

Положение
об административных и организационных мерах, технических,
программно-аппаратных средствах, применяемых в МАОУ «СГ № 14»
для защиты детей от информации, причиняющей вред их здоровью и (или)
развитию, распространяемой посредством сети Интернет

1. Общие положения

1.1. Положение об административных и организационных мерах, технических, программно-аппаратных средствах, применяемых в МАОУ «СГ № 14» для защиты детей от информации, причиняющей вред их здоровью и(или) развитию, распространяемой посредством сети Интернет разработано в соответствии с федеральными нормативно правовыми актами, учет которых обязателен для деятельности образовательной организации, а также с учетом Методических рекомендаций по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и(или) развитию детей, а также не соответствующей задачам образования (письмо Минпросвещения России от 07.06.2019 №04-474).

1.2. Положение является локальным актом МАОУ «СГ № 14» (далее - Гимназия), обязательным для всех участников образовательных отношений в Гимназии, посетителей Гимназии.

1.3. Положение регулирует применение административных и организационных мер, технических, программно-аппаратных средств для защиты детей от информации, причиняющей вред их здоровью и(или) развитию, распространяемой посредством сети Интернет.

1.4. Использование сети Интернет в Гимназии направлено на решение задач образовательного процесса.

1.5. К компетенции Гимназии среди прочего относится создание безопасных условий обучения, в том числе при проведении практической подготовки обучающихся, а также безопасных условий воспитания обучающихся, присмотра и ухода за обучающимися, в соответствии с установленными нормами, обеспечивающими жизнь и здоровье обучающихся, работников Гимназии.

1.6. Информационная безопасность детей - это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. Гимназия в рамках своей работы должна обеспечивать информационную безопасность своих обучающихся.

2. Технические и программно-аппаратные средства, применяемые в МАОУ «СГ № 14» для защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети Интернет

2.1. Гимназия имеет право самостоятельно принимать решения о технологиях и формах организации системы ограничения обучающихся к информации, причиняющей вред их здоровью и (или) развитию (далее - негативная информация).

2.2. К основной технологии организации системы ограничения обучающихся к негативной информации, используемой в Гимназии, является система контентной фильтрации (далее - СКФ), которая обеспечивает ограничение доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред

здоровью и (или) развитию детей, а также не соответствующая задачам образования.

2.3. Технологии организации системы ограничения обучающихся к негативной информации в Гимназии включают:

2.3.1. контентную фильтрацию и ограничение доступа обучающихся к информации, включенной в Перечень видов информации, запрещенной к распространению посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования в соответствии с Положением об ограничении в МАОУ «СГ № 14» доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

2.3.2. контентную фильтрацию и предоставление доступа обучающимся к сайтам в сети "Интернет", включенных в Реестр безопасных образовательных сайтов в соответствии с Положением об ограничении в МАОУ «СГ № 14» доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

2.4. СКФ, используемые в Гимназии, должна соответствовать ряду требований.

2.4.1. Применяемые при разработке и использовании интерфейсов технологии, стандарты и спецификации должны соответствовать нормативно установленным и общепринятым стандартам и требованиям в области информационных технологий и программного обеспечения.

2.4.2. При использовании сетевых протоколов передачи данных рекомендуется придерживаться следующих спецификаций:

- протокол передачи гипертекста версии 1.11 - RFC 2616;
- расширенный протокол передачи гипертекста версии 1.1 с обеспечением безопасности транспортного уровня;
- протокол защищенных соединений (SSL) версии 3 - RFC 5246;
- протоколы использования системы поддержки пространства имен - FC 1035.

2.4.3. При описании данных, а также информации о данных, их составе и структуре, содержании, формате представления, методах доступа и требуемых для этого полномочиях пользователей, о месте хранения, источнике, владельце и др. (далее - метаданные) и используемых наборах символов, применяемых в процессе информационного обмена, рекомендуется придерживаться следующих спецификаций:

- расширяемый язык разметки XML-набор стандартов Консорциума Всемирной паутины;
- расширяемый язык описания схем данных (XML Schema) версии не ниже 1.0.

2.4.4. Описания разрабатываемых электронных сервисов и описания схем данных, согласно базовому профилю интероперабельности версии 1.1, рекомендуется создавать в кодировке UTF-8 или UTF-16 (с указанием этой кодировки в заголовке соответствующего описания).

