

# Информационная безопасность

## Информация о доступе к информационным системам и информационно-телекоммуникационным сетям

### в МАОУ Лицей-интернат № 84 имени

#### Гали Акыша

Одним из приоритетных направлений в деятельности школы является информатизация образовательного процесса, которая рассматривается как процесс, направленный на повышение эффективности и качества учебных занятий, и администрирования посредством применения ИКТ (информационно-коммуникативных технологий). Все компьютеры школы имеют выход в Интернет. Школьники имеют возможность работать в сети Интернет на уроках информатики и ежедневно в свободном доступе после уроков в компьютерном классе. В свободное от уроков время каждый желающий (учитель или обучающийся) при помощи точки доступа к сети Интернет может воспользоваться техническими и сетевыми ресурсами для выполнения учебных задач.

1. [Локальные акты, регламентирующие открытость и доступность информации о деятельности лицея](#)
2. Регламент работы учителей и школьников в сети Интернет
3. Должностная инструкция ответственного за работу «точки доступа к Интернету» в школе
4. Регламент работы образовательных учреждений с электронной почтой
5. Инструкция по организации антивирусной защиты в образовательных учреждениях
6. Письмо прокуратуры РТ "О рассмотрении информации о доступе учащихся к интернет-ресурсам

Рассматривая процессы повышения эффективности образовательного и управленческого процессов через призму информатизации, мы считаем, что школьный компьютер может и должен стать тем инструментом, который позволяет: во-первых, повысить эффективность учебных занятий, так как: включение в урок мультимедиа материалов (видео, звука, иллюстрационного материала) повышает его наглядность; использование цифровых образовательных ресурсов предметной направленности позволяет организовать изучение материала каждым учащимся индивидуально, в наиболее предпочтительном для него темпе; компьютер позволяет включить межпредметные интеграционные процессы, так как он по своей сути инструмент надпредметный, а применение, к примеру, одних и тех же программных средств и алгоритмов при решении математических, физических, химических и других задач акцентирует внимание на общности изучаемых в рамках разных предметов тем и законов; сетевые возможности компьютера позволяют выйти в поисках необходимой информации за рамки

учебной аудитории, того объема информации, которая предоставляется учителем или родителями.

- Памятка для обучающихся об информационной безопасности детей
  - [Информационная памятка для обучающихся для размещения на официальных Интернет-ресурсах](#)
  - [Памятка для родителей об информационной безопасности детей](#)
  - [Детские безопасные сайты](#)
1. На сайте гимназии размещаются документы, касающиеся организации образовательного процесса – расписание занятий; документы, регламентирующие работу школы и т.д.
  2. Принципы размещения информации на интернет-ресурсах ОУ призваны обеспечивать:
    - о соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
    - о защиту персональных данных обучающихся, учителей и других работников;
    - о достоверность и корректность информации.
  3. Персональные данные обучающихся (включая фамилию и имя, класс/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на интернет-ресурсах, создаваемых ОУ, только с письменного согласия родителей (законных представителей обучающихся). Персональные данные преподавателей и работников ОУ размещаются на его интернетресурсах только с письменного согласия лица, чьи персональные данные размещаются.

### **Классификатор информации, доступ к которой обучающихся запрещен**

1. Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения:
  - о информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию,
  - о антиобщественное поведение.
2. Злоупотребление свободой СМИ /экстремизм: информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы.
3. Злоупотребление свободой СМИ/ наркотические средства: сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганду каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров.

