

МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«РАЙВАТТАЛЬСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА»

186700, Республика Карелия, Лахденпохский район, п.Хийтола, ул. Ленина, д.16. Тел.(81450) 4-45-45 ОКПО 57750784
ОГРН 1021000993639 ИНН/КПП 1012002131/101201001 E-mail: rssh66@mail.ru
(МОУ «Райваттальская СОШ»)

ПРИКАЗ

от 28.09.2022г.

№ 223-О

п. Хийтола

**Об информационной безопасности
МОУ «Райваттальская СОШ» и
назначении ответственного за
организацию работы с ресурсами
сети Интернет и ограничение
доступа**

В целях осуществления ограничения доступа обучающихся к ресурсам и материалам сети Интернет, не имеющим отношения к образовательному процессу, сохранности конфиденциальных сведений о логинах и паролях образовательного учреждения

ПРИКАЗЫВАЮ:

1. Утвердить:

- Правила использования сети Интернет (Приложение 1);
- Инструкцию для сотрудников школы о порядке действий при осуществлении контроля использования обучающимися сети Интернет (Приложение 2);
- Положение о сайте школы (Приложение 3);
- Правила организации доступа к сети Интернет в образовательной организации с системой классификации информации, запрещенной законодательством Российской Федерации к распространению, причиняющей вред здоровью и развитию детей, а также не совместимой с задачами образования и воспитания (Приложение 4).
- Инструкция для обучающихся по обеспечению информационной безопасности при использовании сети «Интернет» для размещения в учебных кабинетах, в которых осуществляется доступ в сеть «Интернет» (Приложение 5)

2. Назначить ответственным лицом за обеспечение эффективного и безопасного доступа к сети Интернет в школе всех участников образовательного процесса в соответствии с установленными в МОУ «Райваттальская СОШ» правилами и инструкциями учителя информатики Акуленко Е.В.

3. Контроль исполнения приказа возложить на заместителя директора Виноградову К.Е.

Директор



С.Ф. Корхонен

С приказом ознакомлены:

«28» 09 2022 г.  /Акуленко Е.В./

«28» 09 2022 г.  /Виноградова К.Е./

Правила использования сети Интернет

1. Общие положения

1.1. Использование сети Интернет в образовательном учреждении направлено на решение задач учебно-воспитательного процесса.

1.2. Настоящие Правила регулируют условия и порядок использования сети Интернет в образовательном учреждении.

1.3. Настоящие Правила имеют статус локального нормативного акта образовательного учреждения.

2. Организация использования сети Интернет в образовательном учреждении

2.1. Правила вводятся в действие приказом директора школы.

2.2. Директор школы отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в школе, а также за выполнение установленных правил.

2.3. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети Интернет осуществляет учитель, ведущий занятие.

При этом учитель:

наблюдает за использованием компьютера и сети Интернет обучающимися;

принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

2.4. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют работники.

Работник образовательного учреждения:

наблюдает за использованием компьютера и сети Интернет обучающимися;

принимает меры по пресечению обращений к ресурсам, не имеющих отношения к образовательному процессу;

сообщает классному руководителю о преднамеренных попытках обучающегося осуществить обращение к ресурсам, не имеющим отношения к образовательному процессу.

2.5. При использовании сети Интернет в школе обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношение к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в школе.

2.6. Пользователи сети Интернет в школе должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим существует вероятность обнаружения обучающимися ресурсов, не имеющих отношения к образовательному процессу и содержание которых противоречит законодательству Российской Федерации. Участникам использования сети Интернет в школе следует осознавать, что школа не несет ответственности за случайный доступ к подобной информации, размещенной не на интернет-ресурсах школы.

2.7. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническими средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в школе правилами обеспечивается учителем информатики.

2.8. Принципы размещения информации на интернет-ресурсах школы призваны обеспечивать:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защиту персональных данных обучающихся, учителей и сотрудников;
- достоверность и корректность информации.

2.9. 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 школой, только с письменного согласия родителей или иных законных представителей обучающихся.

Персональные данные учителей и сотрудников школы размещаются на ее интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.

2.10. В информационных сообщениях о мероприятиях, размещенных на сайте школы без уведомления и получения согласия упомянутых лиц или их законных представителей, могут быть указаны лишь фамилия и имя обучающегося либо фамилия, имя и отчество учителя, сотрудника или родителя.

2.11. При получении согласия на размещение персональных данных представитель школы обязан разъяснить возможные риски и последствия их опубликования. Школа не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

3. Использование сети Интернет в образовательном учреждении

3.1. Использование сети Интернет в школе осуществляется, как правило, в целях образовательного процесса.