2.4.5. Аутентификацию рекомендуется обеспечить на основе сертификатов PKI в формате X.509.

2.5. В зависимости от технологии СКФ должна обеспечивать следующие основные функции:

2.5.1. осуществлять в режиме реального времени анализ сайтов в сети "Интернет", к которым обращаются пользователи, на предмет отсутствия на сайтах в сети "Интернет" информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

2.5.2. пропускать, блокировать или модифицировать информацию от сайта к пользователю в зависимости от результатов проверки;

2.5.3. автоматически передавать данные во внешнюю систему о сайте, информация из которого удовлетворяет заданным правилам;

2.5.4. Собирать статистику фильтрации.

2.6. СКФ должна обеспечивать возможность анализа информационной продукции в любой форме и виде, в частности возможность:

2.6.1. семантического и морфологического анализа информации сайтов, получаемых по HTTP протоколу, на основе списков запрещенных слов,

словообразований и словосочетаний, содержащих информацию, причиняющую вред здоровью и (или) развитию детей, а также не соответствующую задачам образования, а также сочетаний слов, образующих совокупности запрещенных выражений; информация сайтов должна интерпретироваться строго согласно стандартам на протокол передачи гипертекста и язык разметки гипертекста, в том числе должна корректно определяться кодировка передаваемых данных;

2.6.2. анализа поисковых HTTP-запросов путем разбора запроса, сформированного поисковыми машинами, и сравнением составных частей запроса со словарем слов, словосочетаний и словообразований, содержащих информацию, причиняющую вред здоровью и (или) развитию детей, а также не соответствующую задачам образования; СКФ должна поддерживать множество категорий запрещенных слов, словообразований и словосочетаний.

2.7. СКФ должна обеспечивать сопоставление категории сайта в сети Интернет с возрастной категорией пользователя и принимать решение о доступе пользователя к информации в соответствии с классификацией информационной продукции.

2.8. СКФ не должна предоставлять возможности для пропуска пользователя к информации сайта, содержащего информацию, причиняющую вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

2.9. СКФ должна обеспечивать возможность по результатам анализа сайтов:

- блокировки URL-адреса сайта, запрашиваемой по HTTP протоколу;
- отображение специальной страницы блокировки в случае блокировки URL-адреса сайта;
- блокировки части информации от сайта, запрашиваемой по HTTP протоколу, и пропуск только не заблокированных частей пользователю;
- метод принудительного включения безопасного поиска в поисковых системах путем добавления аргументов "&family=yes&", "&safe=yes&" и других в зависимости от поисковых систем.

2.10. СКФ должна обеспечивать сбор статистики фильтрации, включая:

- время;
- IP-адрес, с которого произошло обращение;
- образовательное учреждение (по соответствию IP-адреса);
- URL сайта или домен системы DNS, к которому было произведено обращение, либо ключевые слова, по которым было заблокировано обращение, если обращение было заблокировано методом поисковой или контентной фильтрации;
- вид фильтрации, согласно которому обращение было заблокировано, если обращение было заблокировано;
- подтверждение пользователя, если он был предупрежден о потенциально опасной информации.

2.11. СКФ должна обеспечивать хранение статистики в течение срока, устанавливаемого соответствующими нормативными документами, и возможность передачи статистики во внешние системы в соответствии с установленными требованиями к взаимодействию.

2.12. СКФ должна обеспечивать автоматическое обновление конфигурации СКФ при изменении параметров настройки СКФ. Параметрами СКФ являются:

- пороговая величина блокировки сайта на основе семантического и морфологического анализа;
- адрес специальной страницы блокировки;
- адрес специальной страницы блокировки поисковых HTTP-запросов;
- адрес специальной страницы предупреждения с возможностью пропуска информации от сайта.

2.13. СКФ должна обеспечивать автоматическое обновление конфигурации (правил) фильтрации при изменении информации в РБОС. Обновление должно осуществляться не более чем через 3 рабочих дня после изменений в РБОС (реестр безопасных образовательных сайтов) списков URL адресов сайтов.

