Когда речь заходит об информационной безопасности, обычно мы начинаем думать о компьютерах, сетях, интернете и хакерах. Но для образовательной среды проблема стоит шире: в ограждении учащегося от информации, которая может негативно повлиять на его формирование и  развитие, то есть о пропаганде различной направленности.

**Понятие информационной безопасности**

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

На практике важнейшими являются три аспекта информационной безопасности:

* доступность (возможность за разумное время получить требуемую информационную услугу);
* целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
* конфиденциальность (защита от несанкционированного прочтения).

Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

**Основные угрозы информационной безопасности**

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты автоматизированной информационной системы можно разбить на следующие группы:

***Аппаратные средства.*** Это компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – принтеры, контроллеры, кабели, линии связи и т.д.);

***Программное обеспечение.*** Это приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;

***Данные,*** хранимые временно и постоянно, на дисках, флэшках, печатные, архивы, системные журналы и т.д.;

***Персонал.***Пользователи, системные администраторы, программисты и др.

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Причинами случайных воздействий при эксплуатации могут быть:

* аварийные ситуации из-за стихийных бедствий и отключений электропитания;
* отказы и сбои аппаратуры;
* ошибки в программном обеспечении;
* ошибки в работе персонала;
* помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами:

* недовольством служащего своей карьерой;
* взяткой;
* любопытством;
* конкурентной борьбой;
* стремлением самоутвердиться любой ценой.

Можно составить гипотетическую модель потенциального нарушителя:

* квалификация нарушителя на уровне разработчика данной системы;
* нарушителем может быть как постороннее лицо, так и законный пользователь системы;
* нарушителю известна информация о принципах работы системы;
* нарушитель выбирает наиболее слабое звено в защите.

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ. Несанкционированный доступ использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Проведем классификацию каналов несанкционированного доступа, по которым можно осуществить хищение, изменение или уничтожение информации:

***Через человека:***

* хищение носителей информации;
* чтение информации с экрана или клавиатуры;
* чтение информации из распечатки.

***Через программу:***

* перехват паролей;
* дешифровка зашифрованной информации;
* копирование информации с носителя.

***Через аппаратуру:***

* подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
* перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характерны тем, что против них предпринимают так называемые удаленные атаки. Нарушитель может находиться за тысячи километров от атакуемого объекта, при этом нападению может подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.

**Обеспечение информационной безопасности**

Формирование режима информационной безопасности – проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

***1. Законодательный .***Это законы, нормативные акты, стандарты и т.п.

Нормативно-правовая база определяющая порядок защиты информации:

***2. Морально-этический.***Всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации.

***3. Административный.*** Действия общего характера, предпринимаемые руководством организации. Такими документами могут быть:

* приказ руководителя о  назначении ответственного за обеспечение информационной безопасности;
* должностные обязанности ответственного за обеспечение информационной безопасности;
* перечень защищаемых информационных ресурсов и баз данных;
* инструкцию, определяющую порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников организации.

***4. Физический.***Механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей.

***5. Аппаратно-программный***(электронные устройства и специальные программы защиты информации).

Принятые меры по созданию безопасной информационной системы в школе:

* Обеспечена защита компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т. д.)
* Установлен строгий контроль за электронной почтой, обеспечен постоянный контроль за входящей и исходящей корреспонденцией.
* Установлены соответствующие пароли на персональные ПК.
* Использованы контент-фильтры,  для фильтрации сайтов по их содержимому.

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать. Под защитой должна находиться вся система обработки информации.

Лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность.

Надежная система защиты должна быть полностью протестирована и согласована. Защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора.

В заключение своего доклада хотелось бы дать некоторые рекомендации по организации работы в информационном пространстве, чтобы уберечь себя и своих близких от интернет-преступников.

**Рекомендации по организации работы в информационном пространстве**

1. Перед началом работы необходимо четко сформулировать цель и вопрос поиска информации.

2. Желательно выработать оптимальный алгоритм поиска информации в сети Интернет, что значительно сократит время и силы, затраченные на поиск.

3. Заранее установить временный лимит (2-3 часа) работы в информационном пространстве (просмотр телепередачи, чтение, Интернет).

4. Во время работы необходимо делать перерыв на 5-10 минут для снятия физического напряжения и зрительной нагрузки.

5. Необходимо знать 3-4 упражнения для снятия зрительного напряжения и физической усталости.

6. Работать в хорошо проветренном помещении, при оптимальном освещении и в удобной позе.

7. Не стоит легкомысленно обращаться со спам-письмами и заходить на небезопасные веб-сайты. Для интернет-преступников вы становитесь лёгкой добычей.

8. При регистрации в социальных сетях, не указывайте свои персональные данные, например: адрес или день рождения.

9. Не используйте в логине или пароле персональные данные.

10. Все это позволяет интернет-преступникам получить данные доступа к аккаунтам электронной почты, а также инфицировать домашние ПК для включения их в бот-сеть или для похищения банковских данных родителей.

11. Создайте собственный профиль на компьютере, чтобы обезопасить информацию, хранящуюся на нем.