3.2. По разрешению заместителя директора школы учителя, сотрудники и обучающиеся вправе:

- размещать собственную информацию в сети Интернет на интернет-ресурсах школы;
- иметь учетные записи на интернет-ресурсах школы.

3.3. Обучающемуся запрещается:

- обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
- осуществлять любые сделки через Интернет;
- осуществлять загрузки файлов на компьютер школы без специального разрешения;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

**Инструкция
для сотрудников МОУ «Райваттальская СОШ»
«О порядке действий при осуществлении контроля использования обучающимися
сети Интернет»**

1. Настоящая инструкция устанавливает порядок действий сотрудников школы при обнаружении:
 - обращения обучающихся к контенту, не имеющему отношения к образовательному процессу;
 - отказа при обращении к контенту, имеющему отношение к образовательному процессу, вызванного техническими причинами.
2. Контроль использования обучающимися сети Интернет осуществляют:
 - во время занятия — проводящий его учитель и (или) работник школы, специально выделенный для помощи в проведении занятий;
 - во время использования сети Интернет для свободной работы обучающихся — работники школы .
3. Учитель:
 - определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе соответствующих технических возможностей, а также длительность сеанса работы одного обучающегося;
 - наблюдает за использованием обучающимися компьютеров и сети Интернет;
 - способствует осуществлению контроля объемов трафика школы в сети Интернет;
 - запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;
 - доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;
 - принимает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.
4. При обнаружении ресурса, который, по мнению учителя, содержит информацию, запрещенную для распространения в соответствии с законодательством Российской Федерации, или иного потенциально опасного для обучающихся контента, он сообщает об этом учителю информатики.
5. В случае отказа доступа к ресурсу, разрешенному в школе, учитель также сообщает об этом учителю информатики.

ПОЛОЖЕНИЕ

об официальном сайте школы в информационно-телекоммуникационной сети ИНТЕРНЕТ и обновлении информации муниципального общеобразовательного учреждения «Райваттальская средняя общеобразовательная школа»
(МОУ «Райваттальская СОШ»)

1. Общие положения

1.1. Положение разработано в соответствии с Федеральным законом от 29.12. 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», статья 29;

Постановлением Правительства РФ от 20.10.2021 г. № 1802 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации, а также о признании утратившими силу некоторых актов и отдельных положений некоторых актов Правительства Российской Федерации».

1.2. Положение принимается педагогическим советом, имеющим право вносить в него изменения и дополнения, и утверждается приказом директора МОУ «Райваттальская СОШ»

1.3. Настоящее Положение регламентирует подготовку и размещение информации на сайте, организацию доступа к информации о деятельности образовательной организации. Сайт является общедоступным источником информации о деятельности образовательной организации. Электронный адрес сайта: <https://raivatala.karelschool.ru/> Информация, размещаемая на сайте, является публичной, бесплатной и круглосуточно доступной для пользователей.

2. Цели и задачи сайта

2.1. Целью настоящего Положения является: обеспечение информационной открытости деятельности образовательной организации, своевременного доступа к значимой информации для участников образовательного процесса; развитие информационного пространства образовательной организации, участие в едином информационном пространстве; осуществление связи с общественностью на основе использования возможностей сети Интернет.

2.2. Основными задачами сайта являются:

2.2.1. обеспечение права граждан на получение информации о деятельности образовательной организации (в том числе органов самоуправления);

2.2.2. обеспечение доступа пользователей сайта к разрешительным документам по организации образовательного процесса, текстам нормативно-правовых локальных актов образовательной организации, а также других официальных документов;

2.2.3. всестороннее информирование пользователей сайта о школьной жизни, истории образовательной организации, структуре органов управления школой, наиболее значимых событиях в школе, ходе приема документов для зачисления в школу, итогах обучения в школе («Электронный классный журнал»);

2.2.4. предоставление справочной информации об организации образовательного процесса в школе для всех категорий участников образовательного процесса, внеклассной и внеурочной деятельности; изучение общественного мнения, выявление наиболее значимых проблем школ

3. Содержание сайта

3.1. Образовательные организации формируют открытые и общедоступные информационные ресурсы, содержащие информацию об их деятельности, и обеспечивают доступ к ресурсам посредством размещения их в информационно-телекоммуникационных сетях, в том числе на официальном сайте образовательной организации в сети "Интернет".

