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

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»

Методические рекомендации

Екатеринбург
2019

ББК 74.200.5я81+74.6
М 54

Рецензенты:
Н. Ю. Сероштанова, старший преподаватель кафедры прикладной информатики МБОУ ВО ЕАСИ (институт), г. Екатеринбург; руководитель проектов ООО «P2P Технологии»;
М. А. Герасимова, кандидат педагогических наук, доцент, заведующий кафедрой педагогики профессионального образования ГАОУ ДПО СО «ИРО»

Авторы:
Л. И. Долинер, доктор педагогических наук, профессор кафедры информационных технологий ГАОУ ДПО СО «ИРО»;
Г. А. Бутакова, заведующий центром дистанционных образовательных технологий ГАОУ ДПО СО «ИРО»;
Е. В. Ахлестина, старший преподаватель кафедры информационных технологий ГАОУ ДПО СО «ИРО»;
Т. А. Сундукова, заведующий отделом исследования состояния системы образования ГАОУ ДПО СО «ИРО»;
Д. Е. Щипанова, кандидат психологических наук, доцент кафедры воспитания и дополнительного образования ГАОУ ДПО СО «ИРО»

М 54 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» : методические рекомендации / Л. И. Долинер [и др.]; Министерство образования и молодежной политики Свердловской области, Государственное автономное образовательное учреждение дополнительного профессионального образования Свердловской области «Институт развития образования». – Екатеринбург: ГАОУ ДПО СО «ИРО», 2019. – 55 с.

Данное издание включает методические рекомендации по повышению уровня информационной безопасности по итогам социологического исследования проблемы «Деятельность подростков в сети Интернет: динамика, риски, реакция родителей». Предлагаемые методические разработки могут быть использованы для проведения уроков информатики, классных часов и внеклассных мероприятий в образовательной организации.

ББК 74.200.5я81

Содержание

Введение

Поколение людей, родившихся до 2000-х гг., называют «цифровыми мигрантами»: эти люди родились до широкого распространения Интернета и осваивали его уже во взрослом возрасте. Современные дети и подростки относятся к «цифровому поколению» или «цифровым аборигенам».

Интернет с раннего возраста становится неотъемлемой частью их жизни. В связи с этим возникает опасность, что в Интернете дети и подростки могут столкнуться с ресурсами, содержащими не соответствующий их возрасту, неэтичный или даже опасный контент.

В 2019 г. специалистами ГАОУ ДПО СО «ИРО» было проведено социологическое исследование «Деятельность подростков в сети Интернет: динамика, риски, реакция родителей»[1].

Согласно результатам исследования, подавляющее большинство школьников 6–11-х классов (более 90 %) пользуются Интернетом каждый день, каждый второй школьник проводит в Интернете ежедневно от 3 до 6 часов. При этом чем старше подростки, тем больше времени они проводят в Интернете.

Следует отметить, что и среди учащихся основной школы, и среди старшеклассников выявлены подростки, которые проводят в сети Интернет от 10 до 15 и более 15 часов в день. Такое длительное пребывание связано с тем, что наиболее популярным устройством, используемым обучающимися для выхода в Интернет, является в настоящее время личный мобильный телефон. Кроме того, многие школьники имеют в распоряжении не только мобильный телефон, но и личный компьютер или ноутбук, планшет. И если раньше пребывание учащихся в Интернете ограничивалось их возможностями использования домашнего компьютера, то сейчас временные возможности использования Интернета практически ничем не ограничиваются.

[1] Выборку социологического исследования составили участники образовательных отношений из 60 общеобразовательных организаций Свердловской области. В исследовании принимали участие педагогические работники, исполняющие должностные обязанности классного руководителя, обучающиеся 6–8-х классов, обучающиеся 9–11-х классов, родители обучающихся. Общая численность участников исследования – 8043 человека.

Информационная безопасность: основные понятия

В Концепции информационной безопасности детей обозначены те риски, которые могут нарушить жизненный мир ребенка:

- отклонения в физическом развитии (избыточный вес, нарушения сна, проблемы со зрением);
- негативные эмоциональные состояния (страх, ужас, паника, тревога);
- киберзависимость от онлайн-игр, интернет-поиска, коммуникации в интернете;
- риски в области сексуального поведения (установление подростками беспорядочных связей благодаря сомнительным сайтам знакомств, киберпедофилия);
- поведение, связанное с риском для жизни или опасное для здоровья (психическая анорексия, суицидальное поведение, потребление психотропных веществ, легкодоступных для приобретения посредством специальных сайтов);
- кибербуллинг (травля, неоднократное умышленное причинение психологического вреда с помощью средств электронной коммуникации, таких как мобильные телефоны, блоги, веб-сайты).

Согласно результатам исследований, проведенных специалистами ГАОУ ДПО СО «ИРО»[2], риски, с которыми сталкиваются подростки в Интернете, прежде всего, обусловлены их собственным рискованным поведением: более половины школьников общаются в Интернете с незнакомыми людьми и впоследствии встречаются с ними лично. Другая группа проблем, с которыми сталкивается каждый второй подросток, – взлом аккаунтов и вредоносное программное обеспечение.

Также стоит обратить внимание на то, что каждый второй подросток подвергался хотя бы однажды кибербуллингу.

Рассмотрим понятие информационной безопасности детей, представленное в нормативно-правовых документах.

Согласно Федеральному закону, информационная безопасность детей – состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию[3].

В Концепции информационной безопасности детей она рассматривается в двух направлениях:

1) защита ребенка от дестабилизирующего воздействия информационной продукции;

---

[2] Деятельность подростков в сети Интернет: динамика, риски, реакция родителей: отчет по итогам социологического исследования. Екатеринбург: ГАОУ ДПО СО «ИРО», 2019

[3] О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон от 29 декабря 2010 г. № 436-ФЗ. Режим доступа: ivo.garant.ru/#/document/77680092/paragraph/1:0

2) создание условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и физического развития, сохранения психического и психологического здоровья и благополучия, а также формирования позитивного мировосприятия[4].

Информационная безопасность – важнейшая составляющая психологической безопасности ребенка в целом. Один из трех доминирующих идеалов информационного сообщества, по мнению А. Г. Асмолова, это безопасность.

Главными направлениями работы педагогов и родителей по обеспечению информационной безопасности обучающихся являются обеспечение безопасности информационной среды для обучающихся и развитие личностных установок и навыков безопасного поведения обучающихся в Интернете.

В рамках данных направлений задачами школы являются:

- деятельность по оценке безопасности информационной продукции;
- организация развития компетентности всех субъектов образовательной среды (педагогов, родителей, обучающихся) в области информационной безопасности;
- организация среды социализации современных обучающихся и развитие детско-родительских отношений;
- развитие ценностной и коммуникативной сферы личности обучающихся;
- развитие умений критического восприятия и оценки информации.

[4] Концепция информационной безопасности детей: Распоряжение Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р. Режим доступа: static.government.ru/media/files/mPbAMyJ29uSPhL3p20168GA6hv3CtBxD.pdf

Виды деятельности, характерные для подростков в сети Интернет

Школьники достаточно много времени проводят в сети Интернет. В ходе исследования «Деятельность подростков в сети Интернет: динамика, риски, реакция родителей» [2] были получены следующие данные (рис. 1):

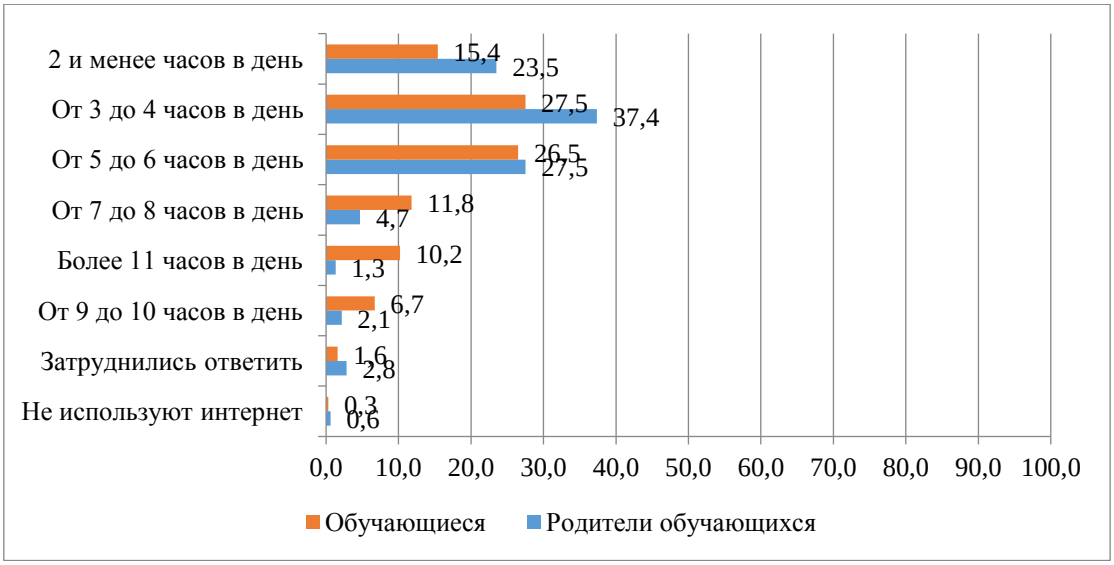


Рис. 1. Мнение обучающихся и их родителей о том, какое количество времени

В Интернете подавляющее большинство обучающихся чаще всего смотрят видео, фильмы, сериалы, слушают музыку, проводят время в социальных сетях и занимаются поиском информации для подготовки домашних заданий (докладов, сообщений, презентаций и др.). Обучающиеся старших классов в большей степени, чем учащиеся основной школы, используют Интернет для образовательных целей: учебы и подготовки домашних заданий, чтения и самообразования (табл. 1).