2.14. В Гимназии могут быть обеспечены следующие формы организации системы

ограничения обучающихся к негативной информации:

2.14.1. использование на персональных устройствах, компьютере-сервере при использовании локальной сети и устройств для создания беспроводной сети (Wi-Fi) программного обеспечения, реализующего необходимый функционал;

2.14.2. использование внешнего фильтрующего сервера, в том числе DNS-сервера и (или) прокси-сервера;

2.14.3. получение услуг фильтрации через оператора связи либо специализированную организацию, обеспечивающую доступ в сеть Интернет для Гимназии;

2.14.4. другие формы.

2.15. Гимназия может использовать многоформатную модель реализации системы контентной фильтрации как в рамках организации самостоятельно, так и взаимодействуя с другими организациями.

2.16. Технология организации системы ограничения обучающихся к негативной информации не может меняться чаще, чем раз в календарный год.

2.17. При использовании технологии контентной фильтрации и ограничении доступа обучающихся к негативной информации соблюдаются следующие положения:

2.17.1. при возможности персональной идентификации каждого обучающегося при осуществлении его доступа в сеть Интернет, должен осуществляться доступ обучающегося к информационной продукции в соответствии с классификацией информационной продукции, предусмотренной Федеральным [законом](#) N 436-ФЗ;

2.17.2. при отсутствии возможности персональной идентификации каждого обучающегося при осуществлении его доступа в сеть "Интернет", осуществляется доступ обучающегося к информационной продукции для детей, достигших возраста шести лет.

2.18. Педагогические работники не имеют права отключать СКФ на компьютерной технике, принадлежащей Гимназии, во время нахождения в здании и на территории Гимназии несовершеннолетних обучающихся.

2.19. Педагогические работники имеют право отключать СКФ на своих персональных устройствах или устройствах, предоставленных педагогическому работнику, после осуществления образовательного процесса и отсутствия несовершеннолетних в здании и на территории Гимназии, после получения письменного согласия от директора Гимназии или административного работника, к компетенции которого относится обеспечение информационной безопасности, с указанием или пояснением целей отключения СКФ и временных сроках отключения СКФ.

2.20. В Гимназии ведется журнал работы системы контентной фильтрации, в который включаются сведения об отключении педагогическим работником на устройстве СКФ.

2.21. Гимназия с целью недопущения обучающихся к негативной информации принимает локальный акт (положение), в котором самостоятельно определяют свою политику в отношении персональных устройств обучающихся, имеющих возможность выхода в сеть Интернет. Данный локальный акт (положение) размещается на сайте Гимназии в открытом доступе в разделе "Документы"

2.22. Гимназии получает согласия родителей (законных представителей) обучающихся о снятии ответственности с директора (администрации) Гимназии в случае предоставления своему ребенку устройства с выходом в Интернет при посещении Гимназии либо предоставления администрации Гимназии права на время учебного процесса забрать устройство(-а) обучающегося.

3. Система организационно-административных мероприятий, направленных на защиту детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

3.1. К организационно-административным мероприятиям, реализуемым Гимназией, направленным на защиту детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а

также не соответствующей задачам образования, относятся:

3.1.1. обеспечение защиты обучающихся от видов негативной информации для детей посредством использования СКФ при выходе в сеть "Интернет" при доступе к сети Интернет из Гимназии; основные аспекты данного направления регламентированы разделом 2 настоящего Положения;

3.1.2. проведение до 30 августа ежегодного мониторинга качества работы СКФ и применения организационно-административных мероприятий, направленных на защиту детей от негативной информации для детей; данное мероприятие предусмотрено в Плане мероприятий по обеспечению информационной безопасности обучающихся в МАОУ «СГ № 14»;

3.1.3. разработка и контроль исполнения локальных актов:

- Положение об ограничении в МАОУ «СГ № 14» доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;
- Положение об административных и организационных мерах, технических, программно-аппаратных средствах, применяемых в МАОУ «СГ № 14» для защиты детей от информации, причиняющей вред их здоровью и(или) развитию, определяющий в Гимназии основные аспекты организации работы СКФ, технологию, формат (форматы) реализации СКФ;
- приказ о назначении ответственного лица (ответственных лиц) в Гимназии за обеспечение безопасного доступа к сети Интернет, включающий функциональные обязанности за обеспечение безопасного доступа к сети Интернет;
- Порядок проведения проверки эффективности использования систем контентной фильтрации в образовательной организации (Приложение 1 к настоящему Положению);
- План мероприятий по обеспечению информационной безопасности в образовательной организации;
- локальный акт (приказ, положение) о порядке использования в Гимназии персональных устройств обучающихся, имеющих возможность выхода в сеть "Интернет";
- инструкции/правила для обучающихся и педагогов по обеспечению информационной безопасности при использовании сети "Интернет" (Приложение 2, 4 к настоящему Положению);
- порядок осуществления контроля педагогическими работниками использования обучающимися сети "Интернет" (Приложение 3 к настоящему Положению);