3.2. Образовательные организации обеспечивают открытость и доступность:

1) информации:

а) о дате создания образовательной организации, об учредителе, учредителях образовательной организации, о месте нахождения образовательной организации и филиалов (при наличии), режиме, графике работы, контактных телефонах и об адресах электронной почты. При размещении информации о местах осуществления образовательной деятельности, сведения о которых в соответствии с Федеральным законом «Об образовании в Российской Федерации» не включаются в

соответствующую запись в реестре лицензий на осуществление образовательной деятельности, данные указываются в виде адреса места нахождения, в том числе:

- места осуществления образовательной деятельности при использовании сетевой формы реализации образовательных программ;
- места проведения практики;
- места проведения практической подготовки обучающихся;
- места проведения государственной итоговой аттестации;
- места осуществления образовательной деятельности по дополнительным образовательным программам;

б) о структуре и об органах управления образовательной организацией указывается в том числе:

- наименование структурных подразделений (органов управления);
- фамилии, имена, отчества (при наличии) и должности руководителей структурных подразделений;
- места нахождения структурных подразделений;
- адреса официальных сайтов в сети «Интернет» структурных подразделений (при наличии);
- адреса электронной почты структурных подразделений (при наличии);
- сведения о наличии положений о структурных подразделениях (об органах управления) с приложением указанных положений в виде электронных документов, подписанных простой электронной подписью в соответствии с Федеральным законом «Об электронной подписи»

в) о реализуемых образовательных программах, включая адаптированные образовательные программы (при наличии) с указанием учебных предметов, курсов, дисциплин (модулей), практики, предусмотренных соответствующей образовательной программой (за исключением образовательных программ дошкольного образования), для каждой из них указывается следующая информация:

- об уровне общего или профессионального образования, о наименовании образовательной программы (для общеобразовательных программ);
- о форме обучения (за исключение образовательных программ дошкольного образования);
- о нормативном сроке обучения;

г) о численности обучающихся по реализуемым образовательным программам за счет бюджетных ассигнований федерального бюджета, бюджетов субъектов Российской Федерации, местных бюджетов и по договорам об образовании за счет средств физических и (или) юридических лиц размещается в форме электронного документа, подписанного простой электронной подписью в соответствии с Федеральным законом «Об электронной подписи». Информация указывается по каждой образовательной программе;

д) о языках образования размещается в форме электронного документа, подписанного простой электронной подписью в соответствии с Федеральным законом «Об электронной подписи», с приложением образовательной программы;

е) о федеральных государственных образовательных стандартах, об образовательных стандартах (при их наличии) размещается в форме электронного документа, подписанного простой электронной подписью в соответствии с Федеральным законом «Об электронной подписи» (в части документов, самостоятельно разрабатываемых и утвержденных образовательной организацией);

ж) о руководителе образовательной организации, его заместителях, руководителях филиалов образовательной организации (при их наличии) указываются в том числе:

- фамилия, имя, отчество (при наличии) руководителя, его заместителей;
- должность руководителя, его заместителей;
- контактные телефоны;
- адреса электронной почты.

з) о персональном составе педагогических работников указываются в том числе:

- фамилия, имя, отчество (при наличии) педагогического работника;
- занимаемая должность;
- преподаваемые учебные предметы, курсы, дисциплины (модули);
- уровень (уровни) профессионального образования с указанием наименования направления подготовки и (или) специальности, в том числе научной, и квалификации;
- ученая степень (при наличии);
- ученое звание (при наличии);
- сведения о повышении квалификации (за последние 3 года);

- сведения о профессиональной переподготовке (при наличии);
- сведения о продолжительности опыта (лет) работы в профессиональной сфере, соответствующей образовательной деятельности по реализации учебных программ, курсов, дисциплин (модулей);
- наименование общеобразовательной программы (общеобразовательных программ), в реализации которых участвует педагогический работник.

и) о материально-техническом обеспечении образовательной деятельности (в том числе о наличии оборудованных учебных кабинетов, объектов для проведения практических занятий, библиотек, объектов спорта, средств обучения и воспитания, об условиях питания и охраны здоровья обучающихся, о доступе к информационным системам и информационно-телекоммуникационным сетям, об электронных образовательных ресурсах, к которым обеспечивается доступ обучающихся в том числе в отношении инвалидов и лиц с ограниченными возможностями здоровья, включая указание на обеспечение их доступа в здания образовательной организации и наличие для них специальных технических средств обучения коллективного и индивидуального пользования).