Таблица 1

Бюджет времени школьника (9–11-й класс) в Интернете (среднее значение в часах)

Деятельность в Интернете	Затраты времени
1. Общение, переписка в социальных сетях и мессенджерах	3,4
2. Просмотр видео, фильмов и сериалов	3,1
3. Прослушивание музыки, радио, подкастов	3,0
4. Поиск информации, не связанной с учебой	2,4
5. Образование, подготовка к урокам, выполнение домашних заданий	2,3
6. Чтение книг, журналов, статей	1,7
7. Онлайн-игры	1,4
8. Творчество, создание своего контента, ведение блога	1,2

Наиболее распространенными причинами, побуждающими старшеклассников использовать Интернет в учебных целях, являются возможность быстрее

найти нужную информацию (69,3 %) и возможность получать новые знания, навыки в удобном режиме, не выходя из дома (62,8 %). Порядка 40 % опрошенных старшеклассников считают, что информация, представленная в Интернете, более качественная, понятная, актуальная, чем в учебниках. Более четверти учащихся 9–11-х классов считают, что курсы, обучающие видео, тексты в Интернете более понятны и интересны, чем уроки в школе.

Информационная безопасность детей в Интернете предполагает минимизацию рисков, связанных с причинением вреда здоровью, физическому, психическому, духовному и нравственному развитию детей. Вместе с тем практически каждый второй участник исследования (47,5 %) сталкивался в Интернете с опасной информацией. При этом чем старше школьники, тем выше среди них доля респондентов, которые считают, что сталкивались в Интернете с опасной информацией.

Угрозу информационной безопасности обучающихся в Интернете прежде всего представляет информация, не предназначенная для детей. К такого рода информации относится: навязчивая реклама, слухи и сплетни, изображения употребления алкоголя, наркотиков, курение; оскорбления представителей отдельных национальностей, религий; сцены насилия и жестокости, откровенные сцены (18+).

В рамках исследования было выявлено, что с информацией той или иной направленности сталкивался в Интернете практически каждый участник исследования, при этом более 25 % школьников регулярно видят в Интернете информацию, не предназначенную для детей.

Следует обратить внимание, что по всем обозначенным содержательным направлениям информационных материалов есть группа опрошенных, которые видят эти материалы каждый раз, когда заходят в Интернет. В связи с этим можно заключить, что у этих респондентов сформировался устойчивый интерес к подобным информационным материалам, вероятно, что они целенаправленно обращаются к ним.

Следует также отметить, что среди обучающихся младшего подросткового возраста (6–8-е классы) доля детей, которые сталкивались с информацией, не предназначенной для детей, ниже, чем среди школьников старшего подросткового возраста (9–11-е классы). Такие отличия могут быть обусловлены тем, что учащимся старших классов предоставляется большая самостоятельность в использовании Интернета, в то время как учащиеся 6–8-х классов чаще осуществляют работу в Интернете под контролем взрослых.

Помимо информации, не предназначенной для детей, в Интернете существуют и другие риски безопасности детей.

Среди рисков информационной безопасности, с которыми в Интернете сталкивались обучающиеся, наиболее распространены такие, как вредоносное программное обеспечение и взлом аккаунтов в социальных сетях. С этими проблемами хотя бы 1 раз сталкивались порядка 60 % школьников.

Более 30 % школьников также признались, что их оскорбляли, унижали в личных сообщениях, комментариях к публикациям. Каждый четвертый школьник столкнулся с тем, что его персональные данные, фото, видео распространяли без его согласия. Порядка 15 % опрошенных потеряли денежные средства из-за

действий злоумышленников в Интернете, а также стали жертвами угроз и шантажа.

Довольно распространенной угрозой для обучающихся является общение в Интернете с незнакомыми людьми. Очевидно, что обучающиеся пренебрегают своей безопасностью в этой сфере. Большинство участников исследования имели не только опыт общения с незнакомыми людьми в Интернете (74 %), но и опыт встреч с ними в реальной жизни (60 %).

Вместе с тем только 10 % опрошенных регулярно переносят виртуальные контакты в реальную жизнь. Для большинства подростков интернет-знакомства представляют скорее определенный эксперимент, чем рутинную практику. Стоит отметить, что доля подростков, которые имеют негативный опыт общения в реальной жизни с интернет-знакомыми (7 %), примерно соответствует доле опрошенных, регулярно встречающихся с новыми знакомыми (10 %). Таким образом, встречи с интернет-знакомыми представляют для школьников определенный риск. В наибольшей степени это характерно для старшеклассников.

Ряд угроз в равной степени актуален для подростков любого возраста, у них взламывают страницы в социальных сетях, они также часто сталкиваются с оскорблениями, угрозами, распространением персональных данных без их согласия. Так, каждый второй школьник признался, что хотя бы однажды его оскорбляли, унижали в личных сообщениях, комментариях к публикациям. При этом 6 % опрошенных утверждают, что терпят это постоянно.

Несмотря на то, что практически все школьники встречались в Интернете с определенными рисками, большинство из них, вне зависимости от возраста, рассматривают интернет-пространство как безопасное для себя. Стоит отметить, что это соответствует данным, полученным в ходе социологического исследования «Особенности обеспечения информационной безопасности обучающихся в образовательной организации и за ее пределами», проведенного специалистами ГАОУ ДПО СО «ИРО» в 2018 году[5]. В связи с этим можно говорить об устойчивости тенденции.

Интернет становится неотъемлемой частью жизни современных подростков, они воспринимают его как естественное пространство общения и жизнедеятельности и, возможно, поэтому могут недооценивать риски, проявлять рискованное поведение.

При этом чем старше подростки, тем более они уверены в собственной безопасности в Интернете, что, вероятно, обусловлено уверенностью в своих навыках использования Интернета и самоидентификацией со взрослыми пользователями. Таким образом, представляется, что рискованное поведение подростков в Интернете может быть обусловлено излишней уверенностью в своих силах и стремлением проявить свою самостоятельность.

Чем более активными пользователями являются подростки, чем больше

[5] Выборку социологического исследования составили участники образовательных отношений из 55 общеобразовательных организаций Свердловской области. В исследовании принимали участие руководящие работники общеобразовательных организаций, педагогические работники, исполняющие должностные обязанности классного руководителя, обучающиеся 7-х и 10-х классов, родители обучающихся. Общая численность участников исследования – 5724 человека.

времени они проводят в Интернете, тем в большей степени они подвержены действию различных интернет-угроз. Важно акцентировать внимание школьников, особенно старшего подросткового возраста, что в интернет-пространстве, как и в реальной жизни, существуют угрозы, которым в равной степени подвержены и взрослые, и дети.

Деятельность по оценке информационной безопасности

При возникновении ***различных сложных, опасных ситуаций*** в Интернете важно, чтобы подростки знали, как следует вести себя и к кому они могут обратиться за помощью. Вместе с тем при возникновении подобных ситуаций школьники предпочитают справляться с ними самостоятельно, особенно это характерно для старшеклассников.

Можно констатировать, что сегодняшние школьники уже самостоятельно оценивают (или пытаются оценить) возникающие угрозы в виртуальной среде. Так, в исследовании [2] получены следующие данные (табл. 2):

Таблица 2

Информация, которая, по мнению подростков, является опасной для их сверстников, %

Варианты ответа	Доля респондентов
1.Вредоносное программное обеспечение, платные подписки, вирусные сайты, запрещенные сайты	13,2
2.Информация о суицидах, группы смерти, склонение к суицидам	11,9
3.Пропаганда/продажа наркотиков, запрещенных веществ	9,0
4.Пропаганда терроризма, вовлечение в террористическую деятельность	6,2
5.Спам, реклама, рассылки	5,3
6.Мошенничество, взлом банковских карт, вымогательство	5,2
7.Жестокость, убийства, насилие	3,8
8.Пропаганда алкоголя	3,1
9.Порнография	3,1
10.Дезинформация, ложная информация, фейковые новости	2,4
11.Информация о легком заработке денег	2,2
12.Взлом аккаунтов	2,1
13.Пропаганда экстремизма, вовлечение в экстремистскую деятельность (в т. ч. банды «АУЕ»)	2,0
14.Пропаганда курения	1,6
15.Информация, не предназначенная для детей, имеющая маркировку «18+»	1,4
16.Сайты знакомств, общение с незнакомыми людьми в Интернете	1,4

Варианты ответа	Доля респондентов
17.Запрещенная информация, товары и услуги, подстрекательство к незаконной деятельности	1,4
18.Угрозы	1,2
19.Азартные игры, онлайн-казино	1,1
20.Оскорбления, травля в Интернете, кибербуллинг	0,8
21.Вовлечение в деятельность религиозных сект	0,5
22.Спойлеры	0,4
23.Педофилия, сексуальные домогательства	0,2
24.Инструкции по созданию оружия	0,2
25.Пропаганда анорексии, булимии, бодишейминга	0,2
26.Расизм	0,1
27.Гомофобия	0,1
28.Нет ответа	26,3
29.«Для разумных людей не существует опасной информации»	6,8
30.Любая информация в Интернете опасна для подростков	1,1

Наиболее распространены ответы, касающиеся вредоносного программного обеспечения, склонения к суициду, пропаганды и распространения наркотиков.

В целом примерно половина школьников не рассказывают родителям о проблемах, с которыми сталкиваются в Интернете. К родителям обращаются за помощью чаще всего тогда, когда сталкиваются с вредоносным программным обеспечением, взломом аккаунтов.

Проблемы, связанные не с технической стороной, а с коммуникацией в Интернете и выстраиванием взаимоотношений с людьми, школьники предпочитают решать самостоятельно, не прибегая к помощи кого-либо из взрослых.

Таким образом, риски информационной безопасности в равной степени актуальны для подростков младшего и старшего возраста. Однако старшие подростки более склонны к рискованному поведению.

Важно подчеркнуть, что родители обучающихся и классные руководители информированы о тех рисках, с которыми учащиеся могут столкнуться в Интернете, однако многие из них недооценивают степень реальной угрозы именно для их детей.

С различными угрозами безопасности в Интернете сталкивалась значительно большая доля обучающихся, чем думают их родители и классные руководители.