12. Не забывайте, что факты, о которых вы узнаете в Интернете, нужно очень хорошо проверить, если выбудете использовать их в своей домашней работе. Целесообразно сравнить три источника информации, прежде чем решить, каким источникам можно доверять.

13. О достоверности информации, помещенной на сайте можно судить по самому сайту, узнав об авторах сайта.

14. Размещая информацию о себе, своих близких и знакомых на страницах социальных сетей, спросите предварительно разрешение у тех, о ком будет эта информация.

15. Не следует размещать на страницах веб-сайтов свои фотографии и фотографии своих близких и знакомых, за которые вам потом может быть стыдно.

16. Соблюдайте правила этики при общении в Интернете: грубость провоцирует других на такое же поведение.

17. Используя в своей работе материал, взятый из информационного источника (книга, периодическая печать, Интернет), следует указать этот источник информации или сделать на него ссылку, если материал был вами переработан.

**Методические и справочные материалы**

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**

**ПО ОБУЧЕНИЮ УЧАЩИХСЯ ПРАВИЛАМ БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ, ПРОФИЛАКТИКЕ ИНТЕРНЕТ-ЗАВИСИМОСТИ**

Методические рекомендации разработаны с целью обеспечения реализации образовательными организациями системы мероприятий, направленных на обучение учащихся правилам безопасного поведения в интернет-пространстве, профилактику интернет-зависимости, националистических проявлений в молодежной среде и устранение риска вовлечения подростков в противоправную деятельность. Рекомендации разработаны на основании письма Министерства образования и науки Мурманской области от 12.12.2014 №17-02/9115-ИК «О методическом обеспечении деятельности по противодействию экстремизму среди обучающихся и профилактике интернет-зависимости».

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. Также следует обратить внимание на гигиенические требования, которые необходимо соблюдать при работе с компьютером:

* школьникам среднего и старшего возраста можно проводить перед монитором до двух часов в день, устраивая 10-15-минутные перерывы каждые полчаса;
* ребенок младшего возраста может находиться за компьютером не более 15 минут в день, в условиях классно-урочной деятельности – не более одного урока, а при наличии противопоказаний офтальмолога – только 10 минут, не более 3 раз в неделю;
* лучше работать за компьютером в первой половине дня;
* комната должна быть хорошо освещена;
* при работе за компьютером следить за осанкой, мебель должна соответствовать росту;
* расстояние от глаз до монитора – 60 см;
* периодически делать зарядку для глаз.

В соответствии с федеральными государственными образовательными стандартами общего образования в структуру основной образовательной программы основного общего образования включена программа воспитания и социализации учащихся, которая содержит такое направление, как формирование культуры здорового и безопасного образа жизни. В рамках этой программы может осуществляться информационно-просветительская работа среди школьников, пропагандирующая важность владения навыками безопасной работы в сети Интернет.

В образовательных организациях необходимо проводить занятия для учащихся по основам информационной безопасности («основы медиа- безопасности»); знакомить родителей с современными программно- техническими средствами (сетевыми фильтрами, программами «родительский контроль»), ограничивающими доступ детей и подростков к ресурсам сети Интернет, несовместимыми с задачами воспитания; проводить специальные мероприятия по вопросам информационной безопасности несовершеннолетних.

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](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](http://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 объем 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](http://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>

Рекомендации по безопасному использованию Интернета для несовершеннолетних и их родителей даны и на сайте Майкрософт.

<http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx>, [http://www.microsoft.com/ru-](http://www.microsoft.com/ru-ru/security/default.aspx) [ru/security/default.aspx.](http://www.microsoft.com/ru-ru/security/default.aspx)

Вышеуказанные сетевые ресурсы могут быть использованы для проведения педсоветов в образовательных организациях по вопросам безопасности детей в сети Интернет.

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>.

В письме Министерства образования и науки РФ от 25.12.13 № НТ- 1338/08 об учебной программе «Интернет: возможности, компетенции, безопасность» предлагаются модели уроков по вышеуказанной теме, даются рекомендации для учёта возрастных особенностей учащихся.

<http://www.dagminobr.ru/documenty/informacionnie_pisma/pismo_3431018_ot_29_yanvarya_2014_g/print>.

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.

В основной школе учащиеся активно начинают использовать Интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в онлайновые игры и так далее. Все более часто их любимым способом общения становится мгновенный обмен сообщениями. Для учащихся этого возраста желание выяснить, что они могут себе позволить делать без разрешения взрослых, является абсолютно нормальным. Педагогам для обеспечения интернет-безопасности учащихся 10-15 лет необходимо:

* познакомить учащихся с ответственным, достойным поведением в Интернете;
* рассказать об основных опасностях и правилах безопасного использования сети Интернет;
* убедить никогда не выдавать личную информацию, в том числе фамилию, имя, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения, по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете;
* объяснить опасность личных встреч с друзьями по Интернету без присутствия взрослых;
* убедить сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им.
* ознакомь с правилами поведения на форумах и чатах, убедить их, что они не должны использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

Организуя работу с учащимися старших классов по безопасному использованию информации в Интернете, следует обратить внимание на неформальные молодежные объединения, которые возникают в образовательной организации. Сетевая безопасность подростков – трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее, участие взрослых тоже необходимо:

* Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются. Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы.
* Интересуйтесь, какими чатами и досками объявлений пользуются подростки, и с кем они общаются. Поощряйте использование модерируемых (контролируемых) чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме.
* Настаивайте, чтобы подростки осторожно соглашались или не соглашались вовсе на личные встречи с друзьями из Интернета. Напоминайте, какие опасности это может за собой повлечь.
* Убедите подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться.
* Помогите подросткам защититься от спама. Научите их не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
* Обсудите с подростками азартные сетевые игры и связанный с ними риск.

