Муниципальное бюджетное общеобразовательное учреждение средняя общеобразовательная школа (военвед) г Зернограда

Программа по созданию безопасной информационной среды в школе на 2017-2020 годы

«Безопасный интернет в школе»

Зерноград 2017 г

ПАСПОРТ ПРОГРАММЫ ПО СОЗДАНИЮ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СРЕДЫ В ШКОЛЕ
«Безопасный интернет в школе»

Нормативные документы

1. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ;
2. Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите учащихся от информации, причиняющей вред их здоровью и развитию»;
3. Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
4. Федеральный закон от 27.07.2006 №152 «О персональных данных»;
5. «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10 с изменениями и дополнениями от 29 июня 2011 г., 25 декабря 2013 г., 24 ноября 2015 г.
6. Концепция информационной безопасности учащихся, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471р

Сроки реализации

2017-2020 годы

Разработчики программы

А. В. Гурова – учитель физики, ответственный за информатизацию в образовательном учреждении

Исполнители программы

- ✓ Классные руководители 7-11 классов
- ✓ Учитель информатики и ИКТ, учителя предметники
- ✓ Заместители директора по УВР и по ВР

Материально-техническое обеспечение учебного процесса

в школе для участников образовательного процесса созданы:

- ✓ 1 компьютерный класс,
- ✓ 18 учебных кабинетов, оборудованных мультимедийным оборудованием;
- ✓ имеется скоростной выход в Интернет;
- ✓ 13 компьютеров, используемых в учебном процессе, подключены к проводному интернету;
- ✓ 2 ноутбука, используемых в учебном процессе и работе администрации, подключены к интернету через WI-FI;
- ✓ создан и функционирует официальный сайт школы;

Цели программы:

- обеспечение гармоничного развития молодого поколения при условии минимизации всех негативных факторов, связанных с формированием гиперинформационного общества в России;
- формирование безопасной информационной образовательной среды в школе, обеспечение информационной безопасности учащихся, использующих Интернет в образовании и пропаганда безопасного поведения в сети Интернет.

Задачи программы:

- формирование у учащихся навыков самостоятельного и ответственного потребления информационной продукции;
- повышение уровня медиаграмотности учащихся;
- формирование у учащихся позитивной картины мира и адекватных базисных представлений об окружающем мире и человеке;
- ценностное, моральное и нравственно-этическое развитие учащихся; формирование и расширение компетентностей работников образования в области медиабезопасного поведения учащихся и подростков;
- формирование информационной культуры как фактора обеспечения информационной безопасности;
- изучение нормативно-правовых документов по вопросам защиты учащихся от информации, причиняющей вред их здоровью и развитию;
- формирование знаний в области безопасности учащихся, использующих Интернет;
- организация просветительской работы с родителями и общественностью;
- организация технического контроля безопасности.

Основные направления программы

- Разработка и внедрение эффективной модели организации процесса информатизации, включающей информационно-методическое, кадровое и материально-техническое обеспечение.
- Формирование и апробация инновационных подходов к информатизации школы.
- Оснащение школы современными электронными учебными материалами.
- Подготовка педагогических кадров к освоению и эффективному внедрению информационных и коммуникационных технологий в образовательный процесс.
- Обеспечение школы средствами информационных и коммуникационных технологий.

Планируемые результаты реализации программы

Системный подход в решении задач построения в школе безопасной среды для доступа к сети Интернет:

- обеспечит потребность учителя в постоянном повышении уровня своей квалификации и профессионализма по данному вопросу;
- поможет родителям грамотно организовать информационное пространство ребенка в семье;
- совместные усилия педагогов и родителей создадут рабочую среду ребенка и в школе, и дома с учетом его интересов, сообразно возрастным особенностям и духовным потребностям в рамках общечеловеческих ценностей.

