№	Раздел/подраздел	Формат представления материалов	Содержание материалов
1.	Локальные нормативные акты в сфере обеспечения информационной безопасности	Копии документов в формате ***PDF**	Положение об обработке и защите персональных данных обучающихся и родителей № 23 от 31.03.2014г.
2.	Нормативное регулирование	**Ссылки или копии *PDF**	**Актуальные сведения об федеральных и региональных законах, письмах органов власти и другие нормативно-правовые документы, регламентирующие обеспечение информационной безопасности несовершеннолетних:** 1. Федеральный закон РФ от 27.07.2006 г. № 152 — ФЗ «О персональных данных» 2. Федеральный закон РФ от 28.12.2010 г. № 390 — ФЗ «О безопасности» 3. Федеральный закон РФ от 29.12.2010 г. № 436 — ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» 4. Указ Президента РФ от 04.03.2013 г. № 183 «О рассмотрении общественных инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса «Российская общественная инициатива» В состав законодательства по обеспечению информационной безопасности включаются федеральные законы, подзаконные нормативные правовые акты федеральных органов исполнительной власти, законы и подзаконные нормативные правовые акты субъектов Российской Федерации. К числу наиболее значимых нормативных правовые актов в области обеспечения информационной безопасности относятся следующие законы и подзаконные акты. Конституция Российской Федерации содержит нормы, которые определяют правовые основы информационной безопасности: основные положения правового статуса субъектов

			информационных отношений, принципы информационной безопасности (законности, уважения прав, баланс интересов личности, общества и государства), конституционный статус государственных органов, обеспечивающих информационную безопасность и др. Например, к таким положениям относятся нормы, которые устанавливают право каждого субъекта свободно искать, получать, передавать, производить и распространять информацию любым законным способом (п.4.ст. 29). Это конституционное право, устанавливающее возможность удовлетворения интересов личности и общества сбалансировано необходимостью их ограничения федеральным законом в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (п.3.ст.55). Конституция Российской Федерации устанавливает запрет на доступ к информации о частной жизни и передачу сообщений по линиям телефонной связи (ст.23). Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности» (87)закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности. Закон определяет ключевые термины в области безопасности, которые применимы и для сферы информационной безопасности, принципы и систему безопасности, правовой статус и состав Совета Безопасности Российской Федерации. Федеральный закон от 27.07.2006, г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации»(88)фиксирует базовые нормы для всей системы информационного законодательства, в т.ч. правового обеспечения информационной безопасности. Они определяют основные термины и их определения, принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации (ст.3), классификацию информации по категориям доступа – общедоступную и ограниченного доступа (ст. 5), порядку ее предоставления или распространения (свободно распространяемую, обязательного предоставления или распространения, ограниченного распространения или запрещаемую для распространения

			вообще). Закон определяет базовые положения правового режима доступа к информации (ст.8) и его ограничения (ст.9), основные параметры правовых режимов распространения (ст.10) и документирования (ст.11) информации, информационных систем (ст.13), информационно-телекоммуникационных сетей (ст.15) и общие условия защиты информации (ст.16), информационных систем (ст.13) и использования информационных технологий, а также в общих чертах описывает ответственность за правонарушения в сфере информации, информационных технологий и защиты информации. Федеральный закон от 21 июня 1993 № 5485-1 «О государственной тайне», Федеральные законы от 29 июля 2004 № 98-ФЗ «О коммерческой тайне» и от 27.07.2006 г. № 152-ФЗ «О персональных данных» (89, 90, 91) устанавливают правовые режимы информации ограниченного доступа, в том числе, сведений, составляющих государственную и коммерческую тайну. Нормы названных законов на более конкретном уровне, чем норма ст.9 закона «Об информации» регулируют формирование условий правового режима доступа к сведениям конфиденциального характера, конкретизируют правовой статус субъектов отношений, возникающих по поводу тайн и персональных данных. Именно в названных законах содержатся основные запреты, ограничения и дозволения, которые составляют правовые основания для формулировок составов информационных правонарушений, направленных на интересы личности, общества и государства в области конфиденциальности информации. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (92).Нормы названного закона определяют правовой режим технологического обеспечения защиты информации в системе базовых законов информационного законодательства. В ст. 1 этого закона определена его цель – обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. В законе сформулированы функции электронной цифровой подписи: удостоверяющая, защитная и устанавливающая. Уголовный кодекс РФ вглаве 28 Кодекса предусматривает ответственность за совершение преступлений в сфере компьютерной информации (ст.272-275). Всего в тексте Кодекса содержится более 50 отдельных статей, устанавливающих уголовную ответственность за нарушение