Результатами мероприятий по безопасному использованию Интернета могут стать как бумажные, так и электронные ресурсы, созданные учащимися: рисунки, сочинения (рассказы, сказки, стихи), буклеты, презентации. Интересной формой представления результатов могут стать театрализованные выступления и видеофильмы учащихся.

Для учащихся старших классов при создании материалов по безопасности можно использовать сервисы Интернета для совместной деятельности. Работа команды учащихся в этом случае можем проводиться дистанционно. Одним из примеров является схема «Безопасность детей в Интернете». <http://www.mindmeister.com/ru/12485180/>

Рекомендуем обратить внимание на создание условия для ознакомления с результатами творчества учащихся. Разработанные материалы можно размещать на сайте образовательной организации, в социальных сетях, блогах и сетевых сообществах.

Для эффективной профилактики интернет-зависимости, профилактики националистических проявлений в молодежной среде и устранения риска вовлечения подростков в противоправную деятельность педагогам необходимо проводить разъяснительную и консультационную работу с родителями учащихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в Интернет.

Возможно проведение бесед о работе учащихся в сети Интернет на классных и общешкольных родительских собраниях или при индивидуальных встречах; информирование через школьный сайт на страничке для родителей. На таких страничках можно разместить рекомендации по профилактике компьютерной зависимости у детей, по обеспечению безопасности детей в Интернете.

Примеры подобных страничек для родителей:

<http://borovoeshc.ucoz.ru/load/shkola_bezopasnosti/bezopasnyj_internet_dlja_detej/7-1-0-109>— школьный сайт МКОУ Боровская ООШ, о программах родительского контроля.

<http://nsportal.ru/site/112423/bezopasnyy-internet>школьный сайт [МБОУ «Кипринская](http://nsportal.ru/site/112423) [СОШ» Алтайский край](http://nsportal.ru/site/112423), статьи, советы родителям.

Эффективной мерой является установка на компьютер программного обеспечения с функциями «родительского контроля». Родителям можно порекомендовать установить на домашнем компьютере бесплатную программу «Интернет Цензор [www.icensor.ru](http://icensor.ru/).

Родителям могут быть даны следующие рекомендации по формированию у учащихся навыков безопасного поведения в сети Интернет:

* Научите детей советоваться с вами перед раскрытием информации через электронную почту, чаты, доски объявлений, регистрационные формы и личные профили.
* Научите детей не загружать программы, музыку или файлы без вашего разрешения.
* Позволяйте заходить на детские сайты только с хорошей репутацией и контролируемым общением.
* Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.
* Приучите детей сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится.

Единство родительских и педагогических усилий поможет оптимально использовать «плюсы» и нейтрализовать «минусы» работы с ресурсами всемирной Сети.

v

Интернет-ресурсы для педагогических работников:

* <http://www.fid.su/projects/deti-v-internete>сайт Фонда Развития Интернет.
* <http://content-filtering.ru/>сайт «Ваш личный интернет», советы, рекомендации для детей и родителей по безопасной работе в Интернет.
* <http://www.ligainternet.ru/>Лиги 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://www.saferunet.org/children/>Центр безопасности Интернета в России.
* [https://edu.tatar.ru/upload/images/files/909\_029%20Orangepdf](https://edu.tatar.ru/upload/images/files/909_029%20Orange7.pdf)Безопасно и просто: родительский контроль. — Буклет
* Урок в 9–10 классах. Профилактика интернет-зависимости «Будущее начинается сегодня» [http://festival.1september.ru/articles/612789/](https://docviewer.yandex.ru/r.xml?sk=0c02c71819619c959a25742d60574947&amp;url=http%3A%2F%2Ffestival.1september.ru%2Farticles%2F612789%2F)Материал разработан для учащихся 9-11 классов, но может модифицироваться и для учащихся среднего звена школы.
* Материалы (буклет, презентация и текст) для бесед профилактике игровой и интернет-зависимости у детей и подростков на сайте Министерства образования и науки Республики Татарстан: [http://mon.tatarstan.ru/prof\_internet\_zavisimosti.htm](https://docviewer.yandex.ru/r.xml?sk=0c02c71819619c959a25742d60574947&amp;url=http%3A%2F%2Fmon.tatarstan.ru%2Fprof_internet_zavisimosti.htm)
* <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/](http://xn--b1afankxqj2c.xn--p1ai/)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.