4. Злоупотребление свободой СМИ/ информация с ограниченным доступом: сведения о специальных средствах, технических приемах и тактике проведения контртеррористической операции.
  - воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, соединенное с насилием или угрозой его применения;

5. Злоупотребление свободой СМИ / скрытое воздействие : информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающих вредное влияние на их здоровье.
6. Экстремистские материалы или экстремистская деятельность (экстремизм):
- А) экстремистские материалы, т.е. предназначенные для обнародования документы либо информация, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал- социалистской рабочей партии Германии, фашистской партии Италии, публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы;
- Б) экстремистская деятельность (экстремизм) включает в себя деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков:
- насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации;
  - подрыв безопасности Российской Федерации;
  - захват или присвоение властных полномочий;
  - создание незаконных вооруженных формирований;
  - осуществление террористической деятельности либо публичное оправдание терроризма;
  - возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию;
  - унижение национального достоинства;
  - осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы;
  - пропаганду исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности;
  - публичную клевету в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, соединенную с обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке;

- применение насилия в отношении представителя государственной власти либо на угрозу применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей;
- посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность;
- нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением.

7. Вредоносные программы : программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.

8 . Преступления :

- клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию);
- оскорбление (унижение чести и достоинства другого лица, выраженное в неприлично форме);
- публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма;
- склонение к потреблению наркотических средств и психотропных веществ;
- незаконное распространение или рекламирование порнографических материалов;
- публичные призывы к осуществлению экстремистской деятельности;
- информация, направленная на пропаганду национальной, классовой, социальной Нетерпимости, а также пропаганду социального, расового, национального и религиозного неравенства;
- публичные призывы к развязыванию агрессивной войны.

9. Ненадлежащая реклама : информация, содержащая рекламу алкогольной продукции и табачных изделий.

10. Информация с ограниченным доступом: информация, составляющая государственную, коммерческую, служебную или иную специально охраняемую законом тайну.

**Классификатор информации, несовместимой с задачами образования**

1. Алкоголь: Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию.
2. Баннеры и рекламные программы: Баннерные сети, всплывающая реклама, рекламные программы. 3. Вождение и автомобили: (ресурсы данной категории, несовместимые с задачами образования).  
Несовместимая с задачами образования информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям.
4. Досуг и развлечения: (ресурсы данной категории, несовместимые с задачами образования). Несовместимая с задачами образования информация в виде фотоальбомов и рейтингов фотографий, открыток, гороскопов, сонников, гаданий, магии, астрологии, ТВ-программ, прогнозов погоды, тестов, рейтингов, фотоконкурсов, конкурсов онлайн, несовместимая с задачами образования информация о туризме, путешествиях, тостах, поздравлениях, кроссвордах, сканвордах, ответов к ним, фэнтези и фантастике, кулинарии, рецептах, диетах, моде, одежде, обуви, модных аксессуарах, показах мод, текстах песен, кино, киноактерах, расписаниях концертов, спектаклей, кинофильмов, заказе билетов в театры, кино и т.п., дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними, рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании, службах знакомств, размещении объявлений онлайн, анекдотах, приколах, слухах, сайтах и журналы для женщин и для мужчин, желтая пресса, онлайн-ТВ, онлайн радио, знаменитости, косметика, парфюмерия, прически, ювелирные украшения.

5. Здоровье и медицина: (ресурсы данной категории, несовместимые с задачами образования). Несовместимая с задачами образования информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иных материалах по теме «Здоровье и медицина», которые, являясь академическими, по сути, могут быть также отнесены к другим категориям, например, порнография, трупы и т.п.
6. Компьютерные игры: (ресурсы данной категории, несовместимые с задачами образования). Несовместимая с задачами образования компьютерные онлайн-овые и оффлайн-овые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты.
7. Корпоративные сайты, Интернет -представительства негосударственных учреждений: (ресурсы данной категории, несовместимые с задачами образования). Содержащие несовместимую с задачами образования информацию сайты коммерческих фирм, компаний, предприятий, организаций.
8. Личная и немодерируемая информация: Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники (блоги).
9. Отправка SMS с использованием Интернет-ресурсов Сайты, предлагающие услуги по отправке SMSсообщений 10. Модерируемые доски объявлений: (ресурсы данной категории, несовместимые с задачами образования). Содержащие несовместимую с задачами образования информацию модерируемые доски сообщений/объявлений, а также модерируемые чаты.
11. Нелегальная помощь школьникам и студентам: Банки готовых рефератов, эссе, дипломных работ и проч.
12. Неприличный и грубый юмор: Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека.
13. Нижнее белье, купальники: Сайты, на которых рекламируется и изображается нижнее белье и купальники.
14. Обеспечение анонимности пользователя, обход контентных фильтров: Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам. Peer — to- Peer программы, сервисы бесплатных прокси — серверов, сервисы, дающие пользователю анонимность
15. Онлайн — казино и тотализаторы: Электронные казино, тотализаторы, игры на деньги, конкурсы и проч.
16. Платные сайты: Сайты, на которых вывешено объявление о платности посещения веб-страниц. 17. Поиск работы, резюме, вакансии: (ресурсы данной категории, несовместимые с задачами образования) . Содержащие несовместимую с задачами образования Интернетпредставительства кадровых агентств, банки вакансий и резюме.
18. Поисковые системы: (ресурсы данной категории, несовместимые с задачами образования). Содержащие несовместимую с задачами образования Интернет-каталоги, системы поиска и навигации в сети Интернет.