По мнению **родителей**, подростки сталкиваются преимущественно с теми угрозами, которые связаны с вредоносными программами, взломом профилей в социальных сетях и которые родители считают наименее опасными. С теми же угрозами, которые родители относят к числу наиболее опасных (контент, содержащий сцены насилия и жестокости, «группы смерти», пропаганда наркотиков, алкоголя, табакокурения), по мнению родителей, сталкивалась незначительная

доля подростков. Можно предположить, что наибольшие угрозы для своих детей в Интернете родители определяют, основываясь на информации, полученной из СМИ, от работников общеобразовательных организаций, а не из личного опыта.

Согласно результатам исследования, большинство родителей (67,4 %) контролируют деятельность своих детей в Интернете.

Действия, которые предпринимают родители подростков, чтобы обезопасить ребенка от угроз, связанных с Интернетом, чаще всего подразумевают разъяснительные, информационные, воспитательные меры (информирование ребенка об опасностях, с которыми он может столкнуться в Интернете, и, с другой стороны, о возможностях Интернета, полезных сайтах; советы о поведении в Интернете и т. п.).

Ограничительные меры используются реже, самая распространенная из них – ограничение времени, которое ребенок проводит в Интернете. Порядка 40 % родителей мониторят социальные сети ребенка, каждый четвертый при этом просматривает личную переписку ребенка в социальных сетях и мессенджерах.

При этом подростки зачастую не осознают, что родители контролируют их деятельность в Интернете. С одной стороны, это может быть вызвано тем, что родители используют скрытые формы контроля, с другой – тем, что родители осуществляют контроль посредством разговоров с ребенком, советов, установления доверительных отношений и т. п.

Важно отметить, что большинство подростков в достаточной степени доверяют родителям, чтобы обращаться к ним за помощью в случае возникновения серьезной проблемы в Интернете, и данные ситуации преимущественно разрешаются совместно родителями и детьми. При этом часть проблем, с которыми подростки сталкиваются в Интернете, они решают самостоятельно.

Многие родители считают эффективными для обеспечения безопасности ребенка в Интернете методы жесткого контроля, но по тем или иным причинам не применяют их. В то же время родители, применяющие разъяснительные меры, беседующие с ребенком о его деятельности в Интернете и дающие ему советы, как обезопасить себя, не всегда находят данные меры эффективными.

Родители обучающихся достаточно высоко оценивают собственную информированность о том, чем занимаются их дети в Интернете. Вместе с тем оценки информированности родителей, данные обучающимися, несколько ниже, чем самооценка информированности родителей. Можно предположить, что, с одной стороны, некоторые обучающиеся не подозревают о наличии контроля со стороны родителей, с другой – некоторые родители обучающихся недостаточно информированы о том, чем их дети занимаются в Интернете.

В настоящее время работа классных руководителей должна быть направлена на изучение особенностей пребывания обучающихся в сети Интернет. Большинство **классных руководителей** отслеживают деятельность обучающихся своего класса в Интернете, но лишь половина из них может сказать о том, чем занимаются в Интернете большинство обучающихся их класса, о деятельности всех обучающихся класса знают только 6,9 % классных руководителей, принявших участие в исследовании.

Наиболее распространенной формой работы по обеспечению информационной безопасности в Интернете классных руководителей с обучающимися является проведение тематических уроков, классных часов и индивидуальных бесед по вопросам информационной безопасности обучающихся в Интернете.

Чаще всего классные руководители для обеспечения информационной безопасности в Интернете рассказывают обучающимся о правонарушениях в Интернете, обучают распознавать мошеннические сообщения, разговаривают с учениками о том, что следует делать в случае столкновения с трудными/неприятными ситуациями в Интернете (оскорблениями, шантажом, правонарушениями и т. д.), а также рассказывают о возможностях Интернета для обучения, общения, показывают полезные сайты.

Примерно треть классных руководителей отметили, что обучающиеся обращались к ним за помощью в связи с проблемами в Интернете. При этом основная часть вопросов, с которыми обращались обучающиеся, была связана с кибербуллингом, взломом их профилей, страниц в социальных сетях, почты. Классные руководители решали проблему совместно с обучающимися, советовали, как лучше поступить. Следует отметить, что чаще всего обращаются за помощью к классному руководителю дети младшего подросткового возраста, старшие подростки в большинстве случаев решают проблемы, с которыми они столкнулись в Интернете, самостоятельно.

В заключение хотелось бы обратить внимание на ряд важных выводов. Современные подростки располагают достаточно полной информацией о том, как защититься от таких угроз, как вирус, спам, навязчивая реклама. Очень многие из них зачастую лучше, чем взрослые, разбираются в технической стороне вопроса.

Вместе с тем дети не готовы противостоять угрозам, исходящим от реальных людей и связанным с оскорблениями и унижениями. У них отсутствуют четкие установки, не сформированы определенные стереотипы поведения в подобных ситуациях. У многих учащихся отсутствует также представление о том, что деятельность, которая осуществляется в Интернете, становится одной из сторон реальной жизни современного человека, на которую распространяются нормы поведения, принятые в обществе.

Именно на эти вопросы мы предлагаем обратить внимание и классных руководителей, и других специалистов, занимающихся вопросами воспитания в целом и информационной безопасности обучающихся в частности.

Важным аспектом информационной безопасности школьников является обеспечение безопасности информационного контента, предоставляемого обучающимся педагогами и родителями.

Согласно закону (Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»), к информации, причиняющей вред здоровью и (или) развитию детей, относится запрещенная для распространения среди детей информация, распространение которой среди детей определенных возрастных категорий ограничено.

Информация, запрещенная для распространения среди детей:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;
2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом (3.1 – содержащая изображение или описание сексуального насилия);
4) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;
5) оправдывающая противоправное поведение;
6) содержащая нецензурную брань;
7) содержащая информацию порнографического характера;
8) о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

Информация, распространение которой среди детей определенных возрастных категорий ограничено:

1) представляемая в виде изображения или описания жестокости, физического и (или) психического насилия (за исключением сексуального насилия), преступления или иного антиобщественного действия;
2) вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
3) представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
4) содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Важно также обеспечивать возрастно-психологическое соответствие предъявляемой информационной продукции. Классификация информационной продукции, предназначенной и (или) используемой для обучения и воспитания

детей в организациях, осуществляющих образовательную деятельность по реализации основных общеобразовательных программ, образовательных программ среднего профессионального образования, дополнительных общеобразовательных программ, осуществляется в соответствии с Федеральным законом и законодательством об образовании и в соответствии с классификацией информационной продукции по следующим категориям:

1) информационная продукция для детей, не достигших возраста шести лет;
2) информационная продукция для детей, достигших возраста шести лет;
3) информационная продукция для детей, достигших возраста двенадцати лет;
4) информационная продукция для детей, достигших возраста шестнадцати лет.

Информационная продукция для детей, не достигших возраста шести лет (маркировка информационной продукции 0+)

К информационной продукции для детей, не достигших возраста шести лет, может быть отнесена информационная продукция, содержащая информацию, не причиняющую вреда здоровью и (или) развитию детей (в том числе информационная продукция, содержащая оправданные ее жанром и (или) сюжетом эпизодические ненатуралистические изображение или описание физического и (или) психического насилия (за исключением сексуального насилия) при условии торжества добра над злом и выражения сострадания к жертве насилия и (или) осуждения насилия).

Информационная продукция для детей, достигших возраста шести лет (маркировка информационной продукции 6+)

К допускаемой к обороту информационной продукции для детей, достигших возраста шести лет, может быть отнесена информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

1) кратковременные и ненатуралистические изображение или описание заболеваний человека (за исключением тяжелых заболеваний) и (или) их последствий в форме, не унижающей человеческого достоинства;
2) ненатуралистические изображение или описание несчастного случая, аварии, катастрофы либо ненасильственной смерти без демонстрации их последствий, которые могут вызывать у детей страх, ужас или панику;
3) не побуждающие к совершению антиобщественных действий и (или) преступлений эпизодические изображение или описание этих действий и (или) преступлений при условии, что не обосновывается и не оправдывается их допустимость и выражается отрицательное, осуждающее отношение к лицам, их совершающим.

Информационная продукция для детей, достигших возраста двенадцати лет (маркировка информационной продукции 12+)

К допускаемой к обороту информационной продукции для детей, достигших возраста двенадцати лет, может быть отнесена информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

1) эпизодические изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);
2) изображение или описание, не побуждающие к совершению антиобщественных действий (в том числе к потреблению алкогольной и спиртосодержащей продукции, участию в азартных играх, занятию бродяжничеством или попрошайничеством), эпизодическое упоминание (без демонстрации) наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий при условии, что не обосновывается и не оправдывается допустимость антиобщественных действий, выражается отрицательное, осуждающее отношение к ним и содержится указание на опасность потребления указанных продукции, средств, веществ, изделий;
3) не эксплуатирующие интереса к сексу и не носящие возбуждающего или оскорбительного характера эпизодические ненатуралистические изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

Информационная продукция для детей, достигших возраста шестнадцати лет (маркировка информационной продукции 16+)

К допускаемой к обороту информационной продукции для детей, достигших возраста шестнадцати лет, может быть отнесена информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

1) изображение или описание несчастного случая, аварии, катастрофы, заболевания, смерти без натуралистического показа их последствий, которые могут вызывать у детей страх, ужас или панику;
2) изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);

3) информация о наркотических средствах или о психотропных и (или) об одурманивающих веществах (без их демонстрации), об опасных последствиях их потребления с демонстрацией таких случаев при условии, что выражается отрицательное или осуждающее отношение к потреблению таких средств или веществ и содержится указание на опасность их потребления;
4) отдельные бранные слова и (или) выражения, не относящиеся к нецензурной брани;
5) не эксплуатирующие интереса к сексу и не носящие оскорбительного характера изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

При отборе информационного контента, предъявляемого обучающимся, педагогам и родителям важно анализировать содержание информации, ориентироваться на данные критерии (маркировку информационной продукции), с целью обеспечить возрастно-психологическое соответствие.