3.1.4. разработка и контроль ведения учетных документов:

- журнал работы системы контентной фильтрации;
- типовой акт проверки СКФ в образовательной организации;

3.1.5 внесение изменений в должностные инструкции педагогических работников об ограничении доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

3.1.6. организация просветительской работы с детьми и их родителями (законными представителями) по повышению культуры информационной безопасности путем реализации программ и проведения мероприятий, таких как Единый урок по безопасности в сети "Интернет", квест по цифровой грамотности "Сетевичок" и другие; данное мероприятие предусмотрено в Плане мероприятий по обеспечению информационной безопасности обучающихся в Гимназии;

3.1.7. направление на повышение квалификации ответственных лиц по темам "Организация защиты детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также несоответствующей задачам образования, в образовательных организациях" и педагогических работников по теме "Безопасное использование сайтов в сети Интернет в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации"; данное мероприятие предусмотрено в Плане мероприятий по обеспечению информационной безопасности обучающихся в МАОУ

«СГ № 14»;

3.1.8. организация информационной работы в соответствии с [письмом](#) Минобрнауки России от 14.05.2018 N 08-1184 "О направлении информации"; данное мероприятие предусмотрено в Плане мероприятий по обеспечению информационной безопасности обучающихся в МАОУ «СГ № 14»:

3.1.8.1. на информационных стендах в Гимназии размещаются информационные памятки, содержащие основные советы по обеспечению информационной безопасности учащихся (Приложение 4 к настоящему Положению);

3.1.8.2. в средствах массовой информации, ориентированных на обучающихся, в течение учебного года регулярно публикуются информационные материалы, посвященные отдельным аспектам информационной безопасности, а также различные памятки общего характера;

3.1.8.3. в средствах массовой информации, ориентированных на педагогическую общественность, в течение календарного года публикуются информационные материалы, посвященные отдельным аспектам информационной безопасности как несовершеннолетних, так и общеобразовательных организаций, а также различные памятки, обзоры нормативно-правового регулирования данной сферы и информацию о актуальных мероприятиях и событиях в данной сфере;

3.1.8.4. на сайте Гимназии обеспечено функционирование самостоятельного и специализированного раздела "Информационная безопасность", в рамках которого предусмотрено размещение следующей информации:

N	Раздел/подраздел	Содержание материалов
1.	Локальные нормативные акты в сфере обеспечения информационной безопасности обучающихся	Размещаются копии документов, т.е. сканированный вариант документа, соответствующий требованиям к параметрам сканирования. Размещаются документы, регламентирующие организацию и работу с персональными данными, планы мероприятий по обеспечению информационной безопасности обучающихся и другие.
2.	Нормативное регулирование	Публикуются актуальные сведения о федеральных и региональных законах, письмах органов власти и другие нормативно-правовые документы, регламентирующие обеспечение информационной безопасности несовершеннолетних. Допускается вместо копий размещать гиперссылки на соответствующие документы на сайтах органов государственной власти.
3.	Педагогическим работникам	Размещаются методические рекомендации и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной
4.	Обучающимся	Размещается информационная памятка и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной
5.	Родителям (законным представителям) обучающихся	Размещается информационная памятка
6.	Детские безопасные сайты	Размещается информация о рекомендуемых к использованию в учебном процессе безопасных сайтах, баннеры безопасных детских сайтов.

