать все возможные риски, рассказать о них детям и, как следствие, принять меры предосторожности вместе с ними: разработать политику безопасного поведения в Сети и подобрать мобильные приложения для достижения максимальной безопасности.

Что же предлагают провайдеры и компании для ответственных родителей (табл. 1, 2)?

Таблица 1

Контроль местоположения ребенка

Приложение	Функционал	Достоинства	Недостатки	Цена
«Где мои дети» – локатор для телефона и GPS-часов	Программа следит за местоположением ребенка. Если он не слышит ваш звонок, можно отправить ему на устройство громкий сигнал. Установить приложение «Где мои дети» тайно не получится, поэтому его использование возможно лишь по обоюдному согласию родителей и ребенка	Можно ввести данные нескольких детей и контролировать их местоположение. В приложение встроен семейный чат. Позволяет контролировать заряд батареи телефона ребенка и медленно тратит батарею телефона родителя. Сохраняет историю передвижений ребенка. Можно установить «зоны безопасности», приложение оповестит вас, когда ребенок покидает их. Если на смартфоне ребенка отключился GPS или сбились настройки приложения, оно пришлет родителю оповещение. Если у вашего ребенка Android, то вам будут доступны еще несколько интересных функций: запись разговоров ребенка по мобильному и запись звуков вокруг него, а также еженедельный отчет о времени в том или ином приложении на смартфоне		Приложение бесплатное со встроенными покупками. В течение первых двух недель работает весь функционал. По окончании пробного периода остается только определение местоположения ребенка. Годовая подписка стоит 1490 рублей, на месяц – 169 рублей. **Поддерживаемые платформы:** iOS, Android
Kaspersky Safe Kids	Программа также показывает местоположение ребенка на карте. Особенность ее в том, что она позволяет отслеживать его активность в Интернете и ограничивать время пребывания в Сети и доступ к определенным сайтам	Показывает местоположение ребенка и уведомляет, если он покидает установленные вами безопасные зоны. Можно смотреть, сколько времени ребенок провел в Facebook и «ВКонтакте», и получить отчет о его активности. Позволяет получить консультацию психолога об активности ребенка в Сети	Ограниченный функционал в мобильных версиях по сравнению с версией для компьютера	Есть бесплатная версия. Премиум-версия с расширенным числом функций стоит 900 рублей в год. **Поддерживаемые платформы**: Windows, MAC, iOS, Android

Приложение	Функционал	Достоинства	Недостатки	Цена
Life 360	Это приложение можно отнести к семейным локаторам. Оно позволяет создать группу и включить в нее всех членов семьи	Можно установить определенные зоны: «дом», «школа» и т. д. – и получать уведомление, когда кто-то из членов семьи окажется вблизи них. Показывает на карте ближайшие пункты полиции, пожарные части, больницы. Содержит функцию «паники». Уведомление о том, что вы попали в беду, с указанием ваших GPS-координат, придет на смартфоны и почту ваших родных	Нет адаптированной версии на русском языке. Служба поддержки отвечает не на все претензии пользователей и общается только на английском	**Б**есплатно 30 дней. Есть подписка на месяц (до 150 рублей) и на год (до 4700 рублей). **Поддерживаемые платформы**: Android, iOS
Family Locator	Еще одна программа, которую можно использовать для отслеживания перемещений всех членов семьи. В сравнении с другими приложениями оно очень просто в использовании, но часть функций, которые есть у других программ, отсутствует	Содержит встроенный чат для общения. Можно отправлять родным и близким сообщения SOS и просьбы о помощи. Уведомляет, если члены семьи прибыли в обозначенную вами зону или приблизились к опасному месту, которое вы заранее обозначили. Можно создавать журнал перемещений за неделю	Нельзя отслеживать работу ребенка в Интернете. Нет функции записи разговоров ребенка по телефону	**Пр**иложение имеет бесплатную и платную версии: 94,8–149 рублей в месяц и 990–1490 рублей в год. **Поддерживаемые платформы**: Android, iOS

Таблица 2

Контроль ребенка в Интернете

Приложение	Функционал	Достоинства	Недостатки	Цена
ESET NOD32 Parental Control	Эта программа поможет родителям малышей и школьников младшего и среднего возраста контролировать их использование смартфона и планшета. Это приложение более универсально в сравнении с другими, которые мы включили в обзор,	Может обращаться к ребенку по имени и давать ему советы по работе с устройством, напоминать о домашних делах или уроках. Позволяет установить периоды времени, когда можно включать устройство, и подстроить его, например, под школьное расписание. Блокирует посещение сайтов по 20 категориям. Позволяет создавать собственные списки. Можно следить за работой ребенка в Сети и получать отчеты за день, неделю или месяц.		Бесплатное, имеет платный контент стоимостью от 99 до 999 рублей в зависимости от содержания. **Поддерживаемые платформы**: Android