<http://xn--b1afankxqj2c.xn--p1ai/partneram-o-proekte> 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»

Интернет-ресурсы для педагогических работников:

* <http://www.fid.su/projects/deti-v-internete>сайт Фонда Развития Интернет.
* <http://content-filtering.ru/>сайт «Ваш личный интернет», советы, рекомендации для детей и родителей по безопасной работе в Интернет.
* <http://www.ligainternet.ru/>Лиги 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://www.saferunet.org/children/>Центр безопасности Интернета в России.
* [https://edu.tatar.ru/upload/images/files/909\_029%20Orangepdf](https://edu.tatar.ru/upload/images/files/909_029%20Orange7.pdf)Безопасно и просто: родительский контроль. — Буклет
* Урок в 9–10 классах. Профилактика интернет-зависимости «Будущее начинается сегодня» [http://festival.1september.ru/articles/612789/](https://docviewer.yandex.ru/r.xml?sk=0c02c71819619c959a25742d60574947&amp;url=http%3A%2F%2Ffestival.1september.ru%2Farticles%2F612789%2F)Материал разработан для учащихся 9-11 классов, но может модифицироваться и для учащихся среднего звена школы.
* Материалы (буклет, презентация и текст) для бесед профилактике игровой и интернет-зависимости у детей и подростков на сайте Министерства образования и науки Республики Татарстан: [http://mon.tatarstan.ru/prof\_internet\_zavisimosti.htm](https://docviewer.yandex.ru/r.xml?sk=0c02c71819619c959a25742d60574947&amp;url=http%3A%2F%2Fmon.tatarstan.ru%2Fprof_internet_zavisimosti.htm)
* <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/](http://xn--b1afankxqj2c.xn--p1ai/)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.

<http://xn--b1afankxqj2c.xn--p1ai/partneram-o-proekte> 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»

**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 заражённая 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 серьёзный уровень защиты от вредоносных программ;
2. Постоянно устанавливай почти (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 ненадёжных 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 высший 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 Wi­Fiсети не являются безопасными.

Советы по безопасности работе в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fiсети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
3. При использовании Wi-Fiотключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
4. Не используй публичный WI-FIдля 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-Fiавтоматически». Не допускай автоматического подключения устройства к сетям Wi-Fiбез твоего согласия.

**Социальные сети**

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebookуже 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 идентификации 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, StROng!;;
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 свой 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:

1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему твоего смартфона;
4. Используй антивирусные программы для мобильных телефонов;
5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
7. Периодически проверяй какие платные услуги активированы на твоем номере;
8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
9. Bluetoothдолжен 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 phishingчитается 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 окружающее 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 установленный не легальная программа. Не стоит также забывать, что существует легальные и бесплатные программы, которые можно найти в сети.

О портале

[Сетевичок.рф](http://xn--b1afankxqj2c.xn--p1ai/) — 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!

**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 заражённая 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 серьёзный уровень защиты от вредоносных программ;
2. Постоянно устанавливай почти (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 ненадёжных 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 высший 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 Wi­Fiсети не являются безопасными.

Советы по безопасности работе в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fiсети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
3. При использовании Wi-Fiотключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
4. Не используй публичный WI-FIдля 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-Fiавтоматически». Не допускай автоматического подключения устройства к сетям Wi-Fiбез твоего согласия.

**Социальные сети**

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebookуже 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 идентификации 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, StROng!;;
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 свой 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:

1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему твоего смартфона;
4. Используй антивирусные программы для мобильных телефонов;
5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
7. Периодически проверяй какие платные услуги активированы на твоем номере;
8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
9. Bluetoothдолжен 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 phishingчитается 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 окружающее 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 установленный не легальная программа. Не стоит также забывать, что существует легальные и бесплатные программы, которые можно найти в сети.

О портале

[Сетевичок.рф](http://xn--b1afankxqj2c.xn--p1ai/) — 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!

**Интернет-ресурсы для педагогических работников**

[http://www.prosv.ru/](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.prosv.ru/%26sa%3DD%26ust%3D1582654767306000&sa=D&source=editors&ust=1617532056340000&usg=AOvVaw0RhtiQEWDhW1ts5DEuNtb5)Сайт издательства ПРОСВЕЩЕНИЕ

 [http://sputnik.mto.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://sputnik.mto.ru%26sa%3DD%26ust%3D1582654767306000&sa=D&source=editors&ust=1617532056341000&usg=AOvVaw2MojWTIR-dfB-5kPA7WLsU) – Спутниковый канал единой образовательной информационной   среды.

[http://www.apkppro.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.apkppro.ru%26sa%3DD%26ust%3D1582654767306000&sa=D&source=editors&ust=1617532056341000&usg=AOvVaw2AnJAAeRMnybavtJ1J83i8) – Академия повышения квалификации и профессиональной переподготовки работников образования РФ.

[http://www.curator.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.curator.ru%26sa%3DD%26ust%3D1582654767306000&sa=D&source=editors&ust=1617532056342000&usg=AOvVaw3GgXCjVssyMgX76VPLuBew)– «Куратор». Сайт посвящён применению Интернет- технологий в образовании. Новости образования, материалы по дистанционному обучению через Интернет, сайтостроению, web-обзоры, обзоры электронных учебников, материалы в помощь методисту,

 [http://www.ed.gov.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.ed.gov.ru%26sa%3DD%26ust%3D1582654767307000&sa=D&source=editors&ust=1617532056342000&usg=AOvVaw0mxIuG5ItVavhmLOSq4sgw)– Федеральное агенство по образованию.