Образовательная организация при размещении информации об условиях питания обучающихся по образовательным программам начального общего образования размещает в том числе меню ежедневного горячего питания, информацию о наличии диетического меню в образовательной организации, перечни юридических лиц и индивидуальных предпринимателей, оказывающих услуги по организации питания в образовательной организации, перечни юридических лиц и индивидуальных предпринимателей, поставляющих (реализующих) пищевые продукты и продовольственное сырье в образовательную организацию, формы обратной связи для родителей обучающихся и ответы на вопросы родителей по питанию;

к) о количестве вакантных мест для приема (перевода) по каждой образовательной программе (на места, финансируемые за счет бюджетных ассигнований федерального бюджета, бюджетов субъектов Российской Федерации);

л) о наличии и об условиях предоставления обучающимся стипендий, мер социальной поддержки;

м) о наличии общежития, интерната, количестве жилых помещений в общежитии, интернате для иногородних обучающихся, формировании платы за проживание в общежитии. Эта информация указывается в том числе в отношении инвалидов и лиц с ограниченными возможностями здоровья, включая указание на обеспечение их доступа в здания образовательной организации и наличие для них специальных технических средств обучения коллективного и индивидуального пользования;

н) об объеме образовательной деятельности, финансовое обеспечение которой осуществляется за счет бюджетных ассигнований федерального бюджета, бюджетов субъектов Российской Федерации, местных бюджетов, по договорам об образовании за счет средств физических и (или) юридических лиц;

о) о поступлении финансовых и материальных средств и об их расходовании по итогам финансового года;

п) о трудоустройстве выпускников прошлого учебного года;

2) копий:

а) устава образовательной организации;

б) лицензии на осуществление образовательной деятельности (с приложениями);

в) свидетельства о государственной аккредитации (с приложениями);

г) плана финансово-хозяйственной деятельности образовательной организации, утвержденного в установленном законодательством Российской Федерации порядке, или бюджетной сметы образовательной организации;

д) локальных нормативных актов, предусмотренных частью 2 статьи 30 настоящего Федерального закона, правил внутреннего распорядка обучающихся, правил внутреннего трудового распорядка, коллективного договора;

3) отчета о результатах самообследования. Показатели деятельности образовательной организации, подлежащей самообследованию, и порядок его проведения устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере образования; 4) документа о порядке оказания платных образовательных услуг, в том числе образца договора об оказании платных образовательных услуг, документа об утверждении стоимости обучения по каждой образовательной программе;

5) предписаний органов, осуществляющих государственный контроль (надзор) в сфере образования, отчетов об исполнении таких предписаний. Копии предписаний органов, осуществляющих государственный контроль (надзор) в сфере образования, размещаются на официальном сайте

образовательной организации до подтверждения указанными органами исполнения предписания или признания его недействительным в установленном законом порядке (при наличии);

б) иной информации, которая размещается, публикуется по решению образовательной организации и (или) размещение, опубликование которой являются обязательными в соответствии с законодательством Российской Федерации.

3.3. В целях обеспечения осуществления мониторинга системы образования образовательная организация размещает на официальном сайте информацию о заключенных и планируемых к заключению договорах с иностранными и (или) международными организациями по вопросам образования и науки.

3.4. Информация и документы, указанные в пункте 3.2, если они в соответствии с законодательством Российской Федерации не отнесены к сведениям, составляющим государственную и иную охраняемую законом тайну, подлежат размещению на официальном сайте образовательной организации в сети "Интернет" и обновлению в течение десяти рабочих дней со дня их создания, получения или внесения в них соответствующих изменений. Порядок размещения на официальном сайте образовательной организации в сети "Интернет" и обновления информации об образовательной организации, в том числе ее содержание и форма ее предоставления, устанавливается Правительством Российской Федерации. При размещении информации на официальном сайте и ее обновлении обеспечивается соблюдение требований законодательства Российской Федерации о персональных данных.

3.5. Текущая информация (информация о текущих событиях, актуальная и представляющая интерес в течение небольшого промежутка времени)

3.5.1. Новости (короткие сообщения на главной странице).

3.5.2. Анонсы ближайших олимпиад и мероприятий (с целью привлечения внимания к мероприятию и стимулирования участия в нём).

3.5.3. Результаты олимпиад и других мероприятий (по мере поступления, но в кратчайшие сроки; публикация результатов с целью первоочередного информирования; в том числе публикация результатов экзаменов сразу после проверки работ) и др..

3.6. Сервисы обратной связи и общения.

3.7. Прочая информация (обусловленная специфическими особенностями Сайта как информационного объекта в сети Интернет)

3.7.1. Полезные ссылки (ссылки на ресурсы, рекомендуемые посетителям Сайта – в основном, образовательные и официальные ресурсы органов управления образованием), включающие в себя ссылку на официальные сайты Министерства просвещения Российской Федерации в сети «Интернет».

4. Технические особенности.

4.1. Директором школы назначается Администратор сайта, имеющий доступ к редактированию материалов Сайта в сети Интернет (обладающей соответствующими паролями).

4.2. Администратор Сайта в своих действиях руководствуется настоящим Положением и законодательством РФ.

4.3. Дизайн сайта формируется оптимальным образом в рамках имеющихся возможностей.