Приложение	Функционал	Достоинства	Недостатки	Цена
	и просто в использовании. Кроме того, оно может работать с гаджетами – умными браслетами и часами	Ребенок может отправлять родителю запрос на посещение сайта, которое заблокировано в приложении. Показывает на карте положение ребенка, когда устройство у него		
Kids Place	Еще одно приложение для контроля ребенка в Интернете и играх. Также позволяет ограничивать время доступа к устройству и нежелательным сайтам, блокировать случайные звонки, покупки и т. д.	Блокирует поступление сигналов на телефон, когда на нем работает Kids Place, – это предотвращает излучение от устройства	Нет настройки работы приложения по времени. Нет статистики по посещению сайтов ребенком	Бесплатное, со встроенными покупками стоимостью от 15 до 790 рублей за товар. **Поддерживаемые платформы**: Android
Блокировка от детей Child Lock	Предназначение этого приложения очень просто: оно ограничивает доступ ребенка к смартфону	Разрешает доступ только к выбранным вами приложениям. Выйти из него можно только после введения пароля. Блокирует регулировку клавиш громкости, подключения к Wi-Fi, выхода в меню, включения камеры и других основных функций смартфона	Последнее обновление приложения было два года назад, программа может работать нестабильно – зависать или вылетать	Бесплатное. Есть встроенные покупки от 15 до 45 рублей за товар. **Поддерживаемые платформы**: Android

Предложения от мобильных операторов

Мегафон

Родительский контроль: следите, где находится ваш ребенок, управляйте настройками его телефона и доступом к сайтам.

Следите за балансом: проверяйте в любой момент, сколько денег на телефоне ребенка, и получайте уведомления о приближении его баланса к нулю.

Управляйте звуком: включайте или отключайте звук на телефоне ребенка удаленно.

Следите за зарядом батареи: смотрите, какой заряд батареи на телефоне ребенка.

Управляйте доступом к Интернету: ограничивайте доступ к опасным сайтам или отключайте Интернет на устройстве.

Смотрите, где ребенок, на карте:

- Размечайте зоны и получайте уведомления при пересечении этих зон.
- Следите за перемещениями ребенка в течение дня.

Ограничивайте доступ к опасным сайтам: оградите ребенка от информации в Интернете, которая предназначена для взрослой аудитории, содержит ненормативную лексику или другой опасный контент.

МТС

Услуга «Родительский контроль» позволяет ограничивать доступ к веб-страницам, содержащим:

- информацию для взрослых;
- азартные игры;
- нецензурную лексику;
- экстремистские, пропагандирующие насилие или наркотики материалы.

Всего предусмотрена блокировка свыше 80 категорий опасного контента. Услуга действует по принципу «черного списка» и запрещает прямой доступ более чем к 60 миллионам веб-сайтов на 23 языках, включая русский. База данных «черного списка» обновляется ежедневно, за год пополняясь 10–15 миллионами новых веб-адресов.

Дополнительно услуга позволяет:

- осуществлять анализ трафика и блокировку данных по содержимому (например, картинок для взрослых);
- принудительно устанавливать режим безопасного поиска в поддерживающих эту функцию поисковых системах (например, Яндекс и Google).

«Черный список» для детей: звонки и SMS, входящие и исходящие – помогите своему ребенку сформировать безопасный круг общения.

Билайн

Мобильное приложение для защиты детей

Позаботьтесь о защите ваших детей – пусть они открывают только подходящие по возрасту сайты и приложения, учатся грамотно распределять время между играми и учебой и не пропадают из вашего поля зрения. Будьте спокойны за ваших детей и безопасность семьи.

Дети активно используют планшеты и смартфоны для общения со сверстниками, учебы, поиска информации и игр, не подозревая об опасностях, которые могут подстерегать их в Интернете.

Именно поэтому «Билайн» рекомендует всем своим мобильным абонентам установить на смартфоны и планшеты «Родительский контроль».

«Родительский контроль» для абонентов «Билайн» поможет родителям ограничить доступ детского устройства к нежелательным сайтам и приложениям, настроить время для игр и учебы, удаленно контролировать смартфон или планшет ребенка, а также отправить тактичное сообщение в случае необходимости.

Веб-контроль

Компонент «Веб-контроль» позволяет детям исследовать Интернет, не подвергая себя опасности. Укажите возраст ребенка, чтобы приложение «Родительский контроль» для абонентов «Билайн» автоматически указало, какие категории доступны. Родители могут изменять эти параметры и разрешать или блокировать доступ к любой приведенной категории.

Если ребенок заходит на запрещенную веб-страницу, он может попросить разрешения получить доступ к содержимому.

Контроль приложений

С помощью компонента «Контроль приложений» родители могут контролировать, какие приложения использует ребенок и как долго он может это делать. Список приложений можно загрузить с мобильного устройства, которым пользуется ребенок. Вы можете выбрать пять готовых возрастных групп, для которых уже настроено, какое содержимое блокируется, а какое разрешено.

Временные ограничения для приложений, входящих в категорию «Игры», можно задать с помощью компонента «Контроль приложений». Разные временные ограничения можно задать для учебных и неучебных дней. Ограничения могут относиться также к определенным часам каждого дня.

У региональных мобильных операторов (Мотив, Теле2) отдельно выделенных тарифов нет, но в некоторых можно найти и подключить платные услуги, аналогичные по функциям, описанным выше. Список очень ограничен, и вопрос детской безопасности они решают просветительскими публикациями и рекомендациями по установке соответствующих мобильных приложений.

Идеальных решений нет, но любые неприятности всегда легче предотвращать, чем потом с ними разбираться [7].

Профилактика интернет-зависимости у детей и подростков

Интернет-зависимость - навязчивое желание войти в Интернет, находясь офлайн и неспособность выйти из Интернета, будучи онлайн (Гриффит В., 1996).

Фактически интернет-зависимость – это расстройство психики, заключающееся в неспособности человека вовремя выйти из сети, а также в постоянном присутствии желания в нее зайти.