Организация развития компетентности всех субъектов образовательной среды (педагогов, родителей, обучающихся) в области информационной безопасности

Цифровая и медиаграмотность предполагает формирование и развитие пользовательских умений и установки на эффективную работу с информационными ресурсами, а также ответственное отношение к собственному поведению, основанное на осознавании последствий своих действий в интернет-пространстве.

Целесообразно организовать серию семинаров (возможно, в рамках родительского университета, в том числе в онлайн-форме) для родителей по проблеме обеспечения информационной безопасности школьников с привлечением различных специалистов: из области права, IT-технологий, психологии и др.

Содержание семинаров должно охватывать: технические, правовые и психологические аспекты информационной безопасности.

В настоящее время достаточно разработок в данном направлении. Например, работы «Фонда Развития Интернет» (detionline.com/internet-project/training-aids). Примерная структура дидактических материалов представлена в приложении.

Материалы по информационной безопасности также разработаны и представлены на сайте ГАОУ ДПО СО «ИРО» на сайтах кафедры информационных технологий (irro.ru/index.php?cid=148) и кафедры воспитания и дополнительного образования (irro.ru/index.php?cid=352).

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, так же как и поведение в реальном жизненном пространстве. Поэтому для профилактики интернет-рисков большую значимость имеет управление социализацией 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, развитию 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. По данным исследования, подавляющее большинство подростков используют для общения в Интернете социальные сети. Мессенджеры и электронную почту старшеклассники предпочитают использовать в большей степени, чем обучающиеся 6–8-х классов (коэффициент Гамма составил 0,305 при значимости 0,000). Порядка 1/5 учащихся 6–8-х классов и 16,6 % старшеклассников общаются в чатах онлайн-игр (табл. 3) [2].

Таблица 3

Интернет-ресурсы, которые обучающиеся используют для общения, %

Интернет-ресурсы	Все обучающиеся	Обучающиеся 6–8-х классов	Обучающиеся 9–11-х классов
1. Социальные сети	94,6	93,9	95,2
2. Мессенджеры	37,7	27,6	47,0
3. Skype и похожие программы	28,2	27,5	28,8
4. Электронная почта	22,1	18,7	25,2
5. Чаты в онлайн-играх	18,7	20,9	16,6
6. Ленты комментариев на различных сайтах (за исключением социальных сетей)	7,2	5,7	8,5
7. Не общаюсь в Интернете	2,0	2,4	1,6
8. Затруднились ответить	0,1	0,0	0,2
9. Другое	0,3	0,3	0,2

Наибольшая доля подростков зарегистрирована в социальной сети «ВКонтакте» (93,9 % обучающихся 6–8-х классов и 96,8 % старшеклассников) [2]. Довольно популярной социальной сетью является также Instagram. В нем зарегистрированы 80,0 % учащихся 9–11-х классов и 67,3 % учащихся 6–8-х классов. Не зарегистрированы в социальных сетях порядка 2 % опрошенных обучающихся (см. табл. 4). В основном это обучающиеся более младшего возраста.

В результате проведения исследования выявлено, что подростки из сельских территорий и малых городов реже общаются в мессенджерах, чем подростки из крупных городов (коэффициент Гамма составил -0,130 при значимости 0,000) (табл. 4) [2].

Таблица 4

Социальные сети, в которых зарегистрированы обучающиеся, %

Социальные сети	Все обучающиеся	Обучающиеся 6–8-х классов	Обучающиеся 9–11-х классов
1. ВКонтакте	95,4	93,9	96,8
2. Instagram	73,9	67,3	80,0
3. Facebook	33,7	29,3	37,9
4. Одноклассники	29,5	32,1	27,1
5. Twitter	27,7	20,8	34,1
6. Не зарегистрированы в социальных сетях	2,1	2,7	1,5
7. Затрудняюсь ответить	0,3	0,3	0,3
8. Другое	0,8	0,9	0,7

Причинами «ухода» в соцсети могут являться стремление подростков снизить эмоциональную зависимость от родителей, недостаточный уровень развития родительской компетентности в формировании благоприятных детско-родительских отношений.

В настоящее время достаточно актуальным направлением 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 (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 то же время достаточно конкретен, связан с реальным опытом участников. Работу 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 аудиоматериалов, интерактивных технологий и пр.) позволяет вовлечь слушателей, в разной степени склонных использовать аудиальный, визуальный или кинестетический каналы восприятия[6].

Использование различных методов и практико-ориентированных видов деятельности (деловые и ролевые игры, тренинги, работа с литературой и интернет-ресурсами, работа с глоссарием по изучаемой тематике, написание 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

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

к системе образования. Родители нуждаются в знаниях и навыках, которые помогут выбрать подходящий детский сад, школу, кружок или секцию; 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 ограниченны 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 сенситивности 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 реалистичной 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[7].

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

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

и обращаться к помощи коллег или смежных специалистов в случаях, когда это необходимо.

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» (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; умений целеполагания и планирования;
- коммуникативных навыков и эмоционального интеллекта: безопасной самопрезентации и взаимодействия, разрешения конфликтов;
- умения критически анализировать информацию и содержание информационных сообщений, особенно сообщений, призывающих к каким-либо действиям; 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[8]

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

[8] 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.

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 возможностей 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. В течение некоторого времени сопровождать ребенка в его путешествиях по Сети для того, чтобы убедиться, что ребенок соблюдает соглашения.
6. Для безопасного поведения в Интернете повышать свою информационную грамотность и грамотность ребенка.
7. Другое __ _____

Ребенок должен:

- Обращаться к своим родителям, чтобы узнать правила пользования Интернетом: безопасные сайты, время 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 своей школы, личные и семейные фотографии.
- Всегда немедленно сообщать родителям, если увидит или получит в Интернете что-либо тревожащее его или угрожающее ему; сюда входят сообщения электронной почты, сайты или даже содержимое обычной почты от друзей в Интернете.
- Никогда не соглашаться лично встретиться с человеком, с которым он 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 и пароль от почтового ящика. Никому, кроме родителей, эти сведения сообщать категорически нельзя.
- Другое_____

Дата

Родитель_____
Ребенок_____

Примерная структура серии семинаров для педагогов (родителей) для развития цифровой компетентности обучающихся, основанная на материалах методических пособий «Фонда Развития Интернет»[9]

Модуль 1. Технические аспекты использования Интернета
Тема 1. Цифровой образ жизни
Тема 2. Безопасное подключение
Тема 3. Надежные пароли
Тема 4. Вирусы в Интернете
Тема 5. Искусственный интеллект
Модуль 2. Информация в Интернете
Тема 1. Информация в Интернете: возможности и риски
Тема 2. Возможности поиска в Интернете
Тема 3. Достоверность информации в Интернете
Тема 4. Авторское право в Интернете
Модуль 3. Коммуникация в Интернете
Тема 1. Самопрезентация
Тема 2. Социальные сети
Тема 3. Друзья или френды
Тема 4. Агрессия в Интернете

[9] Солдатова Г., Зотова Е., Лебешева М., Шляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. – М.: Google, 2013. – 165 с.

Модуль 4. Цифровое потребление
Тема 1. Цифровое потребление
Тема 2. Реклама в Интернете
Тема 3. Мошенничество в Сети
Тема 4. Люди, которые играют в игры

Таблица 5

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

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
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

Методические рекомендации по применению технологических средств обеспечения информационной безопасности

Согласно исследованию «Особенности обеспечения информационной безопасности обучающихся в образовательной организации и за ее пределами», которое проводил Институт развития образования в 2018 году, определены актуальные угрозы безопасности детей в Интернете:

- контакты с сетевыми мошенниками;
- вредоносные программы;
- угроза безопасности персональных данных;
- виртуальный террор;
- пропаганда жестокости, экстремизма и нетерпимости;
- «киберсуицид»;
- кибербуллинг;
- информация, причиняющая вред здоровью и развитию детей и др.

Как определить, что вы общаетесь с мошенником?

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».

Блокировка «нежелательных собеседников»
на персональном компьютере в социальных сетях

Facebook

web.facebook.com

1. Зайдите в свой аккаунт[10].
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.

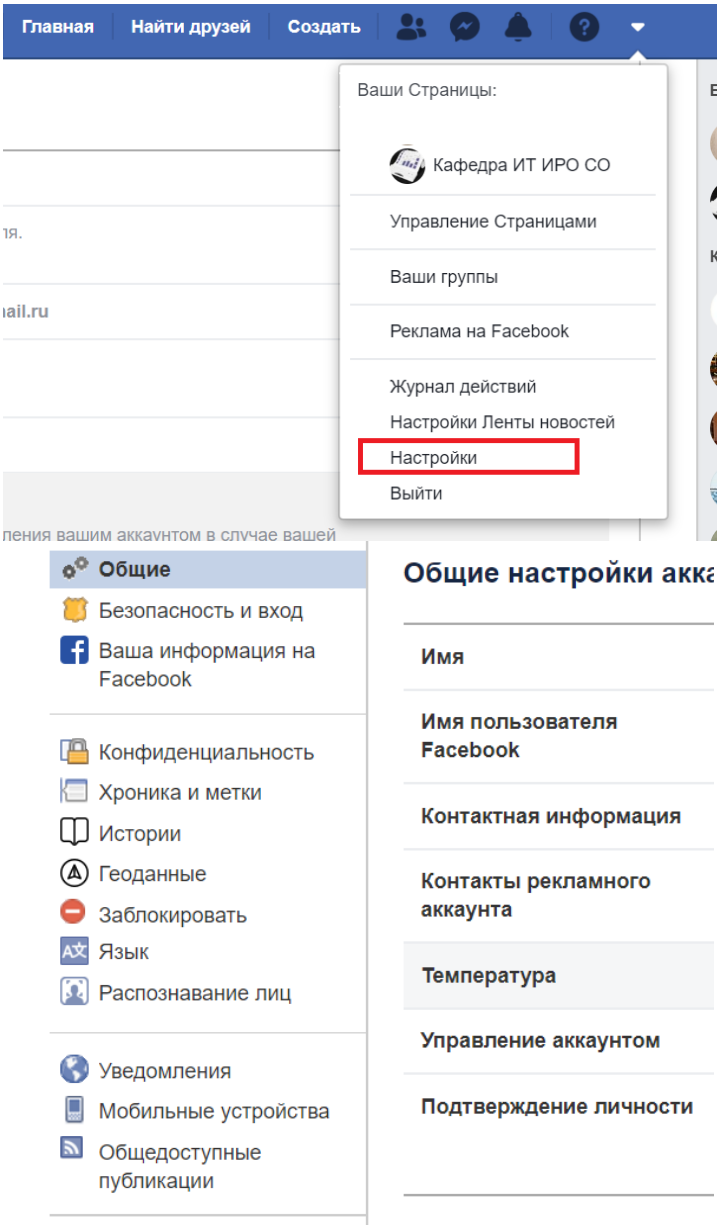


Рис. 2

[10] 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[11] и браузеров[12], 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[13]. 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. Это поможет, если вы заходили в соцсеть с компьютера другого человека и забыли выйти. Если вы увидите в списке подключений подозрительную сессию[14], которая не имеет к вам никакого отношения, можно ее закрыть и, если нужно, поменять пароль.