3.1.9. организация ежеквартального мониторинга изменения федерального законодательства и нормативно-правовых актов федерального уровня, связанных с защитой детей от видов информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, и предоставление ответственным сотрудникам за организацию в образовательной организации СКФ соответствующих актуальных федеральных законов нормативно-правовых актов федерального уровня; данное мероприятие предусмотрено в Плане мероприятий по обеспечению информационной безопасности обучающихся в МАОУ «СГ № 14»;

3.1.10. установка и обеспечение работы на персональных устройствах, принадлежащих Школе, антивирусного программного обеспечения с целью исключения возможности доступа детей к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования; данное мероприятие предусмотрено в Плане мероприятий по обеспечению информационной безопасности обучающихся в МАОУ «СГ № 14»;

3.1.11. проведение мониторинга использования сайтов в образовательном процессе в целях обучения и воспитания обучающихся в Гимназии до 30 августа ежегодно; данное мероприятие предусмотрено в Плане мероприятий по обеспечению информационной безопасности обучающихся в МАОУ «СГ № 14»;

3.1.12.

3.1.13. обеспечение отсутствия информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, на официальном сайте Гимназии и сайтах, задействованных в реализации образовательной деятельности образовательной организации, включая системы электронных дневников и дистанционного обучения; данное мероприятие предусмотрено в Плане мероприятий по обеспечению информационной безопасности обучающихся в МАОУ «СГ № 14»;

3.1.14. рекомендация: заключать договора с поставщиком СКФ при условии наличия в договоре положений об ответственности и обязательстве поставщика СКФ в виде компенсации понесенного ущерба за ненадлежащее оказание услуги.

3.2. Вопросы использования возможностей сети Интернет в образовательном процессе рассматриваются на заседаниях педагогических советов Гимназии, административных планерках, совещаниях при заместителях директора Гимназии и пр.

3.3. Директор Гимназии отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в Гимназии, а также за выполнение установленных правил. Для обеспечения доступа участников образовательного процесса к сети Интернет в соответствии с установленным в Гимназии правилами, директор Гимназии назначает своим приказом ответственного (ответственных) за организацию работы с Интернетом и ограничение доступа.

3.4. Ответственный за информационную безопасность:

- организует работу системы контентной фильтрации (СКФ) в Гимназии;
- принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет; осуществляет действия организационно-административного характера для обеспечения ограничения доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

3.5. Во время уроков и других занятий в рамках образовательного процесса контроль использования обучающимися сети Интернет осуществляет преподаватель, ведущий занятие.

3.6. 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 Гимназии правилами обеспечивается техником/ техническим специалистом.

3.7. Принципы размещения информации на интернет-ресурсах Гимназии призваны обеспечивать:

— соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;

— защиту персональных данных обучающихся, преподавателей и сотрудников;

— достоверность и корректность информации.

3.8. Персональные данные обучающихся (фамилия и имя, класс/год обучения, возраст, фотографию, и иные сведения личного характера) могут размещаться на интернет-ресурсах, создаваемых Гимназией, только с письменного согласия родителей или иных законных представителей обучающихся. Персональные данные преподавателей и работников Гимназии, характеризующие их профессиональный уровень, размещаются на интернет-ресурсах в соответствии с законодательством РФ; иные сведения - только с письменного согласия лица, чьи персональные данные размещаются.

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

4. Общественный контроль за обеспечением защиты детей от видов информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

4.1. Согласно [статье 21](#) Федерального закона N 436-ФЗ зарегистрированные в установленном федеральным законом порядке общественные объединения и иные некоммерческие организации в соответствии с их уставами, а также граждане вправе осуществлять в соответствии с законодательством Российской Федерации общественный контроль за соблюдением требований данного [закона](#).

4.2. В Гимназии может быть создан совет по обеспечению информационной безопасности обучающихся, в деятельность которого могут входить педагогические работники, родители (законные представители) обучающихся, представителей органов власти и общественных организаций. При отсутствии такого совета функциями общественного контроля наделяется Совет родителей обучающихся.

4.3. В Гимназии допускается деятельность организованных групп обучающихся для обеспечения безопасности и развития детей в информационном пространстве - кибердружины, киберпатруль и другие. При отсутствии таких организованных групп функциями общественного контроля наделяется Совет обучающихся.

4.4. В рамках общественного контроля наделенные полномочиями органы могут:

4.4.1. осуществлять мониторинг качества системы контентной фильтрации в Гимназии,

4.4.2. принимать участие в реализации плана мероприятий Гимназии по обеспечению защиты детей от негативной информации;

4.4.3. проводить общественную экспертизу работы Гимназии по обеспечению защиты

детей от негативной информации;

4.4.4. осуществлять экспертизу технологий и продуктов, связанных с фильтрацией информационного контента.