			установленных запретов в информационной сфере. Трудовой кодекс РФ устанавливает правовой режим персональных данных работника, определяет общие требования по их обработке и защите, устанавливает сроки хранения таких данных и процедуру их использования. В случаях нарушения норм, регулирующих получение, обработку и защиту персональных данных работника, виновные лица привлекаются к дисциплинарной, материальной, административной, гражданско-правовой и уголовной ответственности. Трудовой кодекс РФ определяет норму об ответственности за разглашение отдельных видов тайн и персональных данных. КоАП РФ в главе 13 определяет административную ответственность за правонарушения в области связи и информации посвящена отдельная глава (ст. 13.1-13.24). В него включены еще более 90 статей, в которых определяется ответственность за совершение проступков информационного характера. Так, например, устанавливается ответственность за отказ в предоставлении гражданину информации (ст. 5.39), за сокрытие или искажение экологической информации (ст. 8.5), за незаконные действия по получению и (или) распространению информации, составляющей кредитную историю (ст. 5.53). Имеется также массив нормативных правовых актов подзаконного характера, состоящий из большого количества документов, регулирующих отдельные направления правового обеспечения информационной безопасности. Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»(93). В данном Указе устанавливается запрет подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну к информационно-телекоммуникационным сетям международного информационного обмена. В целях защиты информации государственные органы обязаны использовать только средства защиты информации, прошедшие сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данных требований Указа в полной мере должно обеспечить защиту

			информации, составляющей государственную тайну. Приказом ФСО России от 07.08.2009 N 487утвержденоПоложение о сегменте информационно-телекоммуникационной сети Интернет(94) для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Эксплуатацию, поддержание и развитие сегмента информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации обеспечивает Служба специальной связи и информации ФСО России. В соответствии с названным нормативным правовым актом Сегмент сети Интернет – это находящаяся в ведении (эксплуатации) Федеральной службы охраны Российской Федерации (далее именуется – оператор сегмента сети Интернет) часть информационно-телекоммуникационной сети, связывающей информационные системы, информационно-телекоммуникационные сети различных государств посредством сетевых адресов информационно-телекоммуникационной сети Интернет (далее именуется – сеть Интернет). Сегмент сети Интернет предназначен для обеспечения размещения информации о деятельности Администрации Президента Российской Федерации, Аппарата Совета Федерации Федерального Собрания Российской Федерации, Аппарата Государственной Думы Федерального Собрания Российской Федерации, Аппарата Правительства Российской Федерации, аппаратов Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, Высшего Арбитражного Суда Российской Федерации, Генеральной прокуратуры Российской Федерации и Следственного комитета при прокуратуре Российской Федерации, федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, а также для доступа к сети Интернет должностных лиц указанных государственных органов (далее именуются – пользователи сегмента сети Интернет). Функционирование сегмента сети Интернет обеспечивается путем применения стандартных протоколов сети Интернет и регламентов обмена информацией в порядке, определяемом оператором сегмента сети Интернет.