По своим проявлениям она схожа с уже известными формами аддиктивного поведения, например, в результате употребления алкоголя или наркотиков, но относится к типу нехимических зависимостей, то есть не приводящих непосредственно к разрушению организма.

Главной группой риска в этом виде зависимости являются люди, испытывающие проблемы или дефицит реального общения. Отсутствие коммуникативных навыков погружает их в виртуальный мир, заменяющий им круг реальных друзей.

Интернет-зависимым такой стиль жизни легче, поскольку позволяет забыть о проблемах в реальной жизни или разногласиях с друзьями или близкими, что приводит к конфликтам с последними, таким образом поддерживая зависимость.

Зависимость от интернета возникает по ряду причин и может проявляться в различных формах.

Интернет-зависимость опасна по различным причинам, которые приводят к:

1. Снижению концентрации внимания;
2. Ухудшению памяти;
3. Мыслительным и психическим расстройствам;
4. Обострению физических заболеваний;
5. Потере времени для жизни.

Известны многие виды Интернет-зависимости:

1. информационная зависимость (стремление постоянно путешествовать по Интернету в бесцельных поисках информации);
2. игровая зависимость, когда пользователь «подсаживается» и не может оторваться от онлайн игр, тратя реальные деньги;
3. зависимость от интернет-общения;
4. зависимость от азартных игр в интернете. Во многом схожа с обычным пристрастием к игре на деньги. Здесь в качестве главной опасности выступают интернет-казино и другие сайты азартных игр, которые действуют по аналогии с настоящими;
5. стремление к поиску информации агрессивного или непристойного содержания;
6. постоянное стремление к просмотру или скачиванию фильмов и музыки;
7. стремление к совершению вредных действий (целенаправленное нарушение правил сетевого этикета, распространение ненужной или вредной информации и т.п.).
8. хакерство;

9. навязчивое желание тратить деньги и осуществлять ненужные покупки, в частности непроизвольная тяга к покупкам вещей на интернет-аукционах и в онлайн-магазинах;

10. пристрастие к виртуальному общению и виртуальным знакомствам (большие объемы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети);

11. бесконечное скачивание с торрент-трекеров и других источников нелицензионного контента и материалов в целях создания собственной базы и т.д.

Интернет-зависимые как большинство психически нездоровых людей не осознают тяжести своего состояния и с раздражением и агрессией относятся к попыткам отвлечь их от источника зависимости, но это происходит, когда болезнь зашла уже слишком далеко. До этого еще можно и самостоятельно обнаружить у себя признаки формирующейся зависимости и, если хватит силы воли, вовремя остановиться.

Для этого состояния характерны следующие признаки:

1. потеря ощущения времени при использовании устройства
2. эйфория при использовании устройства
3. досада и раздражение при невозможности выйти в Интернет, в частности отвращение ко всем остальным видам деятельности
4. друзья и знакомые перестают общаться, но это не расстраивает
5. интересует только то, что связано с предметом увлечения – играми, социальными сетями и т.п.
6. невозможность остановиться при использовании устройства
7. использование устройства тайно или тайком от посторонних

Интернет-зависимые считают, что:

1. следует потратить все деньги на покупку новых игр, на увеличение мощности компьютера и улучшение или приобретение подобных функций;
2. лучшие друзья – те, которых они встретили в виртуальной среде.

Зачастую Интернет-зависимые врут о своей зависимости, например, говоря, что занимались чем-то другим, а не проводили время в интернете.

Однако с любой проблемой можно справиться, если осознавать в этом необходимость. Для того чтобы не попасть в компьютерную зависимость, помогут следующие действия:

1. Для входа в Интернет должна быть обоснованная цель пребывания в интернете. Можно планировать, какие сайты посетить, что там сделать и посмотреть, сколько времени на это выделить. Если работа с устройством в учебных целях, необходимо следить за тем, чтобы не отвлекаться на ненужные ресурсы.

2. Необходимо уменьшать количество времени, которое пользователь проводит в интернете, чтобы в конечном итоге свести его к минимуму. Возможно установление временных интервалов для работы и отдыха в интернете, а смартфон можно ограничить графиком проверки сообщения, например, один раз в полчаса, а ночью выключать его.

3. Если появилось свободное время, то лучше быть на воздухе, двигаться и заниматься спортом, а также лично общаться с друзьями и знакомыми.

4. Необходимо урегулировать режим сна и питания, исключив практику питания за компьютером [6].

Дети и подростки с признаками интернет-зависимости существенно отличаются от сверстников без зависимости как по характеру, так и по способности к общению, самооценке.

Принимая во внимание особенности подростков с интернет-аддикцией, психологи советуют родителям придерживаться некоторых правил:

1. Отношения в семье следует строить на принципах честности и умении признавать ошибки.

2. Нельзя оскорблять ребенка и его круг общения.

3. Следует быть другом и помощником своему ребенку. Позиция «Я – старший, поэтому делай так, как тебе говорят» никогда не приведет к доверительным отношениям.

4. Следует сделать так, чтобы ребенок мог довериться родителям всегда и при любых обстоятельствах.

5. Не стоит бояться показывать свои чувства ребенку, если родители расстроены сложившейся «компьютерной» ситуацией. Тогда он увидит в родителе не противника, а близкого человека, который тоже нуждается в заботе.