4.5. При проведении проверок Гимназии рекомендовано оценивать следующие аспекты ограничения доступа обучающихся к негативной информации для детей:

- Соответствие указанных в методических рекомендациях требований к СКФ, используемых в Гимназии;
- Применение администрацией Гимназии организационно-административных мероприятий, направленных на защиту детей от видов информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;
- Получение доступа к информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, с персональных устройств, расположенных в образовательной организации и имеющих выход в сеть "Интернет", путем:
 - Осуществления прямого доступа к сайту в сети "Интернет", содержащего негативную информацию;
 - Поиск с помощью поисковых систем информационной продукции, запрещенной для детей, в форме сайтов в сети "Интернет", графических изображений, аудиовизуальных произведений и других форм информационной продукции.

Приложение 1 к Положению об административных и организационных мерах, технических, программно-аппаратных средствах, применяемых в МАОУ «СГ № 14» для защиты детей от информации, причиняющей вред их здоровью и(или) развитию, распространяемой посредством сети Интернет, утвержденному приказом МАОУ «СГ № 14» № 332-о от 31.08.2021

Порядок проведения проверки эффективности использования систем контентной фильтрации в МАОУ «СГ № 14»

1. В МАОУ «СГ № 14» проводится проверка эффективной работоспособности школьной системы контентной фильтрации: систематически - системным администратором, комиссионно - по приказу директора Гимназии.

2. Для проверки эффективной работоспособности школьной системы контентной фильтрации:

2.1. выбираются 3-4 материала, содержание которых может причинить вред здоровью и развитию обучающихся (Федеральный список экстремистских материалов - <http://minjust.ru/nko/fedspisok>). Проверить конкретный сайт можно в едином реестре 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://zapret-info.gov.ru/>, <http://eais.rkn.gov.ru/>.

2.2. вносится название материала (части материала, адрес сайта) в поисковую систему.

2.3. из предложенного поисковой системой списка адресов осуществляется переход на страницу сайта, содержащего противоправный контент. Если материал отображается и с ним можно ознакомиться без дополнительных условий - фиксируется факт нарушения работы системы контентной фильтрации.

2.4. при дополнительных условиях (требуется регистрация, условное скачивание, переадресация и т.д.), при выполнении которых материал отображается, также фиксируется факт нарушения работы системы контентной фильтрации.

2.5. при невозможности ознакомления с противоправным контентом при выполнении условий (регистрация, скачивание материалов, переадресаций и т.д.) нарушение не фиксируется.

3. Проверка эффективной работоспособности школьной системы контентной фильтрации осуществляется путем выборки 3-4 противоправных материалов по определенной теме (экстремизм, проявление жестокости, порнография, терроризм, суицид, насилие и т.д.).

3.1. осуществить запрос через поисковую систему материала по заданной теме (Например: «изготовление зажигательной бомбы», «издевательства над несовершеннолетними», «способы суицида» и т.д.).

3.2. из предложенного поисковой системой списка адресов перейти на страницу 2-3 сайтов и ознакомиться с полученными материалами.

3.3. дать оценку материалам на предмет возможного нанесения ущерба физическому и психическому здоровью обучающимся.

3.4. при признании материала условно противоправным - зафиксировать факт нарушения с указанием источника и мотивов оценки, а также направить адрес материала на проверку 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://zapret-info.gov.ru/>, <http://eais.rkn.gov.ru/>.

4. Проверка работоспособности системы контент-фильтрации должна проводиться систематически на всех компьютерах Гимназии путем ввода в поле поиска любой поисковой *системы ключевых слов из списка информации, запрещенной для просмотра учащимися, с последующими попытками загрузки сайтов из найденных.* Необходимо, в том числе, проверить загружается ли информация, причиняющая вред здоровью и развитию детей, не имеющая отношения к образовательному процессу, в социальных сетях: «В контакте», «Одноклассники», twitter.com, facebook.com, [Живой Журнал livejournal.com](https://livejournal.com) и тд.

Замечание:

Если учреждение не использует перечисленные выше ресурсы в образовательных целях, то доступ к ним необходимо отключить.

5. При проверке работоспособности системы контент-фильтрации проверяется работоспособность журнала, фиксирующего адреса сайтов, посещаемых с компьютеров школы.