4.4. Перемещение между страницами Сайта осуществляется с помощью навигационного меню.

4.5. Администратор Сайта проводит систематическую работу по обеспечению круглосуточного функционирования сайта; копированию данных, необходимых для восстановления работы сайта; содействию в размещении информации на сайте работниками Школы.

4.6. Технологические и программные средства, которые используются для функционирования официального сайта, должны обеспечивать:

а) доступ к размещенной на официальном сайте информации без использования программного обеспечения, установка которого на технические средства пользователя информации требует заключения лицензионного или иного соглашения с правообладателем;

б) защиту информации от уничтожения, модификации и блокирования доступа к ней, а также иных неправомерных действий в отношении нее;

в) возможность копирования информации на резервный носитель, обеспечивающий ее восстановление.

5. Ответственность за информационное и техническое обеспечение сайта

5.1. Ответственность за своевременность представления, достоверность и полноту информации, представляемой для размещения на сайте, несут лица, ответственные за подготовку, сбор и передачу материалов для размещения на сайте.

5.2. Ответственность за своевременность размещения информации, представляемой лицами, ответственными за подготовку, сбор и передачу материалов для размещения на сайте, несет ответственный за работу с сайтом и заместитель директора

5.3. Ответственность за ежедневное выкладывание меню несет заведующий хозяйством.

5.4. Администратор Сайта подчинён директору школы, который информируется обо всех проблемных ситуациях в сфере деятельности Администратора Сайта. Все спорные вопросы и вопросы ответственности Администратора Сайта решаются только с указанными должностными лицами.

6. Функции Администратора Сайта

6.1. Администратор Сайта обладает всеми правами полного управления Сайтом.

6.2. Решения и действия Администрации Сайта, предполагающие существенные изменения или затрагивающие чьи-либо интересы, фиксируются в письменной форме.

6.3. Функции администратора

6.3.1. контроль за соблюдением настоящего Положения и иных норм;

6.3.2. признание и устранение нарушений;

6.3.3. обновление информации на Сайте;

6.3.4. организация сбора и обработки необходимой информации;

6.3.5. передача вопросов посетителей их адресатам и публикация ответов;

6.3.6. обработка электронных писем;

Правила организации доступа к сети Интернет в образовательной организации с системой классификации информации, запрещенной законодательством Российской Федерации к распространению, причиняющей вред здоровью и развитию детей, а также не совместимой с задачами образования и воспитания

1. Общие положения

1.1. В соответствии со статьей Федерального закона от 29 декабря 2010 г. № 4Э6-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее - Федеральный закон № 436-ФЗ) доступ детей к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, в местах, доступных для детей, предоставляется лицом, организующим доступ к сети Интернет в таких местах, другим лицам при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию. МОУ «Райваттальская СОШ» (далее - школа), предоставляющая детям доступ к сети Интернет, обязана применять указанные выше меры по защите детей от информации, причиняющей вред их здоровью и (или) развитию.

1.2. Основным исполнителем комплекса мер, обеспечивающих исключение доступа обучающихся школы к ресурсам сети Интернет, содержащим информацию, причиняющую вред здоровью и развитию детей, а также несовместимую с задачами образования и воспитания обучающихся, является школа, а основной формой реализации мер - выбор и использование средств контентной фильтрации и принятие школой правил и регламентов использования сети Интернет, имеющих статус локальных актов (административных и организационных мер).

1.3. Использование сети Интернет в школе направлено на решение задач учебно-воспитательного процесса.

1.4. Настоящие Правила регулируют условия и порядок использования сети Интернет в школе.

1.5. Настоящие Правила имеют статус локального нормативного акта школы.

2. Организация использования сети Интернет в школе

2.1. Вопросы использования возможностей сети Интернет в учебно-образовательном процессе рассматриваются на педагогическом совете школы.

Правила организации доступа к сети Интернет в школе вводятся в действие приказом директор школы.

2.2. Правила организации доступа к сети Интернет разрабатываются на основе типовых Правил, либо образовательной организацией самостоятельно с привлечением внешних экспертов, в качестве которых могут выступать:

- педагогические работники других образовательных организаций, имеющие опыт использования Интернета в образовательном процессе;
- специалисты в области информационных технологий;
- представители органов управления образованием;
- родители обучающихся.