6. Если вдруг возник конфликт, который выражен в приказном тоне со стороны родителей о прекращении работы за компьютером, то не следует «торговаться» с ребенком: «Сначала сделаешь что-то (уроки, выполнишь домашние обязанности), только потом можешь поиграть».

Если использовать эти несложные советы хотя бы частично, то со временем ребенок поймет, что родители желают ему только хорошего и являются его друзьями. Многие дети уверены в том, что родители создают им проблемы специально. Такие дети постепенно начинают думать о себе плохо, в результате низкой самооценки они могут стать проблемными детьми, с которыми сложно строить общение.

Следующие рекомендации помогут родителям предотвратить возникновение компьютерной и интернет-зависимости.

1. Всегда нужно оговаривать время игры ребенка на компьютере и точно соблюдать эти рамки. Количество времени следует выбирать исходя из возрастных особенностей ребенка. Например, до 5 лет не рекомендуется допускать до компьютера: не стоит мешать ребенку познавать мир постепенно и без вмешательства искусственного интеллекта. Начиная с 5 лет ребенку можно позволить знакомиться с компьютером, но не более 2 часов в день и не подряд, а по 15–20 мин. с перерывами. При этом надо объяснить, что реальная жизнь и герои компьютерных игр – две разные вещи, не совместимые между собой. С 7 лет ребенок может самостоятельно отличить виртуальный образ игры от реального. После 12 лет наступает наименее тревожный период, так как ребенок может различать образы различных реальностей. Но это всего лишь усредненные данные, всегда нужно исходить из конкретных личностных и индивидуальных особенностей детей в том или ином возрасте.

2. Нужно больше общаться с ребенком, развивать в нем гармоничную эмоциональную сферу, посещать с ним различные мероприятия.

3. Категорически запрещается играть в компьютерные игры перед сном.

4. Необходимо привить ребенку интерес к активным играм и физическим упражнениям. Пусть он двигается и испытывает радость от этого. Ведь когда ребенок сидит за компьютером, все его физические нагрузки заключаются лишь в движении мышкой по столу.

5. Необходимо следить, чтобы игра на компьютере не подменяла реальное общение со сверстниками и друзьями.

6. Следует проводить обсуждение игр вместе с ребенком, выбирать развивающие игры.

7. Нужно показывать ребенку личный положительный пример.

Важно не критиковать ребенка, проводящего слишком много времени за компьютером. Это может только усугубить проблему и отдалить его от друзей и близких. Критика воспринимается подростком как отказ понять его интересы и потому вызывает замкнутость, агрессию.

Следует поощрять ребенка за общение со сверстниками в клубах, кружках, в которых подросток может проявить себя, развить свои таланты и способности.

Стоит чаще проводить классные часы, вместе гулять, посещать выставки, концерты, выезжать на природу.

В качестве краткого итога следует отметить, что тяга к компьютерным играм и интернету чревата возникновением сильной зависимости, которая отражается на здоровье и поведении ребенка. Он становится эмоционально неуравновешенным, напряженным, агрессивным, испытывает чувство тревоги, выглядит подавленным и озабоченным, перестает уделять должное внимание спорту и различным физическим нагрузкам, портит свое зрение, так как постоянно находится перед экраном, у него нарушается сон, он не может сосредоточиться ни на каком виде деятельности, иногда «забрасывает» учебу, теряет друзей и знакомых, и как следствие – возникает субъективное ощущение одиночества.

Таким образом, и родителям и педагогам важно своевременно распознать проблему и принять соответствующие меры для ее решения.

Организация среды социализации современных обучающихся и развитие детско-родительских отношений

Наиболее активными пользователями интернета являются подростки. Подростковый возраст характеризуется изменением социальной ситуации развития: потребностью перехода к потенциально самостоятельной и ответственной взрослости, открытие и утверждение своего «Я», поиск собственного места в системе человеческих взаимоотношений. Происходит смена ведущей деятельности, что проявляется в ориентации на общение со сверстниками, принятие группой сверстников.

Познание подростком себя как правило осуществляется через противопоставление миру взрослых, возникает «чувство взрослости», желание доказать и получить подтверждение своей «взрослости».

Поведение обучающихся в сети интернет направлено на удовлетворение этих потребностей, также, как и поведение в реальном жизненном пространстве. Поэтому для профилактики интернет-рисков большую значимость имеют управление социализаций подростка.

Задача педагогов и родителей: проанализировать возможности сетевого взаимодействия и социального партнерства школы в организации среды социализации школьников и определить возможности организации дополнительного образования и досуговой деятельности обучающихся.

Основа профилактики интернет-рисков – работа педагога совместно с родителями по включению школьника в реальные социальные группы, развитие благоприятных межличностных отношений, сплочению класса. Этому аспекту в настоящее время в школах уделяется недостаточно внимания, что приводит к формированию дисфункциональных групп и межличностных отношений в среде обучающихся.

Современные подростки активно используют интернет для общения. Стремление подростков снизить эмоциональную зависимость от родителей, недостаточный уровень развития родительской компетентности в формировании благоприятных детско-родительских отношений.

В настоящее время достаточно актуальным направление является развитие родительских университетов на базе школ или в сетевом взаимодействии.

На всероссийском уровне для создания родительского университета на базе школы интересны разработки Высшей школы экономики https://ioe.hse.ru/parentsuniversity/rodituniver .