6. По итогам мониторинга оформляется заключение (акт) об эффективной (неэффективной) работе контентной фильтрации. При неэффективной работе контент-фильтра необходимо указать выявленные проблемы, пути их решения и сроки исправления.

7. При выявлении компьютеров, подключенных к сети Интернет и не имеющих СКФ, производятся одно из следующих действий:

- немедленная установка и настройка СКФ,
- немедленное программное и/или физическое отключение доступа к сети Интернет на выявленных компьютерах.

Приложение 2 к Положению об административных и организационных мерах, технических, программно-аппаратных средствах, применяемых в МАОУ «СГ № 14» для защиты детей от информации, причиняющей вред их здоровью и(или) развитию, распространяемой посредством сети Интернет, утвержденному приказом МАОУ «СГ № 14» № 332-о от 31.08.2021

Правила использования сети Интернет педагогическими работниками и обучающимися в МАОУ «СГ № 14»

1. Общие положения

1.1. Использование сети Интернет в МАОУ «СГ № 14» направлено на решение задач образовательного процесса.

1.2. Настоящие Правила регулируют условия и порядок использования сети Интернет в МАОУ «СГ № 14» (далее - Гимназия).

1.3. Доступ к сети Интернет в Гимназии имеют административный, педагогический и учебно-вспомогательный персонал, бухгалтера, обучающиеся Гимназии. Доступ к сети Интернет в Гимназии для других пользователей возможен только с разрешения директора Гимназии.

1.4. Доступ к сети Интернет в МАОУ «СГ № 14» для работников Гимназии в пределах их компетенции, для обучающихся Гимназии в пределах образовательного процесса осуществляется безлимитно на безвозмездной основе для пользователя.

1.5. Настоящие Правила имеют статус локального нормативного акта МАОУ «СГ № 14». Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящими Правилами, применяются нормы действующего законодательства Российской Федерации.

1.6. Использование сети Интернет в МАОУ «СГ № 14» подчинено следующим принципам:

- соответствия образовательным целям;
- способствования гармоничному формированию и развитию личности;
- уважения закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;
- приобретения новых навыков и знаний;
- расширения применяемого спектра учебных и наглядных пособий;
- социализации личности, введения в информационное общество.

2. Использование сети Интернет в образовательном процессе

2.1. Во время уроков и занятий в рамках образовательного процесса контроль использования обучающимися сети Интернет осуществляет преподаватель, ведущий урок, занятие. При этом преподаватель:

2.1.1. 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;

2.1.2. наблюдает за использованием компьютера и сети Интернет обучающимися;

2.1.3. обеспечивает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу;

2.1.4. 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;

2.1.5. доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;

2.2. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляет ответственный за учебное помещение, в кабинете информатики - лаборант, который в рамках контроля:

2.2.1. наблюдает за использованием компьютера и сети Интернет обучающимися;

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

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

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

2.4. Пользователи должны соблюдать тишину, чистоту и порядок в кабинете информатики или за рабочим местом, на котором установлена компьютерная техника, в том числе с выходом к ресурсам Интернета.

2.5. По разрешению работника, ответственного за организацию в Гимназии работы сети Интернет и ограничение доступа, преподаватели, сотрудники и обучающиеся вправе:

2.5.1. размещать собственную информацию в сети Интернет на интернет-ресурсах, не противоречащую законодательству РФ;

2.5.2. иметь учетную запись электронной почты;

2.5.3. сохранять полученную информацию в указанный каталог на жестком диске, на съемные носители, предварительно проверенные на вирусы;

2.6. Пользователям ресурсов Интернет запрещается:

2.6.1. обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации;

2.6.2. осуществлять любые сделки через Интернет;

2.6.3. осуществлять загрузки файлов на компьютер Гимназии только в образовательных целях;

2.6.4. устанавливать программное обеспечение;

2.6.5. изменять конфигурацию и настройки компьютера;

2.6.6. включать, выключать и перезагружать компьютер;

2.6.7. распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы;

2.6.8. осуществлять действия, направленные на «взлом» любых компьютеров (сетей), находящихся в школе и за ее пределами.

2.7. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, обучающийся обязан незамедлительно сообщить об этом преподавателю, проводящему занятие. Преподаватель обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом лицу, ответственному за работу локальной сети и ограничение доступа к информационным ресурсам.