 [http://www.edu.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.edu.ru%26sa%3DD%26ust%3D1582654767307000&sa=D&source=editors&ust=1617532056343000&usg=AOvVaw166jUX-Wd7J7ua79fQIDfs) – Федеральный портал «Российское образование».

Каталог образовательных Интернет-ресурсов. Базовые федеральные образовательные порталы. Поиск по подстройке, по рубрикаторам. Рейтинги ресурсов. Нормативные документы системы образования. Государственные образовательные стандарты. Дистанционное обучение (курсы, организации, нормативная база). Глоссарий (образование, педагогика).

http://www.edu.-all.ru– Портал «ВСЕОБУЧ» – всё об образовании. [http://www.ict.edu.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.google.com/url?q%253Dhttp://www.ict.edu.ru/%2526sa%253DD%2526ust%253D1573899793216000%26sa%3DD%26ust%3D1582654767308000&sa=D&source=editors&ust=1617532056344000&usg=AOvVaw3WbpZjmPpN4OXdXkr7aH3s) – Федеральный портал «Информационно-

коммуникационные технологии в образовании».

[http://www.int-edu.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.int-edu.ru%26sa%3DD%26ust%3D1582654767308000&sa=D&source=editors&ust=1617532056345000&usg=AOvVaw1kyRkXKvu4gU0MtUX3glfR) – Институт новых технологий образования. Сайт представляет различные дидактические и методические пособия.

[http://www.lexed.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.lexed.ru%26sa%3DD%26ust%3D1582654767308000&sa=D&source=editors&ust=1617532056345000&usg=AOvVaw36s8WN7aQYozYeQ81S_M6p) – Федеральный центр образовательного законодательства.

[http://www.mon.gov.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.mon.gov.ru%26sa%3DD%26ust%3D1582654767308000&sa=D&source=editors&ust=1617532056345000&usg=AOvVaw2KBw_IRHgpgb5juSnSO2Dg)– Министерство образования и науки Российской Федерации.

[http://www.rost.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.rost.ru%26sa%3DD%26ust%3D1582654767309000&sa=D&source=editors&ust=1617532056346000&usg=AOvVaw1hpbQrksxflRtnfS7YNEyD) – Приоритетные национальные проекты: сайт Совета при Президенте Российской Федерации по реализации приоритетных национальных проектов и демографической политике.

[http://www.school.edu.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.school.edu.ru%26sa%3DD%26ust%3D1582654767309000&sa=D&source=editors&ust=1617532056346000&usg=AOvVaw3Jr9foVbMaIWyS-xlVj7Pd) – Российский общеобразовательный портал. Образовательные ресурсы для воспитателей, учителей, учеников и родителей. Портал содержит многообразную информацию по всем основным вопросам общего образования, от дошкольного до полного среднего.

[http://www.videoresursy.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.videoresursy.ru%26sa%3DD%26ust%3D1582654767309000&sa=D&source=editors&ust=1617532056347000&usg=AOvVaw2be0fuLj9gDimXLWyC3yH-) – «Медиаресурсы для образования и просвещения» - один из лидеров в создании нового поколения электронных учебно-методических пособий на основе демонстрации опыта работы педагогов-практиков. «Медиаресурсы» - коммерческая организация, современная рыночная структура, специализирующаяся в области разработки, издания, тиражирования и сбыта мультимедийных учебно-методических пособий для общего и профессионального образования.

[http://www.vidod.edu.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.vidod.edu.ru%26sa%3DD%26ust%3D1582654767310000&sa=D&source=editors&ust=1617532056347000&usg=AOvVaw1-negKxTl1W20bHRkaZLFW) – Федеральный портал «Дополнительное образование детей». Федеральные и межведомственные программы. Воспитание. Направления дополнительного образования детей. Детский отдых.

МЕТОДИЧЕСКИЕ РЕСУРСЫ ДЛЯ УЧИТЕЛЯ НАЧАЛЬНЫХ КЛАССОВ

[http://www.edu.ru/documents/](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.edu.ru/documents/%26sa%3DD%26ust%3D1582654767310000&sa=D&source=editors&ust=1617532056348000&usg=AOvVaw0ipVPXd38r7poVA-WC-_0N) - обязательный минимум содержания начального общего образования;

[http://festival.1september.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://festival.1september.ru/%26sa%3DD%26ust%3D1582654767310000&sa=D&source=editors&ust=1617532056348000&usg=AOvVaw16kqO3XaSwL5y3Ux1FLBgt) – Фестиваль педагогических идей «Открытый урок». Самый большой педагогический форум в русскоязычном интернете. Содержит свыше 26000 разработок уроков и внеклассных мероприятий для начальной школы.