2.3. При разработке правил организации доступа к сети Интернет школа руководствуется:

- законодательством Российской Федерации, в том числе Федеральным законом от 29 декабря 2010 г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", Федеральным законом от 25.07.2002 г. № 114-ФЗ «О противодействии экстремистской деятельности», Федеральным законом от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», Федеральным законом от

27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- опытом целесообразной и эффективной организации учебного процесса с использованием информационных технологий и возможностей Интернета;
- интересами обучающихся;
- целями образовательного процесса;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

2.4. Директор школы отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в школе, а также за выполнение установленных правил. Для обеспечения доступа участников образовательного процесса к сети Интернет в соответствии с установленным в школе правилами директор назначает своим приказом ответственного за организацию работы с ресурсами сети Интернет и ограничение доступа.

2.5. Ответственный за организацию работы с ресурсами сет Интернет и ограничение доступа:

- принимает меры по защите обучающихся от информации, распространение которой запрещено в соответствии с законодательством Российской Федерации, независимо от возрастного ценза пользователей информации (в соответствии с классификацией информации, приведенной в приложении), от информации, распространение которой запрещено для отдельных возрастных категорий детей в соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", от информации не совместимой с задачами обучения и воспитания, если классификация такой информации установлена на уровне образовательной организации.

- принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет.

2.6. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети Интернет осуществляет учитель, ведущий занятие.

При этом учитель:

- наблюдает за использованием компьютера и сети Интернет обучающимися;
- принимает меры по пресечению обращений к ресурсам, содержащим информацию, причиняющую вред здоровью и развитию детей, а также не совместимую с задачами образования и воспитания;

- наблюдает за появлением отказов при обращении к контенту, имеющему отношение к образовательному процессу, вызванных техническими причинами.

2.7. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют работники школы, определенные приказом директора школы.

Работник школы:

- наблюдает за использованием компьютера и сети Интернет обучающимися;
- принимает меры по пресечению по пресечению обращений к ресурсам, не имеющих отношения к образовательному процессу;
- сообщает классному руководителю о преднамеренных попытках обучающегося осуществить обращение к ресурсам, содержащим информацию, причиняющую вред здоровью и развитию детей, а также не совместимую с задачами образования и воспитания.

2.8. При использовании сети Интернет в школе обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношения к образовательному процессу. Выполнение такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в школе или предоставленного оператором услуг связи.

2.9. Пользователи сети Интернет в школе должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим существует вероятность обнаружения обучающимися ресурсов, содержащих информацию, распространение которой запрещено в соответствии с законодательством Российской Федерации. При обнаружении факта доступа к

таким ресурсам из школы учитель, классный руководитель должен незамедлительно сообщить об этом ответственному за организацию работы с ресурсами сети Интернет и ограничение доступа.

2.10. В случае обнаружения пользователями информации, распространение которой запрещено для отдельных возрастных категорий детей в соответствии с Федеральным законом от 29 декабря 2010 г. № 4Э6-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (2 класса в соответствии с прилагаемой классификацией) ответственный за организацию работы с ресурсами сети Интернет и ограничение доступа принимает меры к ограничению доступа к противоправному ресурсу средствами контентной фильтрации.

2.11. В случае обнаружения пользователями информации, распространение которой запрещено в соответствии с законодательством Российской Федерации, независимо от возрастного ценза пользователей информации, ответственный за организацию работы с ресурсами сети Интернет и ограничение доступа сообщает адрес данного ресурса на официальном сайте Роскомнадзора в Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено <http://eais.rkn.gov.ru/feedback/>, либо направляет информацию о противоправном контенте на электронный адрес «горячей линии» Роскомнадзора zapretinfo@rsoc.ru.

2.12. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническими средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в школе правилами обеспечивается ответственным за организацию работы с ресурсами сети Интернет и ограничение доступа.

2.13. Педагогические работники, проводящие занятия с обучающимися с использованием ресурсов сети Интернет, обязаны знать классификацию информационной продукции, распространение которой запрещено на территории Российской Федерации, причиняющей вред здоровью и развитию детей, а также информации, не совместимой с задачами обучения и воспитания.

3. Правила работы в сети Интернет

3.1. Обучающемуся запрещается:

- обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (в соответствии с утвержденным в школе классификатором);
- осуществлять любые сделки через Интернет;
- осуществлять загрузки файлов на компьютер образовательной организации без специального разрешения;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.2. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, обучающийся обязан незамедлительно сообщить об этом учителю, проводящему занятие. Учитель обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом лицу, ответственному за организацию работы с ресурсами сет Интернет и ограничение доступа.

Ответственный за организацию работы с ресурсами сет Интернет и ограничение доступа обязан:

- принять информацию от учителя;
- принять меры к ограничению доступа к противоправному ресурсу средствами контентной фильтрации, либо сообщить о противоправном контенте в Роскомнадзор.