При создании программы работы с родителями важно предусмотреть планирование тем как для целевых групп родителей (решение конкретной проблемы), так и для широкой аудитории для обсуждения широкого круга вопросов развития и воспитания ребенка.

Спектр обсуждаемых проблем должен быть весьма широк, но, в тоже время, достаточно конкретен, связан с реальным опытом участников. Работа по программам, направленным на решение проблем воспитания, преодоление кризисов и пр. целесообразно ориентировать на участников, имеющих собственный родительский опыт.

Планирование различных методов работы повысит эффективность программы. В зависимости от цели и задач конкретного элемента программы, целесообразно использовать беседу, упражнение, опрос, лекцию, демонстрацию фильма и пр. С организационной точки зрения, смена видов деятельности способствует активизации участников, преодолению утомления, поддержке активного внимания. Кроме того, применение различных по модальности методов и технологий (использование фото, видео- и аудиоматериала, интерактивных технологий и пр.) позволяют вовлечь слушателей в разной степени склонных использовать аудиальный, визуальный или кинестетический каналы восприятия[16].

Использование различных методов и практико-ориентированных видов деятельности (деловых и ролевых игр; тренингов, работа с литературой и Интернет-ресурсами, работы с глоссарием по изучаемой тематике; написанием рефлексивных работ) должно соответствовать особенностям динамики работы группы, оно позволит вовремя сконцентрировать внимание, простимулирует дискуссию, даст возможность разрядить эмоциональное напряжение, снять физическую усталость и т.д. При планировании длительности программы необходимо учитывать степень сложности предстоящей работы. Создавая программу для семей в тяжелых жизненных ситуациях, нужно учитывать, что более эффективными для них являются продолжительные встречи, а также использование дополнительных поддерживающих сессий с различными консультантами. Повторные встречи применяются для решения сложных проблем при работе с группами риска. Зачастую целесообразно дополнять групповую работу индивидуальными занятиями, особенно в случаях, когда родитель не готов обсуждать свою проблему публично.

На всероссийском уровне, согласно исследованиям ВШЭ определены наиболее актуальные темы для родительского университета.

Темы, освещающие проблематику ухода за ребенком, сбережения его физического здоровья. Родители хотят быть более компетентными в вопросах профилактики болезней, знать нормативы физического и психического развития, уметь оказывать первую медицинскую помощь. Им необходимы навыки поиска квалифицированных специалистов в области медицины, логопедии, дефектологии. Следующей по уровню востребованности темой является гармонизация семейных и более широких социальных отношений. Так, родителей волнует, как выстроить взаимоотношения с прародителями (бабушками и дедушками), как следует организовывать общение ребенка со вторым родителем в ситуации развода и т.п. Родителей интересует социальное благополучие ребенка в школе, а именно - его контакты со сверстниками. Большое внимание родители готовы уделить формированию конкретных воспитательных компетенций. Здесь важнейшими темами выступают выработка средств воздействия на ребенка, способов борьбы с ленью, мотивация к учебе. Важной темой также является доступ к системе образования. Родители нуждаются в знаниях и навыках, которые помогут выбрать подходящий детский сад, школу, кружок или секцию;

[16] Методические рекомендации по формированию содержания программ Родительского университета. Режим доступа: https://ioe.hse.ru/data/2016/09/06/1120268643/Методические%20рекомендации.pdf

подготовить к детскому саду и школе; оказать помощь в учебе, повысить успеваемость ребенка, вовлечь его в дополнительные занятия; прикрепить ребенка к образовательным организациям разных ступеней. Разрабатывая содержание программ для работы с родителями необходимо также уделять внимание проблемам, на которых акцентируют внимание педагоги и психологи. Существует дефицит верифицированных надежных знаний в области возрастной и педагогической психологии, педагогики, базовых представлений о физиологии ребенка, способах ухода за ним, обеспечения основных потребностей и разрешения воспитательных задач. Многим родителям трудно отслеживать изменения в законодательстве, далеко не все имеют представления о своих правах и обязанностях, а также о правах своего ребенка. Зачастую весьма ограничены представления о функционировании системы образования и здравоохранения, не хватает знаний о существующих возможностях и способах воспользоваться государственной поддержкой семьи с ребенком. Помимо дефицита знаний, современные родители зачастую испытывают трудности с решением конкретных проблем и отягощены внутренними конфликтами. В связи с этим, востребованными темами могут стать формирование способности самостоятельно выстраивать стратегию воспитания, повышение сензитивности к потребностям, переживаниям и реакциям ребенка. Психолого-педагогическая практика показывает, что необходимо освещать такие темы как образ родителя в общественном мнении и индивидуальных представлениях, гиперболизация и интеллектуализация роли родителя в воспитании ребенка, раскрытие потенциала индивидуальной и реалистичного родительской стратегии; образ ребенка, возможности развития самостоятельности, ответственности и инициативности на разных этапах онтогенеза, совместное эмоциональное пространство ребенка и родителя, право на личное пространство взрослого и способы его организации, индивидуальное воспитательное творчество как основа гармоничного родительства, приносящего удовольствие[17].

Для эффективной организации работы родительского университета необходимо строго следовать принципам этики. Соблюдение этих принципов позволит создать ситуацию безопасного взаимодействия.

Принцип конфиденциальности полученной в ходе работы информации о семьях участников. Материалы не могут быть разглашены или обсуждаться за пределами рабочей ситуации.