[http://nsc.1september.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://nsc.1september.ru/%26sa%3DD%26ust%3D1582654767310000&sa=D&source=editors&ust=1617532056349000&usg=AOvVaw3s4QRLKYCZgt8X3aWrzKVm) – Электронная версия газеты «Начальная школа» издательства «Первое сентября». Удобный рубрикатор позволяет с легкостью найти большинство ресурсов, опубликованных в газете.

[http://school-collection.edu.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://school-collection.edu.ru/%26sa%3DD%26ust%3D1582654767311000&sa=D&source=editors&ust=1617532056349000&usg=AOvVaw3RvuGHRxvkh7bSrExyYQa8) – Единая коллекция цифровых образовательных ресурсов. Удобная навигация и технология поиска дают возможность без труда отыскать необходимый материал. База содержит множество визуальных элементов от рисунков и анимаций, до видео фрагментов для организации обучения по всем предметам с 1 по 11 класс.

[http://www.uchportal.ru/load/46](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.uchportal.ru/load/46%26sa%3DD%26ust%3D1582654767311000&sa=D&source=editors&ust=1617532056349000&usg=AOvVaw3awMEZ1b61HnvMxzmPctx2) - Все для учителя начальных классов на «Учительском портале»: уроки, презентации, контроль, тесты, планирование, программы.

[https://nsportal.ru/shkola](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://nsportal.ru/shkola%26sa%3DD%26ust%3D1582654767311000&sa=D&source=editors&ust=1617532056350000&usg=AOvVaw0NvkeOrZQCiMDiv03swiNh) - социальная сеть работников образования

[https://www.prodlenka.org/](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.prodlenka.org/%26sa%3DD%26ust%3D1582654767312000&sa=D&source=editors&ust=1617532056350000&usg=AOvVaw2p6vScPpUMjRovIcjoI3VI) - сайт для учителей и воспитателей

[http://www.n-shkola.ru/](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.n-shkola.ru/%26sa%3DD%26ust%3D1582654767312000&sa=D&source=editors&ust=1617532056351000&usg=AOvVaw2bqWbeeCm82QNSWI2PUVhj) - Официальный сайт журнала «Начальная школа».

[http://www.sch2000.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.sch2000.ru/%26sa%3DD%26ust%3D1582654767312000&sa=D&source=editors&ust=1617532056352000&usg=AOvVaw0MLY0Qd_XMHtOvcnxrOYN_) - Сайт центра системно-деятельностной педагогики «Школа 2000…» содержит методические рекомендации, курсы, учебные пособия для организации обучения по авторским учебникам Л.Г. Петерсон для начальной школы и дошкольных общеобразовательных учреждений.

[http://www.zankov.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.zankov.ru/%26sa%3DD%26ust%3D1582654767312000&sa=D&source=editors&ust=1617532056352000&usg=AOvVaw2_vJ5dkNWbogrePsg1ktu5) - Официальный сайт федерального научно-методического центра им. Л.В. Занкова. Очень полезен учителям, работающим по УМК этого автора.

[www.school2100.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://nach-school.ru/www.school2100.ru%26sa%3DD%26ust%3D1582654767313000&sa=D&source=editors&ust=1617532056353000&usg=AOvVaw32FMH7AAYWfnoPHgKE3_QS) - Официальный сайт для учителей, работающих по УМК «Школа 2100».

[http://www.ug.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.ug.ru/%26sa%3DD%26ust%3D1582654767313000&sa=D&source=editors&ust=1617532056353000&usg=AOvVaw26wwMnH2prxYip5gc4bwhH) - Официальный ресурс «Учительской газеты».

[http://www.edu.ru/modules.php?op=modload&name=Web\_Links&file=index&l\_op=viewlink&](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.edu.ru/modules.php?op%253Dmodload%2526name%253DWeb_Links%2526file%253Dindex%2526l_op%253Dviewlink%2526cid%253D277%26sa%3DD%26ust%3D1582654767313000&sa=D&source=editors&ust=1617532056354000&usg=AOvVaw24QGqei0x8zKEHwrcbw50A)[cid=277](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.edu.ru/modules.php?op%253Dmodload%2526name%253DWeb_Links%2526file%253Dindex%2526l_op%253Dviewlink%2526cid%253D277%26sa%3DD%26ust%3D1582654767314000&sa=D&source=editors&ust=1617532056355000&usg=AOvVaw01KDCgbP1brpTkayu_npml) – Подборка федерального образовательного портала для организации занятий по природоведению.

[www.nachalka.com](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://nach-school.ru/www.nachalka.com/%26sa%3DD%26ust%3D1582654767314000&sa=D&source=editors&ust=1617532056355000&usg=AOvVaw29gYs-U2srcYFPuWowlGep) - Официальный ресурс для учителей, детей и родителей. Всех, чья жизнь каким-либо образом связана с начальной школой. Дети найдут здесь много интересных и новых для них сведений, поиграют в игры или пообщаются со сверстниками. Родители могут почитать о проблемах воспитания и задать интересующие их вопросы, а учителя пообщаться и поделиться опытом друг с другом.

[http://www.uroki.net/](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.uroki.net/%26sa%3DD%26ust%3D1582654767314000&sa=D&source=editors&ust=1617532056356000&usg=AOvVaw3N4WqLW2msP6SWgi8nFwjZ) - Банк данных в помощь учителю: разработки уроков, сценарии внеклассных мероприятий, школьные песни и караоке, календарно-тематическое планирование и множество других полезных материалов.