19. 19. Религии и атеизм: (ресурсы данной категории, несовместимые с задачами образования). Сайты, содержащие несовместимую с задачами образования информацию религиозной направленности.
20. Системы поиска изображений. Системы для поиска изображений в сети Интернет по ключевому слову или словосочетанию.
21. СМИ: (ресурсы данной категории, несовместимые с задачами образования) Содержащие несовместимую с задачами образования информацию новостные ресурсы и сайты СМИ (радио, телевидения, печати)
22. Табак, реклама табака, пропаганда потребления табака: Сайты, пропагандирующие потребление табака. Реклама табака и изделий из него.
23. Торговля и реклама: (ресурсы данной категории, несовместимые с задачами образования). Содержащие несовместимую с задачами образования информацию сайты следующих категорий: аукционы, распродажи онлайн, Интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, недвижимость, аренда недвижимости,

покупка недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в сети Интернет, ебизнес

24. Убийства, насилие: Сайты, содержащие описания или изображения убийств, мертвых тел, насилия и т. п.

Сайты, пропагандирующие жестокое обращение с животными.

25. Чаты: (ресурсы данной категории, несовместимые с задачами образования). Несовместимые с задачами образования сайты для анонимного общения в режиме онлайн.
26. Здоровье: (ресурсы данной категории, несовместимые с задачами образования) Сайты, чаты, форумы секс меньшинств
27. Экология: (ресурсы данной категории, несовместимые с задачами образования) Сайты, призывающие к нанесению ущерба экологии, загрязнению окружающей среды и т. п.
28. Сбор средств через Интернет : Сайты с информацией для сбора материальных средств в пользу политических партий, религиозных, общественных организаций политической, коммерческой направленности, сект и т. п.
29. Пропаганда войны: (ресурсы данной категории, несовместимые с задачами образования) Сайты, рекрутирующие в организации военизированного толка, а также, могущие содержать информацию об изготовлении оружия в домашних условиях и т.п.

При использовании сети Интернет в ОУ учащимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и Республики Татарстан и которые имеют прямое отношение к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации в государственной интегрированной системе телекоммуникаций (ГИСТ), которые расположены в Центре обработки данных Правительства Республики Татарстан. На данных серверах ведется учет доступа в сеть Интернет (на сайте Электронное образование в Республике Татарстан, раздел Отчеты), а также

контентная фильтрация запрашиваемой информации. Контроль за учащимися в сети Интернет осуществляют:

- во время проведения занятий – преподаватель, проводящий занятие;
- во время использования сети Интернет для свободной работы учащихся — лицо, назначенное приказом директора школы по вопросам регламентации доступа к информации в Интернете.