			В российском правовом пространстве длительное время в обороте используется «служебная информация ограниченного распространения» о деятельности органов государственной власти, которая нередко упоминается в нормативных правовых актах как «служебная тайна». Постановление Правительства РФ № 1233 от 3 ноября 1994 г. «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах государственной власти» (95) определяется правовое положение информации ограниченного доступа, несмотря на то, что п.п.1 и 4 ст.9 ФЗ «Об информации» ограничение доступа к информации и, в частности, отнесение информации к сведениям, составляющим служебную тайну, устанавливаются исключительно федеральными законами. Явное несовершенство информационного законодательства и практики его применения отрицательно влияет на состояние правовой защиты интересов субъектов правоотношений. Пробел в нормативных правовых актах, устанавливающих оборот информации служебного характера, не позволяет установить запрет либо ограничения на ее использование, а вместе с этим создает ситуацию невозможности установить административную и / или уголовную ответственность за нарушения порядка распространения этой важной формы информации.
3.	Педагогическим работникам	Текст на странице сайта Копии документов в формате *PDF	Методические рекомендации для педагогических работников Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 No 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»). В Интернете, как и в реальной жизни, учащихся подстерегают опасности: доступность нежелательного контента в социальных сетях, обман и вымогательство денег, платные СМС на короткие номера, пропаганда насилия и экстремизма, игромания и интернет-зависимость, склонение к суициду и т.п. Интернет-зависимость — это навязчивое желание подключиться к Интернету и болезненная

			неспособность вовремя отключиться от Интернета. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. В частности, некоторые учащиеся настолько увлекаются виртуальным пространством, что начинают предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Видами интернет-зависимости являются навязчивый веб-серфинг, пристрастие к виртуальному общению и виртуальным знакомствам (большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети), игровая зависимость — навязчивое увлечение компьютерными играми по сети. Задача педагогов в связи с имеющимися рисками состоит в том, чтобы указать на эти риски, предостеречь от необдуманных поступков, сформировать у учащихся навыки критического отношения к получаемой в Интернете информации, воспитать культуру безопасного использования Интернет. В качестве возможного варианта предоставления учащимся соответствующих знаний может быть использована учебная программа «Интернет: возможности, компетенции, безопасность», разработанной специалистами факультета психологии МГУ им. М.В. Ломоносова, Федерального института развития образования и Фонда Развития Интернет, рекомендованная Министерством образования и науки РФ (http://detionline.com – главная страница, http://detionline.com/internet-project/about http://detionline.com/assets/files/research/BookTheorye.pdf теория,http://detionline.com/assets/files/research/Book_Praktikum.pdf — практика). Содержание программы направлено на обучение учащихся полезному и безопасному использованию сети Интернет и социальных сетей, обучению критической оценке онлайн контента и навыкам сетевой коммуникации. Авторами программы разработано методическое пособие для преподавателей и практикумы для проведения уроков, а также запущен интернет-ресурс «Разбираем Интернет» (www.razbiraeminternet.ru). На этом сайте в игровой форме представлены мультимедийные средства обучения для детей и подростков, надо рекомендовать обучающимся посещать этот сайт. Содержательная часть и объём учебного курса может определяться индивидуально, в зависимости от потребностей конкретной общеобразовательной организации и учащихся. Обучение навыкам безопасного и эффективного использования интернет-ресурсов возможно в

			рамках учебного курса «Основы безопасности жизнедеятельности» и в рамках программ факультативов, кружков, элективных курсов, а также индивидуальных учебных планов, реализуемых образовательными организациями. Материалы бесплатны и доступны для скачивания www.razbiraeminternet.ru/teacher. Академией повышения квалификации и профессиональной переподготовки работников образования (г.Москва) разработан учебно-методический комплект «Здоровье и безопасность детей в мире компьютерных технологий и Интернет». УМК разработан с учетом потребностей образовательных организаций в области безопасной работы в Интернет и ориентирован на руководителей, методистов, педагогов, заинтересованных в повышении своей компетентности в области безопасного применения ИКТ. Методическое приложение к программе можно использовать при организации просветительской работы с родителями и учащимися.https://edu.tatar.ru/upload/images/files/children_health_and_care_in_it.pdf Рекомендуется провести анкетирование обучающихся и родителей по вопросам безопасного использования сети Интернет. Вопросы для анкетирования учащихся и родителей представлены на сайте «Детионлайн» http://detionline.com/internet-project/competence-research. При работе с младшими школьниками целесообразно использовать игровые методы, в том числе и Интернет — игру «Прогулка через Дикий Интернет Лес» (http://www.wildwebwoods.org/popup.php?lang=ru), посвященную вопросам обеспечения безопасности в Интернете. Интернет-ресурсы для педагогических работников: http://www.fid.su/projects/deti-v-internete сайт Фонда Развития Интернет. http://www.ligainternet.ru/ Лига безопасного Интернета. http://ppt4web.ru/informatika/bezopasnyjj-internet.html презентации о безопасном Интернете. http://www.microsoft.com/ru-ru/security/default.aspx сайт Центра безопасности Майкрософт. http://festival.1september.ru/articles/612789/ Материал разработан для учащихся 9-11 классов, но может модифицироваться и для учащихся среднего звена школы. http://www.nachalka.com/node/950 Видео «Развлечение и безопасность в Интернете».