[http://www.k-yroky.ru/load/67](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.k-yroky.ru/load/67%26sa%3DD%26ust%3D1582654767314000&sa=D&source=editors&ust=1617532056356000&usg=AOvVaw2nHXxbnplp0QT9aZEdh3DX) - Еще один ресурс, содержащий множество методических разработок.

[http://bomoonlight.ru/azbuka/](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://bomoonlight.ru/azbuka/%26sa%3DD%26ust%3D1582654767315000&sa=D&source=editors&ust=1617532056357000&usg=AOvVaw1PW85vhqk86Y2uvABEHJtc) - Азбука в картинках для учеников 1-го класса.

[http://stranamasterov.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://stranamasterov.ru/%26sa%3DD%26ust%3D1582654767315000&sa=D&source=editors&ust=1617532056357000&usg=AOvVaw1th6Z_KUo6YcIKNCS6-_LH) – Всё для творчества учителей, детей и их родителей. Разнообразные техники, мастер-классы дадут возможность творить любому, даже самому неусидчивому ребенку.

[http://viki.rdf.ru/](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://viki.rdf.ru/%26sa%3DD%26ust%3D1582654767315000&sa=D&source=editors&ust=1617532056358000&usg=AOvVaw2f9AU_mfNgOarL9WFdzHQd) - Детские электронные презентации и клипы.

[http://akademius.narod.ru/index1.html](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://akademius.narod.ru/index1.html%26sa%3DD%26ust%3D1582654767315000&sa=D&source=editors&ust=1617532056358000&usg=AOvVaw2kjxvcvcRxPb8QALbQMMxf) - Онлайн-тестирования по русскому языку, математике и истории для учащихся 1-5 классов.

[http://www.it-n.ru/communities.aspx?cat\_no=5025&tmpl=com](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.it-n.ru/communities.aspx?cat_no%253D5025%2526tmpl%253Dcom%26sa%3DD%26ust%3D1582654767316000&sa=D&source=editors&ust=1617532056359000&usg=AOvVaw0cRwBSN5XDD6PRxpMTQ8-0) – Сеть творческих учителей. Сайт создан для педагогов, которые стремятся к улучшению качества учебно-воспитательного процесса с помощью применения на уроках информационно-коммуникационных технологий. На сайте можно найти разработки уроков с применением ИКТ в рамках требований ФГОС, примерные программы внеурочной и урочной деятельности младших школьников, ссылки на материалы о ФГОС в сети Интернет и другую полезную информацию.

[http://suhin.narod.ru/](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://suhin.narod.ru/%26sa%3DD%26ust%3D1582654767316000&sa=D&source=editors&ust=1617532056360000&usg=AOvVaw17enUqT61vn6FihJUnb1Mu) - Занимательные материалы из книг И.Сухина: от литературных затей до шахмат.

[http://www.lenagold.ru/](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.lenagold.ru/%26sa%3DD%26ust%3D1582654767316000&sa=D&source=editors&ust=1617532056360000&usg=AOvVaw2AvYQbtasMTk22G11RQ38l) - Отличный сайт для творческих учителей. Содержит клипарты и фоны, которые помогут в создании презентационных материалов к уроку.

[http://www.tatarovo.ru/sound.html](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.tatarovo.ru/sound.html%26sa%3DD%26ust%3D1582654767317000&sa=D&source=editors&ust=1617532056361000&usg=AOvVaw3LOyDvdpK8TZgf_2o5cxDm) - Отличная подборка звуковых материалов (птицы, насекомые, люди, бытовые приборы и инструменты, природа и многое другое).

[http://rusedu.ru/subcat\_28.html](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://rusedu.ru/subcat_28.html%26sa%3DD%26ust%3D1582654767317000&sa=D&source=editors&ust=1617532056362000&usg=AOvVaw1fPC3BsSxgXgFXUVS5g5QL) - Разработки уроков и сценарии внеклассных занятий для начальной школы с применением ИКТ.

[http://babydreams.bestnetservice.com/index.htm](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://babydreams.bestnetservice.com/index.htm%26sa%3DD%26ust%3D1582654767317000&sa=D&source=editors&ust=1617532056362000&usg=AOvVaw3MOlMMkG8a7JDLWsWRue5k) - Сказочное образование представляет диски с играми и заданиями по образовательным предметам на любой вкус.

[http://laste.arvutikaitse.ee/rus/html/etusivu.htm](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://laste.arvutikaitse.ee/rus/html/etusivu.htm%26sa%3DD%26ust%3D1582654767318000&sa=D&source=editors&ust=1617532056363000&usg=AOvVaw1dGEguH-GB4ngydtWq5UMN) - Сайт для детей и взрослых, раскрывающий такой важный вопрос как безопасность в Интернете.