---

[11] 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)

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

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

[14] Промежуток работы на компьютере

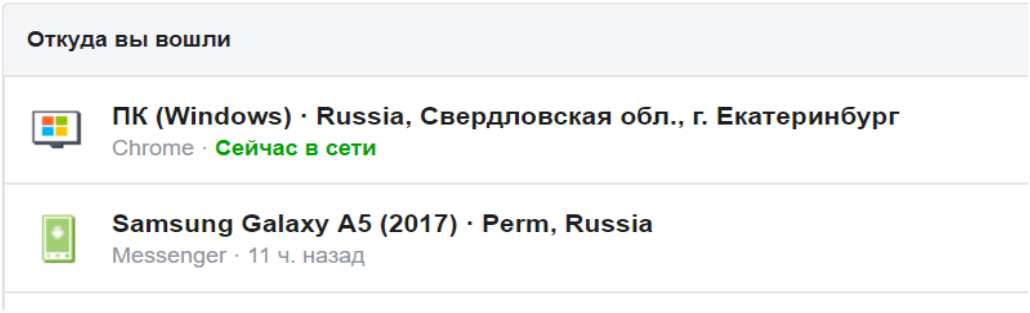


Рис. 3

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».

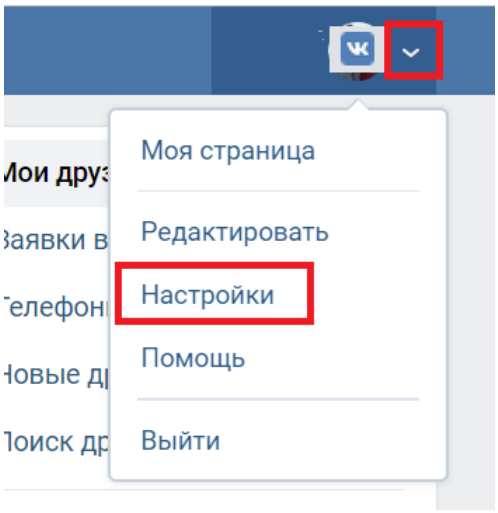


Рис. 4

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.

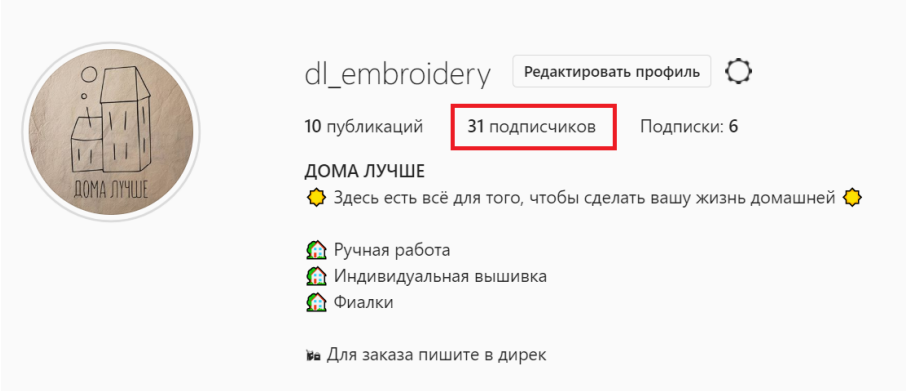


Рис. 5

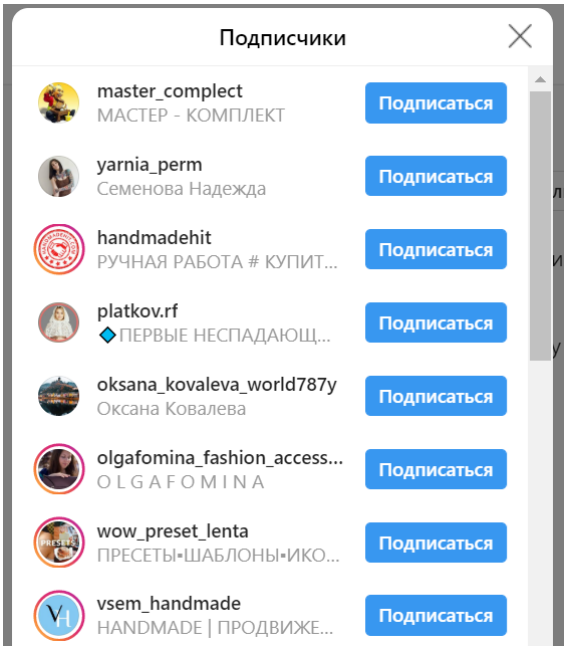


Рис. 6

3. Выберите того пользователя, которого вы желаете заблокировать. Нажмите меню справа от пользователя.

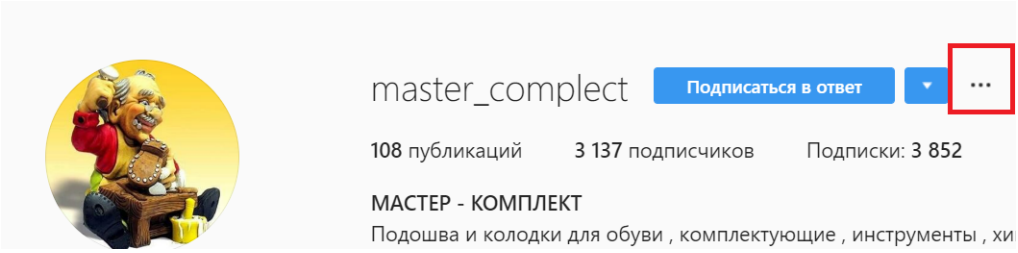


Рис. 7

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

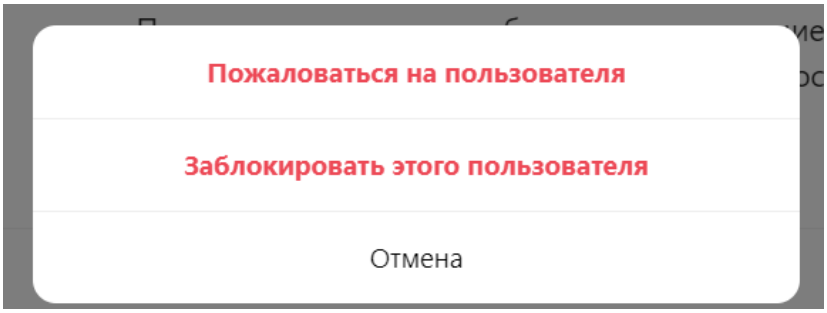


Рис. 8

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.

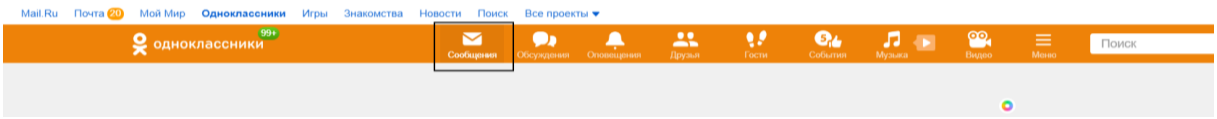


Рис. 9

2. Нажимаете на фото отправителя.

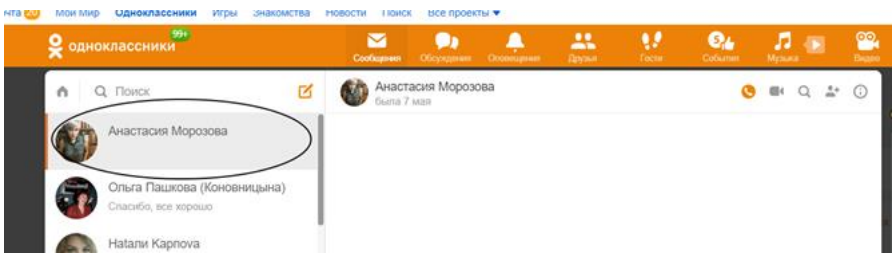


Рис. 10

3. Справа вверху нажимаете на «Настройки».

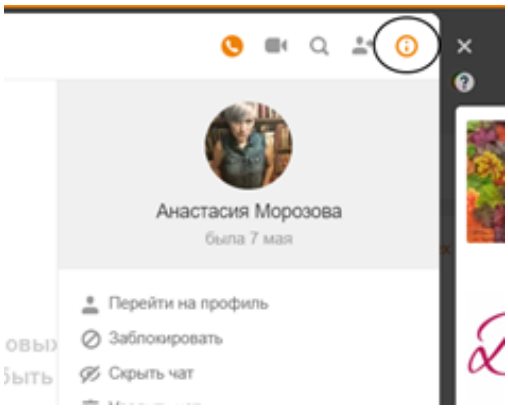


Рис. 11

4. Выбираете «Заблокировать».