			http://i-deti.org/ портал «Безопасный инет для детей», ресурсы, рекомендации, комиксы. http://сетевичок.рф/ сайт для детей — обучение и онлайн-консультирование по вопросам кибербезопасности сетевой безопасности. http://www.igra-internet.ru/ — онлайн интернет-игра «Изучи Интернет – управляй им». http://www.safe-internet.ru/ — сайт Ростелеком «Безопасноть детей в Интернете, библиотека с материалами, памятками, рекомендациями по возрастам. Информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников. http://www.ligainternet.ru/news/ мероприятия Лиги безопасного интернета. Лига безопасного интернета — крупнейшая и наиболее авторитетная в России организация, созданная для противодействия распространению опасного контента во всемирной сети. Лига безопасного интернета была учреждена в 2011 году при поддержке Минкомсвязи РФ, МВД РФ, Комитета Госдумы РФ по вопросам семьи женщин и детей. Попечительский совет Лиги возглавляет помощник Президента Российской Федерации Игорь Щеголев. Мероприятия проекта «Сетевичок». Проект представляет собой группу онлайн-мероприятий: Международный квест по цифровой грамотности «Сетевичок», ориентированный на детей и подростков. Национальная премия за заслуги компаний и организаций в сфере информационного контента для детей, подростков и молодежи «Премия Сетевичок». Всероссийское исследование детей и подростков «Образ жизни российских подростков в сети». Конференция по формированию детского информационного пространства «Сетевичок». Видеоматериалы для проведения уроков по вопросам защиты персональных данных детей 9-11, 12-13 лет http://pd.rkn.gov.ru/multimedia/video114.htm
4.	Обучающимся	Текст на странице сайта	ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ НЕЛЬЗЯ 1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей);

			2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя; 3. Грубить, придираться, оказывать давление - вести себя невежливо и агрессивно; 4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей; 5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь. ОСТОРОЖНО 1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам; 2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха; 3. Незаконное копирование файлов в Интернете - воровство; 4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут; 5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах. МОЖНО 1. Уважай других пользователей; 2. Пользуешься Интернет-источником - делай ссылку на него; 3. Открывай только те ссылки, в которых уверен; 4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут; 5. Пройди обучение на сайте "Сетевичок" и получи паспорт цифрового гражданина! ИНФОРМАЦИОННАЯ ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ С каждым годом молодежи в интернете становиться больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети. Компьютерные вирусы

			Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет. Методы защиты от вредоносных программ: 1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ; 2. Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его; 3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере; 4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз; 5. Ограничь физический доступ к компьютеру для посторонних лиц; 6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников; 7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их. Сети WI-FI Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд "WECA", что обозначало словосочетание "WirelessFidelity", который переводится как "беспроводная точность". До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура "Wi-Fi". Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает "высокая точность". Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются

			безопасными. Советы по безопасности работы в общедоступных сетях Wi-fi: 1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера; 2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство; 3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе; 4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту; 5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://"; 6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi автоматически". Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия. Социальные сети Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями. Основные советы по безопасности в социальных сетях: 1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей; 2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы; 3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить; 4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

			5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение; 6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8; 7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу. Электронные деньги Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги. Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах. В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной. Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам). Основные советы по безопасной работе с электронными деньгами: 1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства; 2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля; 3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;; 4. Не вводи свои личные данные на сайтах, которым не доверяешь. Электронная почта

			Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы. Основные советы по безопасной работе с электронной почтой: 1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге; 2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный_фанат@" или "рок2013" вместо "тема13"; 3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS; 4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль; 5. Если есть возможность написать самому свой личный вопрос, используй эту возможность; 6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах; 7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы; 8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти". Кибербуллинг или виртуальное издевательство Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. Основные советы по борьбе с кибербуллингом: 1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт; 2. Управляй своей киберрепутацией; 3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом; 4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и