Принцип беспристрастности по отношению к участникам. Недопустимо предвзятое отношение к участникам программы, независимо от социального статуса, материального положения, личных предпочтений педагога и пр.

Принцип ограничения профессиональной компетентности специалиста. Он обязан рефлексивно относиться к границам собственных знаний и умений, и обращаться к помощи коллег или смежных специалистов в случаях, когда это необходимо.

[17] Методические рекомендации по формированию содержания программ Родительского университета. Режим доступа: https://ioe.hse.ru/data/2016/09/06/1120268643/Методические%20рекомендации.pdf

Принцип безопасности применяемых методов. Специалист не имеет права применять в работе с родителями методы, в безвредности которых для психического или физического здоровья участника он не уверен.

Принцип соблюдения равноправия позиций специалиста и родителей. Необходимо признавать потенциал родителей к самостоятельному решению проблем, их готовность нести ответственность за свои действия, уважать их выбор. Уважение к индивидуальному опыту родителей. Работая со взрослыми людьми, специалист не должен дискредитировать или преуменьшать значение их личного опыта, переживаний и эмоций. Обращение к жизненному опыту родителей может стать мощным ресурсом в работе.

Специалист должен исходить из признания доброжелательного отношения родителей к ребенку и их стремления повысить свою родительскую компетентность

В Свердловской области родительский университет функционирует на базе ГБУ СО «Центр психолого-педагогической, медицинской и социальной помощи «Ладо» http://centerlado.ru/news/priglashaem-vseh-zhelayuschih-v-roditelskiy-universitet/. Примерное содержание занятий представлено в приложении. Определение содержания занятий родительского университета на базе школы (класса) зависит от потребностей родителей, актуальных проблем класса и возможностей образовательной организации в привлечении специалистов (медиков, психологов и др.).

Профилактическая работа предполагает формирование:

- установок на безопасное поведение и навыков безопасного поведения;
- личностных качеств школьников, связанных с готовностью к ответственному, сознательному выбору; развитие умений целеполагания и планирования;
- развитие коммуникативных навыков и эмоционального интеллекта: безопасной самопрезентации и взаимодействия, разрешения конфликтов;
- развитие умения критически анализировать информацию и содержание информационных сообщений, особенно сообщений, призывающих к каким-либо действиям; развитие умений видеть альтернативные способы поведения, говорить «нет», запрашивать помощь.

Для развития ценностей наиболее адекватной технологией является мастерская ценностных ориентаций. Мастерская предполагает совместную деятельность детей и взрослых. Организация коллективной творческой деятельности детей и взрослых в мастерской имеет свои закономерности, алгоритм, позволяющий каждым этапом его реализации подготовить следующий шаг продвижения к цели.

Алгоритм деятельности в мастерской ценностных ориентаций, ее основные этапы[18].

Начало мастерской (индуктор) – первое задание в мастерской, мотивирующее дальнейшую деятельность участников. Оно актуализирует

[18] Галицких, Е. О. От сердца к сердцу. Мастерские ценностных ориентаций для педагогов и школьников: методическое пособие / Е. О. Галицких. – Санкт-Петербург: Паритет, 2003. – 160 с.

личный опыт каждого и создает ситуацию выбора, сбора ассоциаций, пробуждает фантазию и познавательный интерес, включает в деятельность.

Первый этап работы с материалом, информацией, ситуацией, опытом отношений. Он включает создание творческого продукта, социализацию, т.е. предъявление созданного продукта всем участникам мастерской, промежуточную рефлексию и самокоррекцию деятельности. Эта работа сопровождается активизацией познавательного интереса, завершается формированием вопросов.

Второй этап обращает к новой информации, ее обработке (составлению схем, афиш, рисунков, планов, проектов, газет), к корректировке творческого продукта. Социализация (обсуждение в группе), возникновение «разрыва» между старым и новым пониманием, представлением, выдвижение гипотез, вариантов суждений, новых вопросов – кульминационный момент мастерской. «Афиширование» предполагает представление участниками своих открытий, позиций, проектов, афиш, текстов, ситуаций.

Рефлексивный этап – завершение работы общим анализом пережитого, понятого, открытого в себе. Рефлексия может завершиться выходом на новые проблемы. На этом этапе дети учатся анализировать свой личный духовный, нравственный, познавательный опыт, свое отношение и настроение, учатся высказывать свои суждения открыто, искренне, тактично по отношению к другим.

Проектирование мастерской ценностных ориентаций в контексте обеспечения информационной безопасности обучающихся может быть связано с развитием ценностей семьи, реального общения и др.

Родители несут ответственность за обеспечение безопасности ребенка. Одно из направлений этого – определение правил пользования Интернетом. Оптимальным является совместное определение некоторых аспектов таких правил перед первым выходом в Интернет. Поскольку это зачастую происходит еще в начальной школе, то пропорции совместного определения правил меняются: родители младших школьников практически полностью определяют правила. Обсудите с ребенком куда ему можно заходить (возможно, стоит составить список сайтов), что можно и что нельзя делать, сколько времени можно находиться в Интернете.

В средней и старшей школе – возможности взаимного согласования правил гораздо больше. Интересы и компетенции школьника должны приниматься во внимание.

Для утверждения и большей наглядности, возможно выработанные совместно правила оформить в виде следующего семейного соглашения, объяснив ребенку, что Вы доверяете ему и заботитесь о его безопасности. То же относится и к родителям, ограничивая время нахождения ребенка в интернете, родитель и сам должен являться образцом такого поведения.