**Система классификации информации,
запрещенной законодательством Российской Федерации к распространению,
причиняющей вред здоровью и развитию детей, а также не совместимой с задачами
образования и воспитания**

Система классификация информации, запрещенной законодательством Российской Федерации к распространению, причиняющей вред здоровью и развитию детей и не имеющей отношения к образовательному процессу, представляет собой три класса категорий информации.

К 1 классу относится информация, **распространение которой запрещено** в соответствии с законодательством Российской Федерации, **независимо от возрастного ценза** пользователей информации.

Перечень такой информации установлен Федеральным законом от 25.07.2002 N 114-ФЗ "О противодействии экстремистской деятельности" и Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

В соответствии со ст. 5, 8, 11 Федерального закона от 25.07.2002 N 114-ФЗ "О противодействии экстремистской деятельности" запрещены к распространению экстремистские материалы - предназначенные для обнародования документы либо информация на иных носителях, 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.

В соответствии со ст. 15 Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" запрещено распространение в информационно-коммуникационных сетях (независимо от возраста пользователей информации):

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами.

Ко 2 классу относится информация, распространение которой **запрещено для отдельных возрастных категорий детей** в соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

Частью 2 статьи 5 Федерального закона № 436-ФЗ к информации, запрещенной для распространения среди детей, отнесена информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способная 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;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;

4) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера (понятие информации порнографического характера дано в ст. 2 Федерального закона № 436-ФЗ);

8) о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

На основании обобщения **1 и 2 класса информации**, распространение которых **запрещено в образовательных организациях для детей**, подготовлена классификация информации по тематическим категориям.

п/п	Тематическая категория	Содержание информации
1	Насилие и жестокость	Информация, обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных Федеральным законом № 436-ФЗ; изображение или описание сексуального насилия; насилие и жестокость представляются естественной нормой отношений между людьми; насилие и жестокость представляются правомерным и эффективным средством решения проблем и оправдываются; дегуманизация жертв насилия; описание, изображение или детальное натуралистическое описание пыток, истязаний, мучений, глумление над жертвой, т.е. причинение жертве дополнительных страданий; демонстрация, описание способов нанесения увечий; демонстрация способов лишения жизни; демонстрация, описание, надругательства над телами умерших и местами их захоронения; натуралистическое изображение или описание трупов людей.
2	Антиобщественные, противоправные действия или преступления	Информация, способная 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; описание или демонстрация приготовления наркотических веществ, взрывчатых или ядовитых веществ, оружия; действия, поощряющие или призывающие детей на употребление товаров и услуг, опасных для жизни и здоровья (наркотиков, одурманивающих и психотропных средств,

		<p>алкоголя, никотина и т.п.);</p> <p>информация, оправдывающая противоправное поведение;</p> <p>призыв к уголовно наказуемым деяниям, совершение актов вандализма и надругательства над общенациональными культурно-историческими ценностями; суицидальное поведение и членовредительство как одобряемое</p>
3	Сексуальные отношения	<p>Информация порнографического характера - информация, представляемая в виде натуралистических изображений или описания половых органов человека и (или) полового сношения либо сопоставимого с половым сношением действия сексуального характера, в том числе такого действия, совершаемого в отношении животного включая изображение или имитацию действий сексуального характера, натуралистическое описание таких действий;</p> <p>изображение половых органов,</p> <p>изображение или детальное описание участия в сексуальном поведении;</p> <p>секстинг (самостоятельная публикация собственных изображений сексуализированного характера);</p> <p>изображение или имитация действий сексуального характера по отношению к ребёнку, в том числе в «личном пространстве» ребёнка;</p> <p>изображение половых органов ребёнка в сексуальных целях;</p> <p>изображение или детализированное натуралистическое описание участия ребёнка в сексуальном поведении</p>
4	Совершение действий, представляющих угрозу жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству	<p>Информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству</p>
5	Язык	<p>Употребление ненормативной лексики,</p> <p>наличие бранных, вульгарных нецензурных слов, ненормативные речевые обороты и выражения, сходные до степени смешения с нецензурными</p>
6	Объекты, вызывающие страх, ужас, панику	<p>Информация, представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий</p>
7	Семейные ценности	<p>Информация, отрицающая семейные ценности и формирующую неуважение к родителям и (или) другим членам семьи.</p> <p>Отрицание или принижение ценности социальных институтов семьи, устойчивого брака;</p> <p>дискредитация семейных ценностей материнства и отцовства;</p>

		искажение ориентации и успеха установок в брачно-семейной сфере (пропаганда вне семейных отношений, измены, девиантные формы взаимоотношений полов)
8	Информация о несовершеннолетнем, пострадавшем в результате противоправных действий	Информация о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего
9	Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения	Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение
10	Экстремистские материалы или экстремистская деятельность (экстремизм)	<p>а) Экстремистские материалы, то есть предназначенные для обнародования документы или 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;</p> <p>б) экстремистская деятельность (экстремизм) включает деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков:</p> <ul style="list-style-type: none"> — насильственное изменение основ конституционного строя 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; — пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к