Будет создана новая медиасреда, соответствующая следующим характеристикам:

- наличие развитых информационно-коммуникационных механизмов, направленных на социализацию молодого поколения и раскрытие его творческого потенциала;
- свободный доступ учащихся к историко-культурному наследию предшествующих поколений;
- качественный рост уровня медиаграмотности учащихся;
- гармонизация меж- и внутрипоколенческих отношений;
- популяризация здорового образа жизни среди молодого поколения;
- формирование среди учащихся устойчивого спроса на получение высококачественных информационных продуктов;
- снижение уровня противоправного и преступного поведения среди учащихся;
- формирование у учащихся уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования "пиратского" контента. (Концепция информационной безопасности учащихся, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р»)
- Возможные риски
- Запрет доступа к негативной информации формирует у ребенка желание получить эту информацию.

1. Пояснительная записка

Проблема обеспечения информационной безопасности учащихся в информационно-телекоммуникационных сетях становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей. В современных условиях развития общества компьютер стал для ребенка и «другом» и «помощником» и даже «воспитателем», «учителем». Всеобщая информатизация и доступный, высокоскоростной Интернет уравнял жителей больших городов и малых деревень в возможности получить качественное образование и стал неотъемлемой частью нашей повседневной жизни. Использование Интернета в образовательных учреждениях и дома расширяет информационное образовательное пространство обучающего и позволяет повысить эффективность обучения. Доступ учащихся к информационным ресурсам сети Интернет дает возможность школьникам пользоваться основным и дополнительным учебным материалом, необходимым для обучения в школе, выполнять домашние задания, самостоятельного обучаться. Благодаря таким ресурсам у школьников появляется возможность узнавать о проводимых олимпиадах, конкурсах, и принимать в них активное участие.

Использование Интернета в работе с учащимися и в работе школы достаточно обширно:

- ✓ это использование электронной почты;
- ✓ поиск в сети нужной информации;
- ✓ создание собственных школьных веб-страниц;
- ✓ рассылка и/или съем материалов (нормативных документов, информации о семинарах и конкурсах и т.п.);
- ✓ обмен опытом;
- ✓ ответы на типичные вопросы;
- ✓ получение ("скачивание") небольших учащихся программ по разным предметам;
- ✓ совместные проекты школьников (и учителей) разных школ.

Однако использование Интернета в образовательной деятельности таит в себе много опасностей, существует ряд аспектов, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для учащихся угрозу. «Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие

опасности подстерегают их в сети и как их избежать» (П.А.Астахов, уполномоченный при Президенте РФ по правам ребенка, 2015г.). Важно, чтобы во всех школах был безопасный Интернет.

2. Программа по созданию безопасной информационной среды «Безопасный Интернет в школе»

Согласно российскому законодательству информационная безопасность учащихся – это состояние защищенности учащихся, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ "О защите учащихся от информации, причиняющей вред их здоровью и развитию"). Преодолеть нежелательное воздействие компьютера возможно только совместными усилиями учителей, родителей и самих школьников. Согласно Концепции информационной безопасности учащихся, утвержденной распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р», обеспечение информационной безопасности должно строиться на следующих принципах:

- ✓ признание учащихся равноправными участниками процесса формирования информационного общества в Российской Федерации;
- ✓ ответственность государства за соблюдение законных интересов учащихся в информационной сфере;
- ✓ необходимость формирования у учащихся умения ориентироваться в современной информационной среде;
- ✓ воспитание у учащихся навыков самостоятельного и критического мышления;
- ✓ развитие государственно-частного партнерства в целях обеспечения законных интересов учащихся в информационной среде;
- ✓ повышение эффективности сотрудничества представителей средств массовой информации и массовых коммуникаций и государственных органов в интересах защиты учащихся от информации, способной причинить вред их здоровью и развитию;
- ✓ обучение учащихся медиаграмотности;
- ✓ поддержка творческой деятельности учащихся в целях их самореализации в информационной среде;
- ✓ создание условий для формирования в информационной среде благоприятной атмосферы для учащихся вне зависимости от их социального положения, религиозной и этнической принадлежности;
- ✓ взаимодействие различных ведомств при реализации стратегий и программ в части, касающейся обеспечения информационной безопасности учащихся;

- ✓ обеспечение широкого доступа учащихся к историческому и культурному наследию России через использование современных средств массовых коммуникаций;
- ✓ открытость и взаимодействие с другой информационной культурой и традициями, формирование у учащихся объективного представления о российской культуре как неотъемлемой части мировой цивилизации.