Ответственный обязан:

— принять информацию от преподавателя;

— направить информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения технического ограничения доступа к информации (в течение суток);

— в случае явного нарушения обнаруженным ресурсом законодательства Российской Федерации сообщить о нем по специальной «горячей линии» для принятия мер в

соответствии с законодательством Российской Федерации (в течение суток).

Передаваемая информация должна содержать:

- доменный адрес ресурса;
- сообщение о тематике ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо его несовместимости с задачами образовательного процесса;
- дату и время обнаружения;
- информацию об установленных в ОУ технических средствах технического ограничения доступа к информации.

2.8. В отношении лиц, сознательно не соблюдающие настоящие Правила, принимаются меры привлечения к дисциплинарной ответственности с соблюдением соответствующих процедур.

2.9. При нанесении материального ущерба сети Гимназии и оборудованию, обеспечивающему выход к ресурсам Интернет на базе Гимназии, пользователь (законный представитель) несет материальную ответственность в соответствии с законодательством РФ.

Приложение 3 к Положению об административных и организационных мерах, технических, программно-аппаратных средствах, применяемых в МАОУ «СГ № 14» для защиты детей от информации, причиняющей вред их здоровью и(или) развитию, распространяемой посредством сети Интернет, утвержденному приказом МАОУ «СГ № 14» № 332-о от 31.08.2021

Инструкция о порядке действий при осуществлении контроля использования обучающимися сети Интернет

1. Настоящая инструкция устанавливает порядок действий работников МАОУ «СГ № 14» (далее - Гимназия) при:

1) обращения обучающихся к контенту, не имеющему отношения к образовательному процессу;

2) отказе при обращении к контенту, имеющему отношение к образовательному процессу, вызванного техническими причинами.

2. Контроль использования обучающимися сети Интернет осуществляют:

1) во время занятия — проводящий его преподаватель и (или) техник, лаборант кабинета информатики, оказывающий помощь в проведении занятий;

2) во время использования сети Интернет для свободной работы обучающихся — техник и (или) лаборант кабинета информатики.

3. Преподаватель:

— 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 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 ответственного за организацию работы с ресурсами Интернет и 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 преподавателя, содержит информацию, запрещенную для распространения в соответствии с законодательством Российской Федерации, или иного потенциально опасного для обучающихся контента, он сообщает об этом ответственному за работу Интернета, обеспечивает ограничение доступа к данной информации.

5. В случае отказа доступа к ресурсу, разрешенному для использования в образовательном процессе, преподаватель сообщает об этом работнику, ответственному за работу Интернета.

Приложение 4 к Положению об административных и организационных мерах, технических, программно-аппаратных средствах, применяемых в МАОУ «СГ № 14» для защиты детей от информации, причиняющей вред их здоровью и(или) развитию, распространяемой посредством сети Интернет, утвержденному приказом МАОУ «СГ № 14» № 332-о от 31.08.2021

Памятка для обучающихся об информационной безопасности детей

Рекомендована Письмом Минобрнауки России от 14.05.2018 № 08-1184

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

Рекомендована Письмом Минобрнауки России от 14.05.2018 № 08-1184

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 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 ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «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 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 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 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;

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 твоё местоположение;

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

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

Электронные деньги

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

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

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

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные 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, StR0ng!;;

4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;

2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный фанат@» или «рок2013» вместо «тема13»;

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

7. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

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

2. Управляй своей киберрепутацией;

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

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

5. Соблюдай свой виртуальную честь смолоду;

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

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

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

Мобильный телефон

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

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

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

Основные советы для безопасности мобильного телефона:

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

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

3. Необходимо обновлять операционную систему твоего смартфона;

4. Используй антивирусные программы для мобильных телефонов;

5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

6. После того как ты выйдешь с сайта, где вводил личную информацию, зайти в настройки браузера и удалить cookies;

7. Периодически проверяй какие платные услуги активированы на твоём номере;
8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
9. 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 скриншотов;
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 друзья, 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 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

Рекомендована Письмом Минобрнауки России от 14.05.2018 № 08-1184

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

Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

1. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.

2. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.
3. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
5. Не забывайте принимать непосредственное участие в жизни ребенка беседовать с детьми об их друзьях в Интернете.
6. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
7. Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
8. 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.
9. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
10. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.
11. 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.
12. Расскажите детям о порнографии в Интернете.
13. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
14. 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.