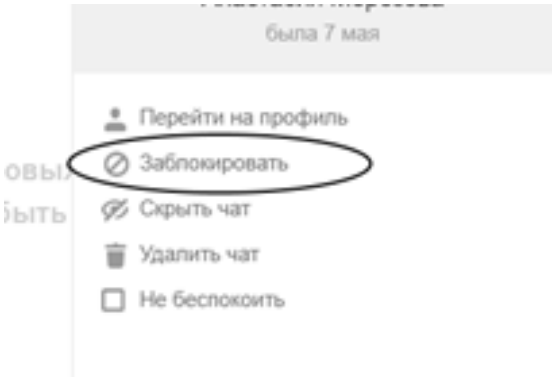
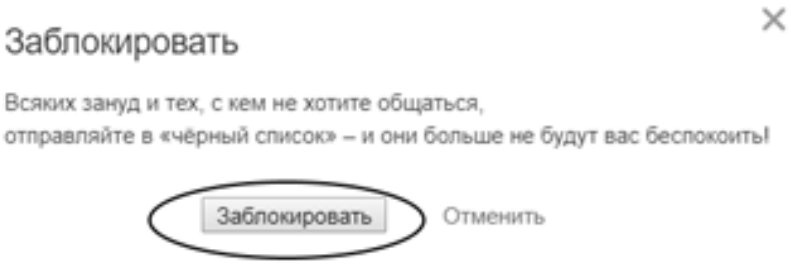


Рис. 12

5. Подтверждаете свое действие.



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

1. Переходите в раздел «Гости».

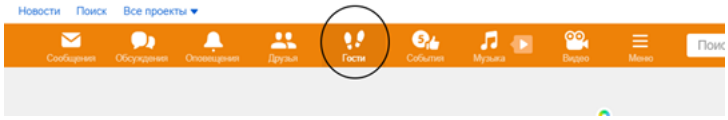


Рис. 13

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

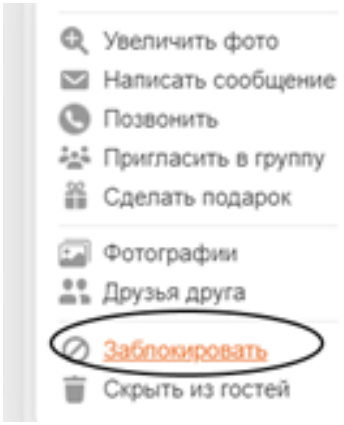


Рис. 14

4. Подтверждаете свое действие.

Как заблокировать друга в одноклассниках

1. Переходим в раздел «Друзья».

Рис. 15

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

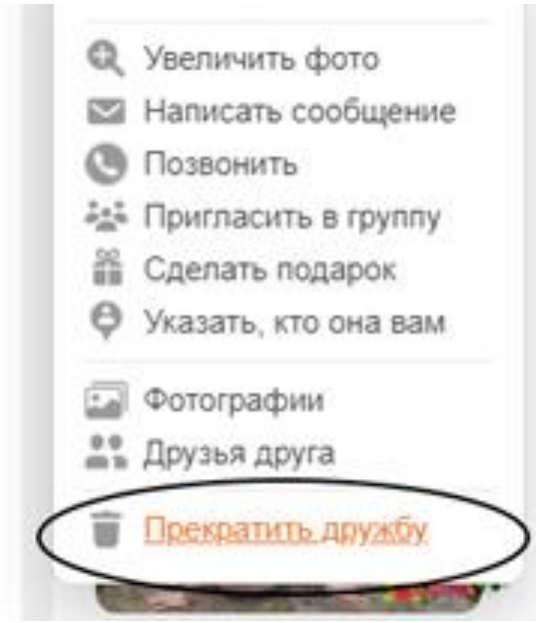


Рис. 16

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[15].

В задачи антивирусного ПО входит обнаружение шпионских программ, вирусов, фишинговых[16] ресурсов, опасных серверов и подозрительного трафика.

Лучшие бесплатные антивирусы по версии журнала PC-magazine[17] представлены на рисунке.

Рис. 17

Антивирус Kaspersky

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

---

[15] ru.wikipedia.org

[16] 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

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

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[18], 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

IM-антивирус обеспечивает безопасность работы с IM-клиентами[19], такими как WhatsApp, Viber, Facebook Messenger, Skype, ICQ, Google Hangouts.

Алгоритм установки антивируса:

1. Зайдите на сайт kaspersky.ru.
2. Выберите в меню продукт для скачивания.

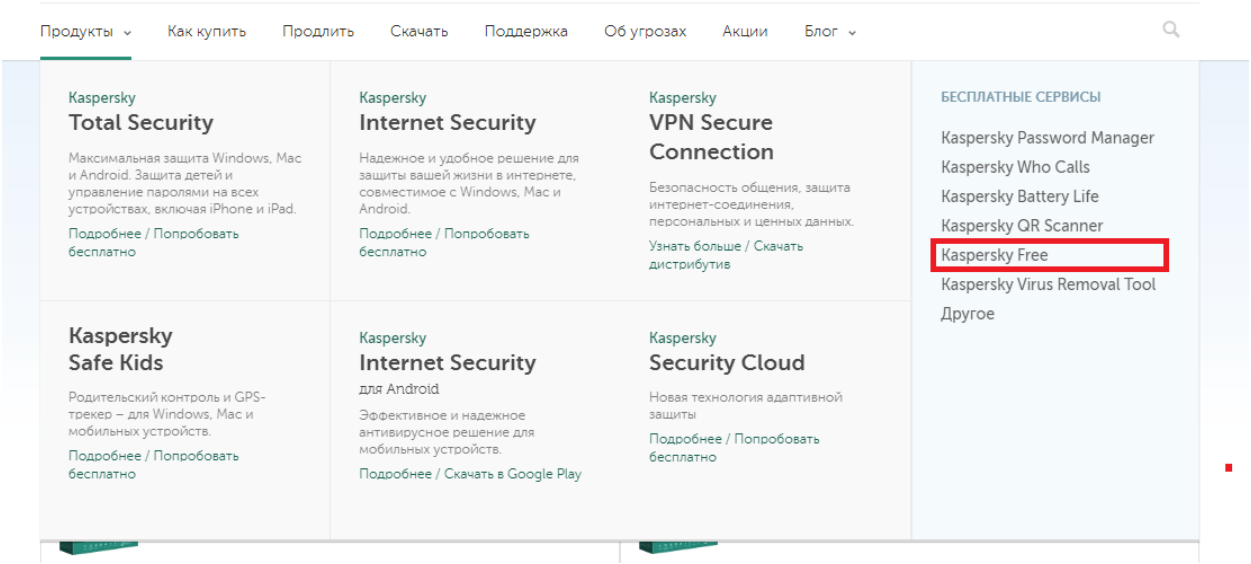


Рис. 18

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

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

3. Нажмите кнопку «Скачать».

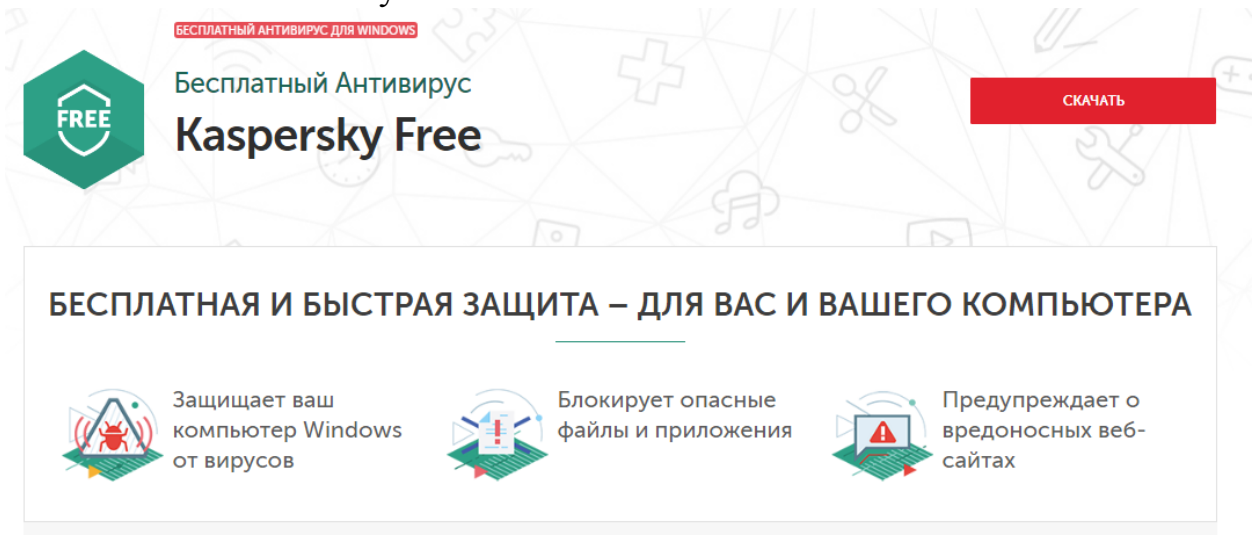


Рис. 19

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[20]. Приложение на устройстве ребенка помогает контролировать его онлайн-активность, позволяет родителям просматривать отчеты и менять настройки.

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[21].

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 kaspersky.ru/safe-kids.

Рис. 20

[20] my.kaspersky.com/

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

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.

Брандмауэр и безопасность сети – данный раздел предоставляет информацию о конфигурации брандмауэра[22] 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. 21

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.

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

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

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[23], историю посещенных сайтов, cookies[24] (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

[23] 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)

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

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.
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? Компания Gemalto Russia, опросив более 1300 пользователей мобильных устройств, предоставила данные о том, как потребители используют свои мобильные устройства и что делают для обеспечения их безопасности.

Как используется мобильное устройство?