Представляем набор пунктов для составления семейного соглашения. Выбор необходимых пунктов определяется индивидуально, в зависимости от индивидуально-психологических и возрастных особенностей ребенка. Набор пунктов дополняется в зависимости от представлений родителей и по итогам совместного согласования с ребенком.

Родитель для безопасности ребенка должен:

1. Объяснить правила безопасного использования интернета:

- посещаемые сайты и правила безопасного поведения на них:_____
- персональные данные, которые нельзя распространять_____
- правила составления и хранения паролей_____
- правила общения в интернете (общение с незнакомыми людьми): _____
- другое_____

2. Обеспечить настройку родительского контроля на всех устройствах, доступных ребенку.
3. Осуществлять мониторинг посещаемых ребенком страниц и аккаунтов в соцсетях.
4. Контролировать время, проведенное в Сети
5. 5. В течение некоторого времени сопровождать ребенка в его путешествиях по сети для того, чтобы убедиться, что ребенок соблюдает данное соглашения.
6. Для безопасного поведения в интернете повышать свою информационную грамотность и грамотность ребенка.
7. Другое

_____

Ребенок должен:

Обращаться к моим родителям, чтобы узнать правила пользования Интернетом: безопасные сайты, время моего использования интернета (___ минут непрерывно / ___ часов в день).

Никогда не выдавать без разрешения родителей для каждого отдельного случая личную информацию (персональные данные): домашний адрес, номер телефона, рабочий адрес или номер телефона родителей, номера кредитных карточек или название и расположение моей школы, личные и семейные фотографии.

Всегда немедленно сообщать родителям, если я увижу или получу в Интернете что-либо тревожащее меня или угрожающее мне; сюда входят сообщения электронной почты, сайты или даже содержимое обычной почты от друзей в Интернете.

Никогда не соглашаться лично встретиться с человеком, с которым я познакомился в Интернете, без разрешения родителей для каждого отдельного случая.

Никогда не отправлять без разрешения родителей для каждого отдельного случая свои фотографии или фотографии членов семьи другим людям.

Никогда никому, кроме своих родителей, не сообщать пароли Интернета (даже лучшим друзьям).

Вести себя в Интернете корректно, проявлять уважение к собеседникам и не делать ничего, что может обидеть или разозлить других людей или противоречить закону.

Никогда не загружать, не устанавливать и не копировать ничего с дисков или из Интернета без разрешения родителей для каждого отдельного случая.

Никогда не делать без разрешения родителей в Интернете ничего, требующего оплаты.

Для сохранения своей безопасности сообщить родителям свое регистрационное имя и пароль, при участии в чатах или блогах - e-mail адрес и пароль почтового ящика. Никому, кроме родителей, эти сведения сообщать категорически нельзя.

Другое_____

Дата

Родитель_____

Ребенок_____ [7].

Примерный план работы Родительского университета (на базе ГБОУ СО «ЦППМСП «Ладо») [7]

Название мероприятия	**Форма проведения мероприятия**
Влияние родительских установок и семейных ценностей на формирование личности ребенка. Закон для всех един	Мастер-класс
Поведенческие проблемы ребенка – тревога, агрессия, негативизм, капризы, упрямство.	Мастер-класс
Рискованное поведение подростков: причины и следствия	Практическое занятие
Родители и дети – трудности взаимопонимания	Мастер-класс
Помощь родителям детей с нарушениями речи	Родительская конференция для родителей детей раннего и дошкольного возраста
Интернет безопасность	Семинар
Адаптация первоклассника к школе	Семинар-тренинг
Родители и подростки.	Семинар
Занятость ребенка в летние каникулы. Как провести время с пользой	Родительская конференция
Занятость ребенка в летние каникулы. Как провести время с пользой	Родительская конференция
На пороге выбора.	Семинар для родителей детей выпускных классов
Как помочь ребенку адаптироваться в начальной школе	Семинар для родителей будущих первоклассников
Нежный возраст. Главное – не опоздать!	Родительская конференция
Секреты правильного воспитания: нужны ли наказания	Семинар

Как помочь ребенку научиться управлять собой	Тренинг для детей и родителей
Как помочь ребенку в трудной ситуации	Семинар
Детская агрессия: причины, последствия, помощь	Семинар-тренинг для родителей
Что делать, если ваш ребенок стал жертвой притеснения (буллинга)	Семинар

Новые формы взаимодействия родителей с детьми

В настоящее время большой популярностью пользуются различные объединения в группы в социальных сетях, мессенджерах и т.п. Почему бы не использовать такие формы для организации совместной деятельности в семье?

Создание семейных чатов в мессенджерах, группы семьи в социальных сетях позволить объединить в сообщество близких родственников, но и членов семьи, проживающих в других городах, регионах и даже странах. Возможность быстро организовать семейное мероприятие, поделиться фотографиями и видеороликами с членами группы, обсудить интересные книги и фильмы, поделиться впечатлениями и даже узнать о здоровье близкого человека – все это позволит нивелировать разницу поколений, выстроить психологический «мостик» с ребенком, стать ему ближе.

Дети дошкольного и младшего школьного возраста с удовольствием будут участвовать в развитии совместного с родителями you-tube канала, записывая сначала игровые ролики, которые постепенно можно заменять тематикой развивающей направленности. Родители с детьми могут разработать и освещать в сети исследовательский проект, период работы с которым может быть достаточно длительным.