Данная программа рассчитана на период 2017-2020 годы. Работа с учащимися ведется в зависимости от возрастных особенностей. Для организации безопасного доступа к сети Интернет в МБОУ СОШ (военвед) г Зернограда созданы следующие условия:

В образовательном учреждении разработаны и утверждены:

1. Правила об использовании сети Интернет в МБОУ СОШ (военвед) г Зернограда
2. Положение об информационной открытости муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школы (военвед) города Зернограда
3. ПОЛОЖЕНИЕ о сайте муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школы (военвед) города Зернограда (http:// sosh16zernograd.ru)
4. Положение о порядке доступа педагогических работников к информационно телекоммуникационным сетям и базам данных
5. Классификатор информации, не имеющей отношения к образовательному процессу в МБОУ СОШ (военвед) г Зернограда
6. Политика МБОУ СОШ (военвед) г Зернограда в отношении обработки персональных данных
7. Инструкция по организации антивирусной защиты МБОУ СОШ (военвед) г Зернограда
8. Инструкция для педагогических работников и сотрудников МБОУ СОШ (военвед) г Зернограда о порядке действий при осуществлении контроля использования обучающимися сети Интернет
9. План мероприятий по обеспечению информационной безопасности учащихся защиты МБОУ СОШ (военвед) г Зернограда

2. Контроль использования учащимися сети Интернет визуального контроля и записи в журнал учета времени работы Интернет-ресурса.

1. На официальном сайте школы для учащихся и родителей создан раздел «Информационная безопасность», http://sosh16zernograd.ru/obuchau.html. Здесь размещены материалы, посвященные безопасному поведению в сети Интернет и его

использованию. А также на сайте размещены полезные ссылки для учащихся и родителей.

2. Ведется журнал учета времени работы Интернет-ресурса.

3. Ежегодно проводится Неделя безопасности в сети Интернет

3. Механизм реализации программы

1. *Аппаратная и программная защита информационной безопасности.* Внедрение систем исключения доступа к информации, несовместимой с задачами гражданского становления учащихся, а также средств фильтрации и иных аппаратно - программных и технико - технологических устройств

№ п/п	Наименование мероприятия	Срок исполнения	Исполнители, ответственные за реализацию мероприятия	Ожидаемые результаты (количественные и качественные показатели)
1.	Установка и своевременное обновление антивирусного ПО	2017-2020	Ответственный за информатизацию	100% установка в школе программного продукта,

				обеспечивающего антивирусную защиту
2.	Мониторинг функционирования и использования в школке программного продукта, обеспечивающего контент фильтрацию Интернет трафика	2017-2020	Ответственный за информатизацию	100% установка в школе программного продукта, обеспечивающего контент-фильтрацию трафика
3.	Мониторинг качества предоставления провайдером услуги доступа к сети Интернет образовательным	2017-2020	Ответственный за информатизацию	100% обеспечение услуги доступа в сеть Интернет школе с обеспечением контент-фильтрации учреждениям с обеспечением контент-фильтрации Интернет - трафика Интернет - трафика
4.	Внедрение и использование программно-технических средств, обеспечивающих исключение доступа учащихся школы к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания	2017-2020	Ответственный за информатизацию	Отслеживание созданных, обновленных программно-технических средств, обеспечивающих исключение доступа учащихся школы к ресурсам сети Интернет и установка их на компьютеры