		<p>религии, социальной, расовой, национальной, религиозной или языковой принадлежности;</p> <p>— воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, сопровождаемое насилием или угрозой его применения;</p> <p>— публичная клевета 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, сопровождаемая обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке;</p> <p>— применение насилия в отношении представителя государственной власти либо угроза применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей;</p> <p>— посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность;</p> <p>— 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</p>
11	Ненадлежащая реклама	Информация, содержащая рекламу алкогольной продукции и табачных изделий

К 3 классу относится информация, распространение которой **не запрещено** в соответствии с законодательством Российской Федерации, в том числе среди детей, **но доступ к которой может быть ограничен** из образовательной организации в связи с тем, что данная информация не соответствует задачам образования и воспитания и не имеет отношения к образовательному процессу.

Образовательная организация свободна в выборе и применении классификаторов информации, не имеющей отношения к образовательному процессу, а также несет ответственность за невыполнение функций, отнесенных к его компетенции.

Классификатор информации, отнесенной к **3 классу**, утверждается локальным актом образовательной организации (решением педагогического совета, положением, приказом и т.д.) и может пополняться и расширяться с соблюдением Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Приводимый далее перечень категорий классификатора информации, не имеющей отношения к образовательному процессу, носит рекомендательный характер и может быть дополнен, расширен или иным образом изменен в установленном порядке, в том числе с учетом специфики образовательной организации.

п/п	Тематическая категория	Содержание информации
1	Досуг и развлечения	Не имеющая отношения к образовательному процессу информация:

		<ul style="list-style-type: none"> — рейтинги открыток, гороскопов, сонников; — гадания, магия и астрология; — ТВ-программы; — прогнозы погоды; — тосты, поздравления; — кроссворды, сканворды, ответы к ним; — кулинария, рецепты, диеты; — мода, одежда, обувь, модные аксессуары, показы мод; — тексты песен, кино, киноактеры, расписания концертов, спектаклей, кинофильмов, заказ билетов в театры, кино и т.п.; — о службах знакомств, размещении объявлений онлайн; — анекдоты, «приколы», слухи; — о сайтах и журналах для женщин и для мужчин; — о знаменитостях; — о косметике, парфюмерии, прическах, ювелирных украшениях.
2	Здоровье и медицина	Информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иные материалы на тему «Здоровье и медицина», которые, являясь академическими, по сути, могут быть также отнесены к другим категориям (порнография, трупы и т.п.)
3	Компьютерные игры	Не имеющие отношения к образовательному процессу компьютерные онлайн-овые и оффлайн-овые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты
4	Корпоративные сайты, интернет – представительства негосударственных учреждений	Содержащие информацию, не имеющую отношения к образовательному процессу, сайты коммерческих фирм, компаний, предприятий, организаций
5	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
6	Отправка SMS с использованием интернет - ресурсов	Сайты, предлагающие услуги по отправке SMS-сообщений
7	Модерируемые доски объявлений	Содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты
8	Нелегальная помощь школьникам и студентам	Банки готовых рефератов, эссе, дипломных работ и пр.
9	Онлайн-казино и тотализаторы	Электронные казино, тотализаторы, игры на деньги, конкурсы и пр.

Инструкция для обучающихся по обеспечению информационной безопасности при использовании сети «Интернет» для размещения в учебных кабинетах, в которых осуществляется доступ в сеть «Интернет»

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 зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;
2. Постоянно устанавливай пачки (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 ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд "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 высшей звуковой техники Hi-Fi, что в переводе означает "высокая точность".

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие - то номера;
2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твоё устройство;
3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;
4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;

5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://";

6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi автоматически". Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;

3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные 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. 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 интернетсервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;

2. Управляй своей киберрепутацией;

3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

5. Соблюдай свою виртуальную честь смолоду;

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие - то платные услуги;

Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

Необходимо обновлять операционную систему твоего смартфона;
Используй антивирусные программы для мобильных телефонов;
Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;

Периодически проверяй, какие платные услуги активированы на 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. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
3. Не указывай личную информацию в профайле игры;
4. Уважай других участников по игре;
5. Не устанавливай неофициальные патчи и моды;
6. Используй сложные и разные пароли;
7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" - это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то 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 установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

О портале

Сетевичок.рф - твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином!

ИНСТРУКЦИЯ ДЛЯ ОБУЧАЮЩИХСЯ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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, придирается, 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!