			сохраняет их. Удалить их будет крайне затруднительно; 5. Соблюдай свою виртуальную честь смолоду; 6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии; 7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов; 8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети. Мобильный телефон Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств. Основные советы для безопасности мобильного телефона: Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги; Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге? Необходимо обновлять операционную систему твоего смартфона; Используй антивирусные программы для мобильных телефонов; Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение; После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies; Периодически проверяй, какие платные услуги активированы на твоем номере; Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

			Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это. Online игры Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции. Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов. В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр. Основные советы по безопасности твоего игрового аккаунта: 1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков; 2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов; 3. Не указывай личную информацию в профайле игры; 4. Уважай других участников по игре; 5. Не устанавливай неофициальные патчи и моды; 6. Используй сложные и разные пароли; 7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить. Фишинг или кража личных данных Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом. Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).

			Основные советы по борьбе с фишингом: 1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее; 2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем; 3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем; 4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты; 5. Установи надежный пароль (PIN) на мобильный телефон; 6. Отключи сохранение пароля в браузере; 7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы. Цифровая репутация Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети. Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу. Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно. Основные советы по защите цифровой репутации: 1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети; 2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого,

			сделай его только "для друзей"; 3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать. Авторское право Современные школьники - активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность. Термин "интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями. Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете. Использование "пиратского" программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети. О портале Сетевичок.рф - твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином!
5.	Родителям(законным представителям) обучающихся	Текст на странице сайта	ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ Определение термина "информационная безопасность детей" содержится в Федеральном **законе** N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию",

			регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону "информационная безопасность детей" - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. В силу Федерального **закона** N 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является: 1. информация, запрещенная для распространения среди детей; 2. информация, распространение которой ограничено среди детей определенных возрастных категорий. 3. К информации, запрещенной для распространения среди детей, относится: 4. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству; 5. способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством; 6. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным; 7. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи; 8. оправдывающая противоправное поведение; 9. содержащая нецензурную брань; 10. содержащая информацию порнографического характера. К информации, распространение которой ограничено среди детей определенного возраста, относится: 1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия; 2. вызывающая у детей страх, ужас или панику, в т.ч. 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.

			С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей. Общие правила для родителей 1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты. 2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео. 3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес) 4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы). 5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями. Возраст от 7 до 8 лет В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т.е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

			Советы по безопасности в сети Интернет для детей 7 - 8 лет 1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения. 2. Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь. 3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей. 4. Используйте специальные детские поисковые машины. 5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю. 6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса. 7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения. 8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей. 9. Научите детей не загружать файлы, программы или музыку без вашего согласия. 10. Не разрешайте детям использовать службы мгновенного обмена сообщениями. 11. В "белый" список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией. 12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни. 13. Не делайте "табу" из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты "для взрослых". 14. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях. Возраст детей от 9 до 12 лет В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом

			нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля. Советы по безопасности для детей от 9 до 12 лет 1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения. 2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером. 3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь. 4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей. 5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю. 6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете. 7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету. 8. Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними. 9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете. 10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение. 11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере. 12. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях. 13. Расскажите детям о порнографии в Интернете. 14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами. 15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз. Возраст детей от 13 до 17 лет

			В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок "для взрослых". Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете. Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в "свободное плавание" по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете. Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей. Советы по безопасности в этом возрасте от 13 до 17 лет 1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов ("черный список"), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах). 2. Компьютер с подключением к сети Интернет должен находиться в общей комнате. 3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы. 4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю. 5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме. 6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет. 7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