СПИСОК ЖУРНАЛОВ И ГАЗЕТ

[http://www.1september.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.1september.ru%26sa%3DD%26ust%3D1582654767333000&sa=D&source=editors&ust=1617532056388000&usg=AOvVaw0sR0lrxQcSNKzeZBmCHZcs) – «Первое сентября». Сервер объединения педагогических изданий. Публикуются номера газеты, а также материалы предметных газет.

[http://psy.1september.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://psy.1september.ru%26sa%3DD%26ust%3D1582654767334000&sa=D&source=editors&ust=1617532056389000&usg=AOvVaw3BxN3ZaVvyFwI_Xc95HB24)– «Школьный психолог».

[http://www.detgazeta.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.detgazeta.ru%26sa%3DD%26ust%3D1582654767334000&sa=D&source=editors&ust=1617532056389000&usg=AOvVaw2VkcozAnyjAOETbybIcjOX) – «Детская газета». Новое весёлое электронное издание для детей от 6 до 10 лет. Сказки, головоломки, викторины, лабиринты, рассказы о животных, кулинарные рецепты, адреса друзей.

[http://www.informica.ru/windows/magaz/higher/higher.html](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.informica.ru/windows/magaz/higher/higher.html%26sa%3DD%26ust%3D1582654767334000&sa=D&source=editors&ust=1617532056390000&usg=AOvVaw06fFDZ-iyic9z4vDCc0Fdk) – Научно- педагогический журнал Министерства Образования и Науки Российской Федерации.

http://[www.kostyor.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.google.com/url?q%253Dhttp://www.kostyor.ru/%2526sa%253DD%2526ust%253D1573899793243000%26sa%3DD%26ust%3D1582654767334000&sa=D&source=editors&ust=1617532056391000&usg=AOvVaw00Neq5IILCGTwV_QjFj3ma) - Детский литературно-художественный журнал

«Костёр». Сегодняшний «Костёр» — это полезное и увлекательное издание, интересное и детям, и их родителям. Цель журнала — привить детям вкус и любовь к художественной литературе, к творческому познанию мира вокруг нас. Авторы – известные детские писатели: Эдуард Успенский, Григорий Остер, Святослав Сахарнов, Владислав Крапивин, Валерий Воскобойников, Александр Курляндский и другие. «Костер» печатает классиков отечественной детской литературы и открывает новые молодые имена. Юные авторы выступают в журнале на равных со взрослыми — ребята публикуют в журнале свои первые литературные опыты: стихи, рассказы, заметки, зарисовки. В журнале много интересных конкурсов и развивающих викторин с призами, есть страницы юмора, кино и музыки.

[http://www.merrypictures.ru/last\_vk](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.merrypictures.ru/last_vk%26sa%3DD%26ust%3D1582654767335000&sa=D&source=editors&ust=1617532056391000&usg=AOvVaw2fgsKO3Z4PaK5rPdgLF59X) - «Весёлые картинки». Детский юмористический журнал. Организует досуг всей семьи: настольные игры, комиксы, ребусы, шутки, загадки. С нового года в журнале вкладка «Учимся вместе с Весёлыми человечками». «Занимательная геометрия», «Давайте сравнивать», «Назови любимый цвет», «Учимся считать» и другие весёлые уроки составят уникальный «Весёлый учебник». Журнал рассчитан на детей от 4 до 10 лет. Просмотреть архив журнала можно на сайте[http://publ.lib.ru/ARCHIVES/V/''Veselye\_kartinki''/\_''Veselye\_kartinki''.html](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.google.com/url?q%253Dhttp://publ.lib.ru/ARCHIVES/V/%25252527%25252527Veselye_kartinki%25252527%25252527/_%25252527%25252527Veselye_kartinki%25252527%25252527.html%2526sa%253DD%2526ust%253D1573899793245000%26sa%3DD%26ust%3D1582654767335000&sa=D&source=editors&ust=1617532056392000&usg=AOvVaw09o8LuZG9VlSbXYhrwVL-y)

Публичная библиотека (Электронные книжные полки Вадима Ершова и К).

[http://www.murzilka.org/info/about/](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.murzilka.org/info/about/%26sa%3DD%26ust%3D1582654767335000&sa=D&source=editors&ust=1617532056393000&usg=AOvVaw0wlecHedd727LfLfELvelB) - популярный детский литературно- художественный журнал «Мурзилка». В журнале печатаются сказки, сказочные повести, рассказы, пьесы, стихи. Главные его авторы - современные талантливые писатели, художники и классики детской литературы. Часто авторами журнала выступают сами читатели. Просмотреть архив журнала можно на сайте: [www.murzilka.km.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.google.com/url?q%253Dhttp://www.murzilka.km.ru/%2526sa%253DD%2526ust%253D1573899793246000%26sa%3DD%26ust%3D1582654767335000&sa=D&source=editors&ust=1617532056393000&usg=AOvVaw2LrrPrPxqoaRQ8XEvQL_Fy). Адресован детям от 6 до 12 лет.

[http://www.vestnik.edu.ru](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttp://www.vestnik.edu.ru%26sa%3DD%26ust%3D1582654767336000&sa=D&source=editors&ust=1617532056393000&usg=AOvVaw0DLuWC36lCNNRioHUA-Bf2) – «Вестник образования». Нормативные документы и аналитические обзоры.