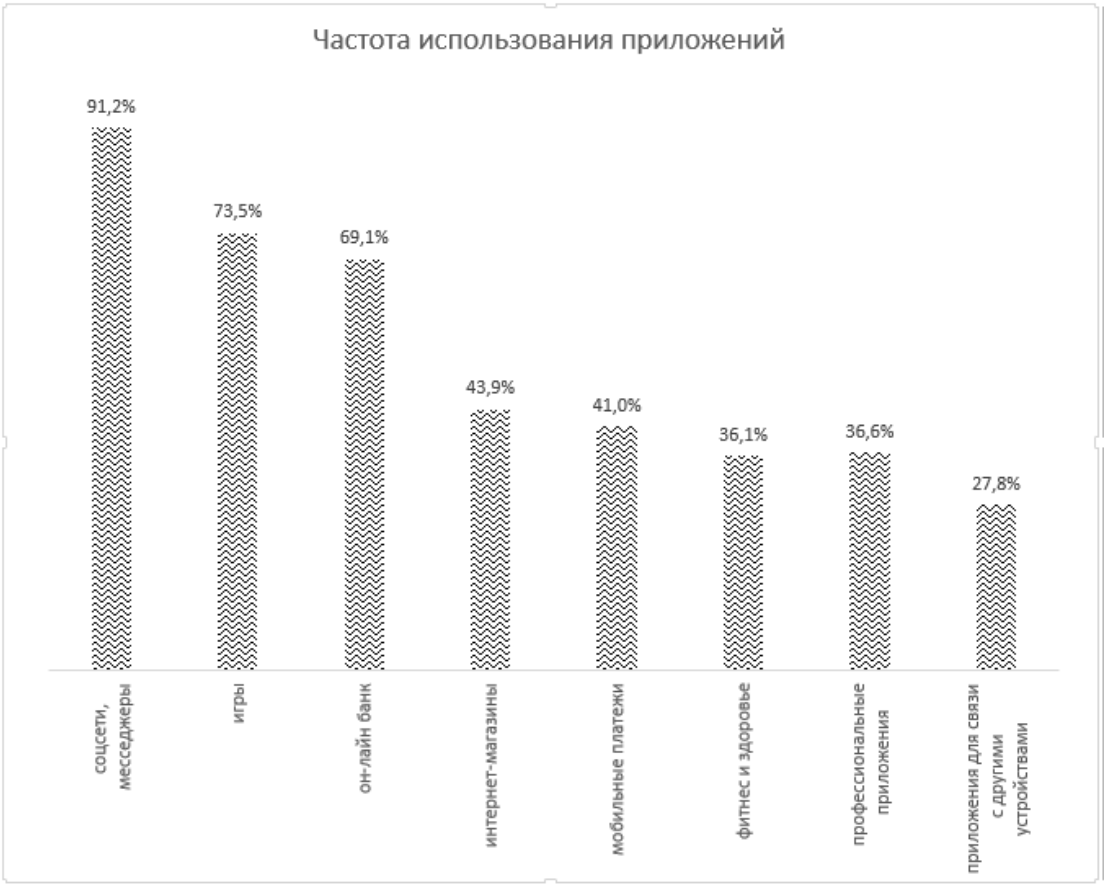


Рис. 22

Какие опасения существуют при использовании мобильного устройства?

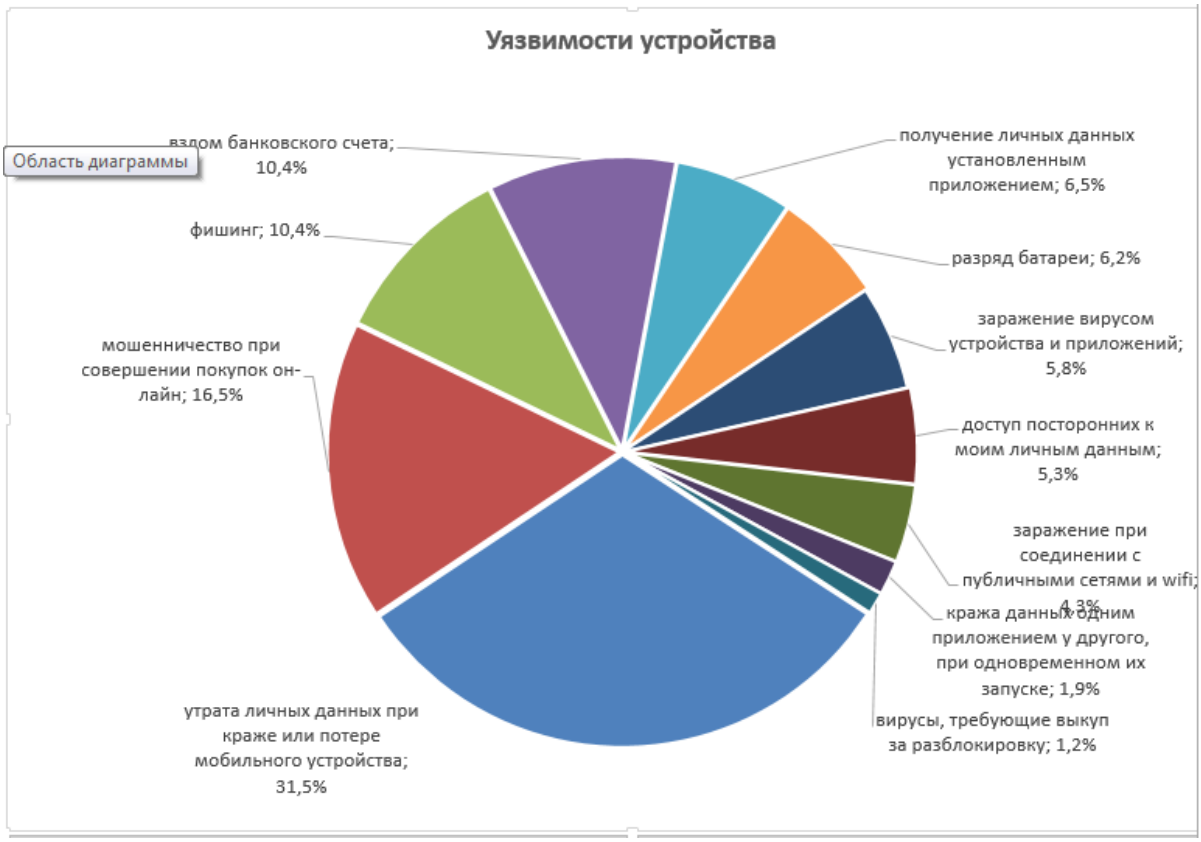


Рис. 23

Какие меры чаще всего принимаются для защиты мобильного устройства?

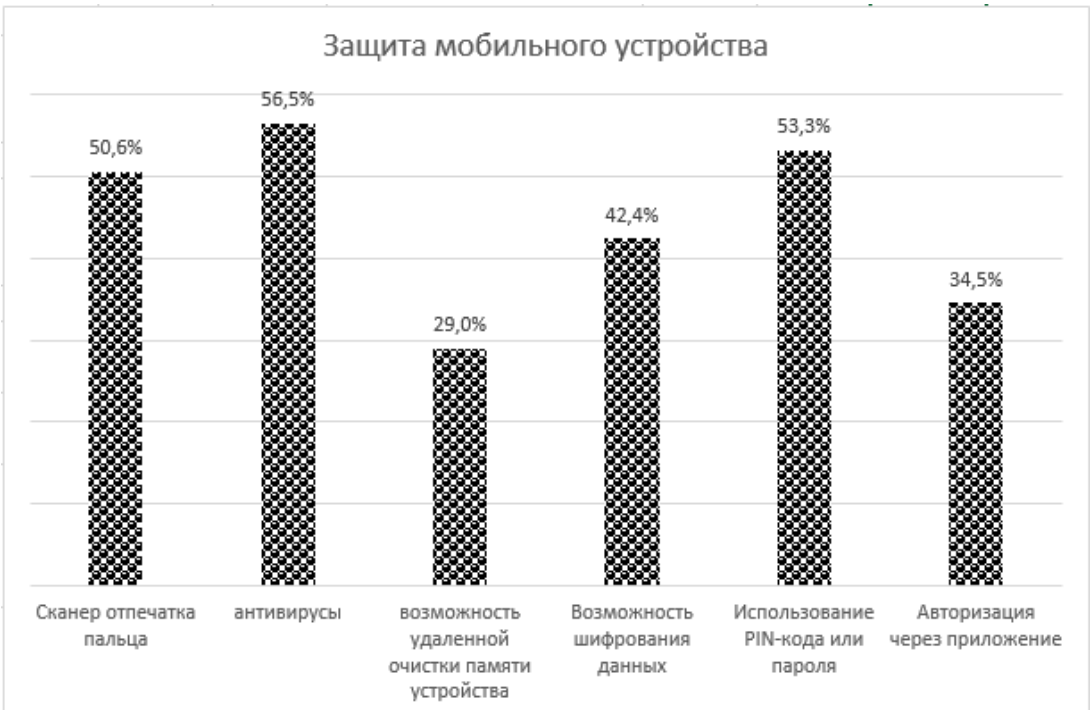


Рис. 24

Эти результаты позволяют получить понимание того, что требуется для того, чтобы обеспечить информационную безопасность своего мобильного устройства.

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. 25

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.

4. 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.

5. 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.

Цифровое детство – реальность сегодняшнего дня

Современные подростки отличаются от предыдущего поколения тем, что практически у каждого из них есть друг, с которым никогда не скучно. И этот друг – смартфон.

К 10 годам практически каждый ребенок (91 %), живущий в крупном городе России, уже имеет свой собственный гаджет. Даже у 25 % детей в 3–4 года есть какое-либо устройство.

Современные исследования показывают удивительные результаты: 78 % школьников признались, что вообще не выпускают из рук смартфоны в течение дня.