			8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение. 9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях. 10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры. 11. Приучите себя знакомиться с сайтами, которые посещают подростки. 12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире. 13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям. 14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону. Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы. **Презентация** Всероссийского родительского собрания "Профилактика Интернет-рисков и угроз жизни детей и подростков" **Памятка** для родителей и детей "Безопасный Интернет" (с официального сайта Следственного комитета РФ)
6.	Детские безопасные сайты	Текст на странице сайта	**Список безопасных сайтов для детей** **http://web-landia.ru/** – Страна лучших сайтов для детей. **http://www.saferunet.ru** – Центр Безопасного Интернета в России.Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. А конкретнее – он занимаемся Интернет-угрозами и эффективным противодействием им в отношении пользователей. Центр был создан в 2008 году под названием «Национальный узел Интернет-безопасности в России». **http://www.friendlyrunet.ru** / – Фонд «Дружественный Рунет». Главной целью Фонда является содействие развитию сети Интернет как блhttp://bir-school9.ru/wp-admin/nav-menus.phpагоприятной

			среды, дружественной ко всем пользователям. Фонд поддерживает проекты, связанные с безопасным использованием интернета, содействует российским пользователям, общественным организациям, коммерческим компаниям и государственным ведомствам в противодействии обороту противоправного контента, а также в противодействии иным антиобщественным действиям в Сети.Фонд «Дружественный Рунет» реализует в России комплексную стратегию в области безопасного использования интернета. Основными проектами Фонда являются: Горячая линия по приему сообщений о противоправном контенте, специализированная линия помощи для детей «Дети онлайн» и просветительские проекты. **http://www.fid.su/projects/saferinternet/year/hotline/** – Линия помощи «Дети онлайн». Оказание психологической и практической помощи детям и подросткам, которые столкнулись с опасностью или негативной ситуацией во время пользования интернетом или мобильной связью. Линия помощи “Дети онлайн” является первым и единственным такого рода проектом в России и реализуется в рамках Года Безопасного Интернета в России. **http://www.nedopusti.ru/** – социальный проект по защите прав детей «Не допусти» – социальный проект по защите детей от похищений, сексуальной эксплуатации и жестокого обращения реализуется с августа 2009 года. Организаторы проекта: Общественная палата РФ, РОЦИТ (Региональная Общественная Организация «Центр Интернет-технологий»), Межрегиональная правозащитная общественная организация «Сопротивление». **http://www.za-partoi.ru/** – Журнал “Здоровье школьников” Ежемесячный журнал «Здоровье школьника» – проект Издательского дома МЦФЭР, который осуществляет выпуск 25 профессиональных журналов федерального значения тиражом 250 тысяч экземпляров ежемесячно и до 100 наименований книг ежегодно общим тиражом около 300 тысяч экземпляров. «Здоровье школьника» – новый журнал о психологии взросления и физическом развитии детей, о возможностях современной медицины, о взаимоотношениях родителей, детей и учителей, о досуге и здоровом образе жизни. Журнал ориентирован на широкий круг читателей, и в первую очередь, на родителей детей школьного возраста. **http://www.newseducation.ru/** – “Большая перемена” сайт для школьников и их родителей **http://www.mirbibigona.ru/** – «Страна друзей»:детская соцсеть: общение, музыка, фотоальбомы, игры, новости. **http://www.smeshariki.ru/** – «Смешарики»: развлекательная соцсеть: игры, музыка, мультфильмы. **http://www.solnet.ee/** – «Солнышко»: детский портал.Развивающие, обучающие игры для самых маленьких и еще много интересного и для родителей. **http://membrana.ru** – «Люди. Идеи Технологии». Информационно-образовательный интернет-

			журнал о новых технологиях. **http://www.teremoc.ru** – Детский сайт «ТЕРЕМОК» с развивающими играми, загадками, ребусами, мультфильмами. **http://www.murzilka.org/** – Сайт журнала «Мурзилка» со стихами, раскрасками, конкурсами и другой полезной информацией. **http://www.ladushki.ru** – Сайт для малышей и малышек. Мультфильмы, азбука, счет, рисунки. **http://www.e-parta.ru/** -Блог школьного «Всезнайки» – это ленты новостей по всем школьным предметам, виртуальные экскурсии, психологические и юридические советы по проблемам в школе и на улице, учебные видео-фильмы, обзоры лучших ресурсов Всемирной паутины. **http://сетевичок.рф/**
7.			