1. [Информационное письмо МОиН РТ от 27.04.2012 № 5141/12 "О системе контентной фильтрации"](#)
2. [О контентной фильтрации Интернет ресурсов в общеобразовательных учреждениях РТ- независимая экспертиза ГАУ "ИТ-парк"](#)

Договор на предоставление услуг связи (Интернет) заключен с оператором связи ПАО

«Ростелеком». *Скорость интернета: «более 10 Мбит/с»*

[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 для размещения на официальных Интернет-ресурсах**

С каждым годом молодежи в интернете становится 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 патчи (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 твоём 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. Ещё в 1991 году нидерландская компания зарегистрировала бренд «WESA», что обозначало словосочетание «Wireless Fidelity», 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 Wi-Fi сети не являются безопасными.

Советы по безопасности работе 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 брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твоё устройство;
3. При использовании Wi-Fi отключи 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-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;

- Используй только защищенное соединение через HTTP'S, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
- 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:

- Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
- 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;
- 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;
- Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
- 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 нефитные 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. 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 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:

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 твоём 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 самую 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.

Пожалуйста 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, твоё 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 опубликовать 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 - 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!

### **Памятка для родителей об информационной безопасности детей**

Определение термина «информационная безопасность детей» содержится в Федеральном законе № 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 № 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 отталкивающим 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 слышаны 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 модерлируемых 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.

## Список безопасных сайтов для учащихся

<http://www.saferunet.ru> - Центр Безопасного Интернета в России.  
<http://www.friendlyrunet.ru> /- Фонд

«Дружественный Рунет». <http://www.microsoft.com> <http://www.icensor.ru/>-  
Интернет-фильтр для детей. [www.tirnet.ru](http://www.tirnet.ru) - Детский Интернет [www.ms-education.ru](http://www.ms-education.ru) и [www.apkpro.ru](http://www.apkpro.ru).

- электронный курс программы "Здоровье и безопасность детей в мире компьютерных технологий и Интернет  
<http://www.nedorusti.ru/> - социальный проект по защите прав детей «Не допусти»

<http://www.newseducation.ru/> - "Большая перемена"

<http://www.tvidi.ru/> - «Твиди» [www.mirbibigona.ru/](http://www.mirbibigona.ru/) -

«Страна друзей»: <http://www.smeshariki.ru/> - «Смешарики

<http://www.solnet.ee/> -

«Солнышко

<http://www.1001skazka.com> - «1001

сказка». <http://vkids.km.ru> Nachalka.info -

учись, играй, развивайся! <http://membrana.ru> –

«Люди. Идеи Технологии» <http://www.murzilka.org/>

- Сайт журнала «Мурзилка lib/1sentember.ru -

Школьная библиотека [skazvikt.ucoz.ru](http://skazvikt.ucoz.ru)

- Литературный детский журнал [www.rba.ru](http://www.rba.ru) –

Российская библиотечная ассоциация [www.rusla.ru](http://www.rusla.ru)

- Российская школьная библиотечная ассоциация

[schoollibrari.ioso.ru](http://schoollibrari.ioso.ru) – Сайт школьная библиотека

[www.bibliogid.ru](http://www.bibliogid.ru) – Библиогид [www.fsu-expert.ru](http://www.fsu-expert.ru) –

Общественногосударственная экспертиза учебников

[www.litera.edu.ru](http://www.litera.edu.ru) – Российский образовательный портал

[www.e-kniga.ru](http://www.e-kniga.ru) – Электронная библиотека художественной

литературы [lib.aldebaran.ru](http://lib.aldebaran.ru) – библиотека Альдебаран

[www.rvb.ru](http://www.rvb.ru) – Русская виртуальная библиотека

[www.mirslovarei.ru](http://www.mirslovarei.ru) – Коллекция электронных словарей

[www.prlib.ru](http://www.prlib.ru) – Президентская библиотека Б.Ельцина

[www.prosv.ru](http://www.prosv.ru) – издательство Просвещение [www.vgf.ru](http://www.vgf.ru) –

издательство Вентана-Граф [www.lbz.ru](http://www.lbz.ru) – издательство

БИНОМ. Лаборатория знаний [www.schoolpress.ru](http://www.schoolpress.ru) – Школьная

пресса