В заключении считаем привести цитаты из интервью Оксаны Силантьевой, специалистом по работе с медиа-пространством. «Чего боимся, то и запрещаем. Когда я слышу, что кто-то хочет закрыть доступ, запереть на замок, привязать к батарее, я сразу вижу страх. Страх перед неизвестным. К примеру, опасен огонь и опасны спички. Но ведь мы не запрещаем ни то, ни другое, мы постепенно учим детей, как ими пользоваться, чтобы было не опасно. В этой ситуации интернет ничем не отличается от тех же спичек и огня. Еще раз повторюсь, мы не запрещаем, мы учим всем этим пользоваться… Уверена важно донести до родителей, что запретами они ничего не решат. Закрыть доступ к информации в наше время неправильно, да и не получится это. Медиа-пространство везде. Если ребёнок не прочтет что-то в интернете, ему всё равно расскажут об этом в школе или во дворе. Родители должны понять, что интернет-грамотностью ребенка никто не займется, кроме них. Это их прямая задача и обязанность. Мы же помогаем детям с уроками, поэтому надо помочь и с освоением интернета».

«У всего должна быть золотая середина. Нельзя ребенка ограничивать полностью, но и уходить в виртуальную реальность с головой все же не стоит. Любому поколению было сложно освоить технические новинки. Но сейчас даже некоторые пенсионеры выкладывают посты в Инстаграмме и Твиттере. А дети самостоятельно монтируют видео и ведут блоги на Ютубе. Интернет – это не вопрос возраста, а свежести восприятия и готовности меняться, в том числе, и самостоятельно».

Симбиоз медиа и реального пространства очень важен. К примеру, нашумевшая игра – «Покемон го». Столько критики в ее адрес со всех сторон. Однако, есть прекрасный взгляд на эту игру. Компьютерная игра выгнала людей на улицу! Они ходят пешком, ищут, изучают город и одновременно занимаются спортом, дышат воздухом. Не бывает чёрного и белого. Вопрос в том, насколько трезво мы смотрим на это явление, и ищем там хорошие стороны!» [8].

Библиографический список

1. «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс]: федеральный закон от 29.12.2010 № 436-ФЗ // Официальный сайт компании «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 24.09.2019)
2. Безопасность детей в Интернете [Электронный ресурс]: рекомендации для родителей / Временная комиссия по развитию информационного общества Совета Федерации. – Режим доступа: https://drive.google.com/file/d/1x8ab139hN7PN590M8mY7UTXDIJB_0HHD/view (дата обращения: 25.09.2019)
3. Информационная безопасность обучающихся в современной информационной среде [Текст]: метод. рекомендации / Н. В. Шпарута [и др.]; М-во общего и профессионального образования Свердловской области; Гос. автоном. образоват. учреждение доп. проф. образования Свердловской области «Институт развития образования». – Екатеринбург: ГАОУ ДПО СО «ИРО», 2017. – 66 с.
4. Теория поколений Н. Хоува и В. Штрауса. Возможности практического применения [Электронный ресурс] / Е. М. Ожиганова // Бизнес-образование в экономике зананий. – 2015. - №1. – С. 94-97. – Режим доступа: https://cyberleninka.ru/article/v/teoriya-pokoleniy-n-houva-i-v-shtrausa-vozmozhnosti-prakticheskogo-primeneniya (дата обращения: 24.09.2019)
5. Социальные сети: возможности и риски для обучения и воспитания [Текст]: метод. рекомендации / Н. В. Шпарута, Г. А. Бутакова; М-во общего и профессионального образования Свердловской области; Гос. автоном. образоват. учреждение доп. проф. образования Свердловской области «Институт развития образования». – Екатеринбург: ГАОУ ДПО СО «ИРО», 2017. – 53 с.
6. Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учетом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности [Электронный ресурс]: методические рекомендации // Онлайн-площадка для проведения Единых уроков. – Режим доступа: https://www.единыйурок.рф/images/doc/metod/cyber.pdf (дата обращения: 25.09.2019)
7. Методические рекомендации для педагогов и родителей по повышению уровня информационной безопасности детей по итогам социологического исследования проблемы «Деятельность подростков в сети Интернет: динамика, риски, реакция родителей» [Текст]: метод. рекомендации / Л. И. Долинер [и др.]; М-во образования и молодежной политики Свердловской области; Гос. автоном. образоват. учреждение доп. проф. образования

Свердловской области «Институт развития образования». – Екатеринбург: ГАОУ ДПО СО «ИРО», 2019. – 55 с.
8. Интернет-пространство современного школьника: возможности и угрозы: метод. рекомендации / Н. В. Шпарута, М. Б. Медведева, Г. А. Бутакова; М-во общего и профессионального образования Свердловской области; Гос. автоном. образоват. учреждение доп. проф. образования Свердловской области «Институт развития образования». – Екатеринбург: ГАОУ ДПО СО «ИРО», 2017. – 65 с.
9. Цифровая грамотность и безопасность в Интернете [Электронный ресурс]: метод. пособие / Г. Солдатова [и др.]; Фонд Развития Интернет, ФГАУ «Федеральный институт развития образования» М-ва образования и науки РФ, факультет психологии МГУ имени. М. В. Ломоносова. – Режим доступа: http://www.razbiraeminternet.ru/files/google_book_theory_stranicy.pdf (дата обращения 26.09.2019)