Во время одного из исследований школьникам задавали вопросы про гаджеты. На вопрос «Вы берете с собой телефон повсюду (в туалет, ванную, постель)?» 70 процентов ответили положительно. «Если вы забыли телефон дома, вы испытываете дискомфорт?» – 77 процентов ответили положительно. «Сколько времени занимает у вас работа с гаджетом?» – 44,5 процента выбрали вариант «весь день», 35 процентов – «более 3–4 часов». «Есть ли вы в социальных сетях?»

– 98 процентов ответили «да». «Почему именно этот телефон вы выбрали?» – ответ «наличие Интернета» выбрали 88 процентов.

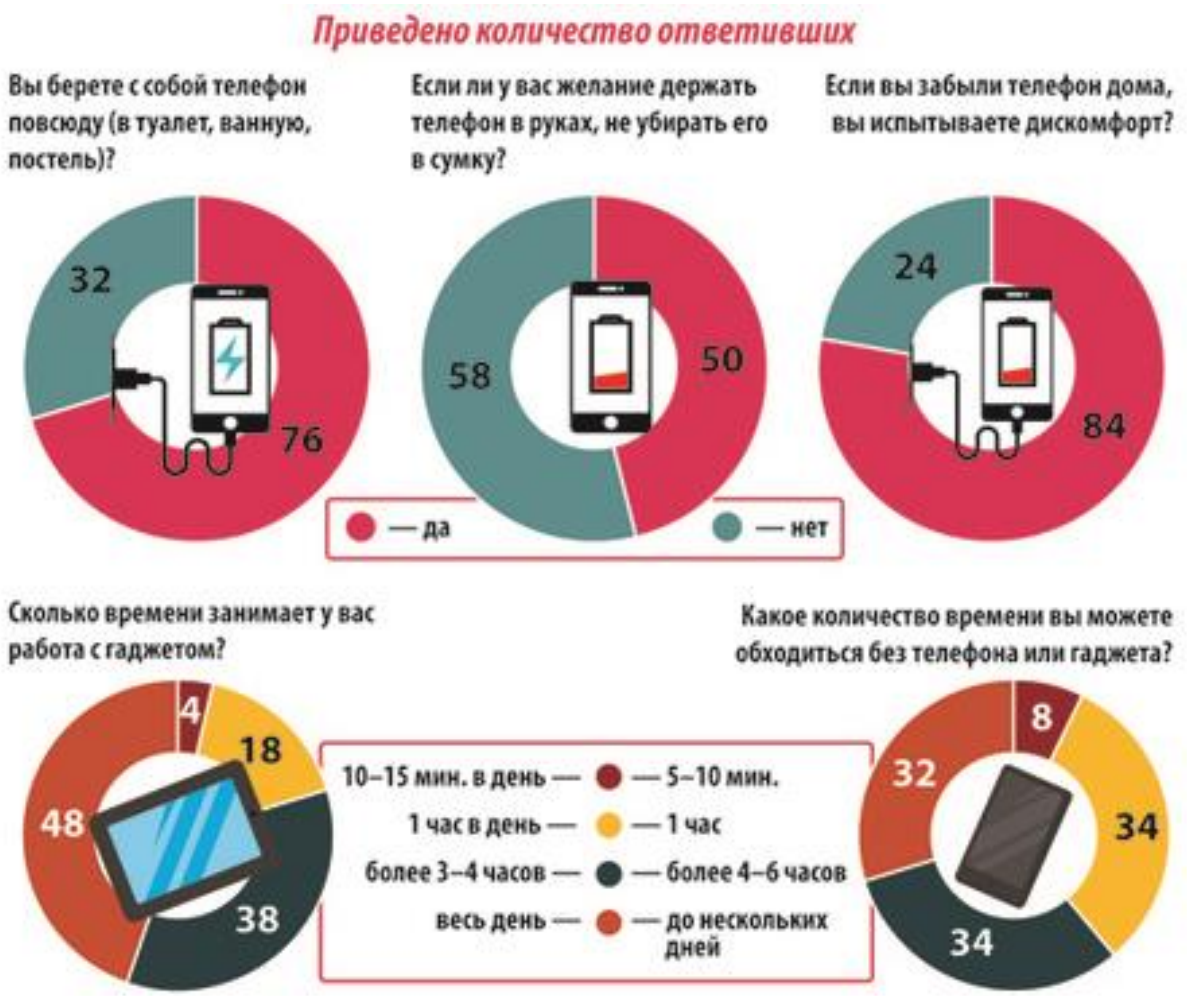


Рис. 26

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?

Таблица 6

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	Бесплатно 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	Приложение имеет бесплатную и платную версии: 94,8–149 рублей в месяц и 990–1490 рублей в год. **Поддерживаемые платформы**: Android, iOS

Таблица 7

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	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.		Бесплатное, имеет платный контент стоимостью от 99 до 999 рублей в зависимости от содержания. **Поддерживаемые платформы**: Android

Приложение	Функционал	Достоинства	Недостатки	Цена
	универсально в сравнении с другими, которые мы включили в обзор, и просто в использовании. Кроме того, оно может работать с гаджетами – умными браслетами и часами	Можно следить за работой ребенка в Сети и получать отчеты за день, неделю или месяц. 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.

И напоследок, никто не отменял «банальную» антивирусную защиту. Предлагаем небольшой рейтинг бесплатных мобильных антивирусных программ.

1. Antiy AVL

Антивирус обнаруживает 99,7 % угроз в режиме реального времени.

Дополнительные функции

- Черный список и блокировка входящих звонков с неизвестных номеров
- Защита от опасных сайтов и фишинга

2. Bitdefender Mobile Security & Antivirus

Антивирус обнаруживает 99,9 % угроз в режиме реального времени.

Дополнительные функции

- Антивор: удаленная блокировка, очистка и поиск мобильного устройства
- Защита от опасных сайтов и фишинга

3. Cheetah CM Security

Антивирус обнаруживает 99,8 % угроз в режиме реального времени.

Дополнительные функции

- Антивор: удаленная блокировка, очистка и поиск мобильного устройства
- Черный список и блокировка входящих звонков с неизвестных номеров
- Защита от опасных сайтов и фишинга

4. Kaspersky Antivirus & Security

Антивирус обнаруживает 99,9 % угроз в режиме реального времени.

Дополнительные функции

- Антивор: удаленная блокировка, очистка и поиск мобильного устройства
- Черный список и блокировка входящих звонков с неизвестных номеров
- Спам-фильтр для сообщений и почты
- Защита от опасных сайтов и фишинга

5. Norton Security & Antivirus

Антивирус обнаруживает 100 % угроз в режиме реального времени.

Дополнительные функции

- Антивор: удаленная блокировка, очистка и поиск мобильного устройства
- Черный список и блокировка входящих звонков с неизвестных номеров
- Защита от опасных сайтов и фишинга

6. ONE App MAX

Антивирус обнаруживает 99,8 % угроз в режиме реального времени.

Дополнительные функции: отсутствуют.

7. Sophos Antivirus & Security

Антивирус обнаруживает 100 % угроз в режиме реального времени.

Дополнительные функции

- Антивор: удаленная блокировка, очистка и поиск мобильного устройства
- Черный список и блокировка входящих звонков с неизвестных номеров
- Спам-фильтр для сообщений и почты
- Защита от опасных сайтов и фишинга
- Родительский контроль

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

Библиографический список

1. **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. – Текст : непосредственный.

2. Деятельность подростков в сети Интернет: динамика, риски, реакция родителей : отчет по итогам социологического исследования / Министерство общего и профессионального образования Свердловской области; Государственное автономное образовательное учреждение дополнительного профессионального образования Свердловской области «Институт развития образования». – Екатеринбург: ГАОУ ДПО СО «ИРО», 2019. – Текст : непосредственный.

3. **Российская Федерация. Законы.** Концепция информационной безопасности детей : распоряжение Правительства Российской Федерации № 2471-р [от 2 декабря 2015 г.]. – Текст : электронный. – URL: static.government.ru/media/files/mPbAMyJ29uSPhL3p20168GA6hv3CtBxD.pdf/.

4. **Российская Федерация. Законы.** О защите детей от информации, причиняющей вред их здоровью и развитию : федеральный закон № 436-ФЗ [от 29 декабря 2010 г.] . – Текст : электронный. – URL: ivo.garant.ru/#/document/77680092/paragraph/1:0.

5. Особенности обеспечения информационной безопасности обучающихся в образовательной организации и за ее пределами : отчет по итогам социологического исследования / Министерство общего и профессионального образования Свердловской области; Государственное автономное образовательное учреждение дополнительного профессионального образования Свердловской области «Институт развития образования». – Екатеринбург: ГАОУ ДПО СО «ИРО», 2018. – Текст : непосредственный.

6. **Солдатова Г., Зотова Е., Лебешева М., Шляпников В.** Интернет: возможности, компетенции, безопасность : методическое пособие для работников системы общего образования / Г. Солдатова, Е. Зотова, М. Лебешева, В. Шляпников. – Москва: Google, 2013. – 165 с. – Текст : непосредственный.

7. **Солдатова Г., Зотова Е., Лебешева М., Шляпников В.** Интернет: возможности, компетенции, безопасность : методическое пособие для работников системы общего образования / Г. Солдатова, Е. Зотова, М. Лебешева, В. Шляпников. – Москва: Google, 2013. 137 с. – Текст : непосредственный.

8. Социальные сети: возможности и риски для обучения и воспитания : методические рекомендации / Министерство общего и профессионального образования Свердловской области; Государственное автономное образовательное учреждение дополнительного профессионального образования Свердловской области «Институт развития образования»; Кафедра информационных технологий; авт.-сост. Н. В. Шпарута, Г. А. Бутакова. – Екатеринбург: ГАОУ ДПО СО «ИРО», 2017. – Текст : непосредственный.

9. Как защитить себя в Интернете. – Текст : электронный. – URL: invlab.ru/texnologii/kak-zashhitit-sebya-v-internete/.

10. Справочный центр. – Текст : электронный. – URL: help.instagram.com.

11. Все, что нужно знать о настройках безопасности Facebook. – Текст : электронный. – URL: kaspersky.ru/blog/facebook-security-settings/13480/.