2. Работа с обучающимися

№ п/п	Название мероприятия	Целевая аудитория	Сроки исполнения	Исполнители, ответственные за реализацию мероприятия
1.	Изучение нормативных документов по организации безопасного доступа к сети Интернет	Педагоги школы	сентябрь	Учитель информатики
2.	Единый урок безопасности в сети «Интернет»	Учащиеся 7-11 классов	30.10.2018	Учитель информатики.
3.	Индивидуальные беседы «Этика сетевого общения»	Учащиеся 7-11 классов	в течение года	Классные руководители, учителя-предметники
4.	Беседы «Юридическая ответственность за размещения запрещенной информации в сети Интернет»	Учащиеся 7-11 классов	октябрь	Социальный педагог
5.	Беседы «Остерегайся мошенничества в Интернете», «Мошенничества с пластиковыми картами»	Учащиеся 7-11 классов	ноябрь	Классные руководители
6.	Круглый стол «Мои любимые сайты»	Учащиеся 8-9 классов	декабрь	Учитель информатики Классные руководители
7.	Разработка буклетов для учащихся: «Защити себя сам!», «Безопасный Интернет», «Интернет-ресурсы для учащихся»	Учащиеся 8 классов	февраль	Учитель информатики
8.	Декада безопасного интернета.	Учащиеся 7-11 классов	март	Зам. директора по ВР Учитель информатики
9.	Участие в городских мероприятиях	Учащиеся 7-11 классов	В течение года	Зам Директора по ВР и по научно-методической работе

3. Работа с родителями и лицами их заменяющими

№ п/п	Наименование мероприятия	Срок исполнения	Исполнители, ответственные за реализацию мероприятия
1.	Ознакомление родителей с информационным курсом для родителей по защите учащихся от распространения вредной для них информации	В течение года	Классные руководители Учитель информатики
2.	Выдача памяток родителям по безопасности в интернете	В течение года	Классные руководители Учитель информатики
3.	Организация консультационной помощи специалистов школы	В течение года	Педагог-психолог Социальный педагог
4.	Включение темы «Интернет безопасность» в родительское собрание «Безопасность учащихся – общая задача школы и родителей», «Как уберечь учащихся от беды. Использование контентной фильтрации дома»	В течение года	Администрация школы
5.	Декада безопасного интернета.	март	Зам. директора по ВР, Учитель информатики
6.	Консультирование родителей по вопросам безопасности в сети «Интернет»	в течение года	Учитель информатики

3. Работа с сотрудниками школы.

Работа с формированием информационной безопасности школьников нуждается в специальных условиях, которые создают возможности взаимодействия и взаимопонимания между педагогом и учащимся на основе тщательно продуманного содержания занятий по информационной безопасности, имеющих смысловую значимость для школьника. Одним из главных условий успешного обучения информационной безопасности является позиция учителя, сущность которой составляет безусловное, безоценочное принятие ребенка, желание укрепить его позицию в социуме, оказать своевременную поддержку в саморазвитии школьника, оградить его от совершения неприемлемых действий, открыть путь к социализации и адаптации ребенка.

Одним из важных условий успешного обучения школьников основам информационной безопасности является осведомленность педагога в теории информационной безопасности: во-первых, в том, что именно защищается, что является объектом или предметом защиты (в нашем случае - это личность школьника; во-вторых, установление, от чего защищается личность школьника, какова угроза (опасность) - внешний по отношению к данной целостности фактор, воздействующий на школьника; в - третьих, в понимании необходимости предотвращения разрушения самооценки ребенка, дезориентации в окружающей обстановке, нарушении адекватности представлений школьника об окружающем мире и своем месте в нем,

снижении самоуважения или чувства уверенности, утрате целостности Я и потере индивидуальной уникальности, крушении планов, намерений, выборе неадекватных целей и способов поведения, попадании в психологическую зависимость от других субъектов воздействия, духовной деградации, нарушениях психического здоровья вплоть до необратимых патологических изменений психики; в-четвертых, в представлении, как избежать возможного ущерба, каким образом и чем защищаться; в-пятых, в уверенности педагога в том, что в процессе обучения именно он является субъектом защиты личности школьника, опережая в данном направлении действия общества и государства.

Условия, которые будут способствовать эффективному формированию информационной безопасности:

- содержательное, включает содержательный компонент программы занятий для учащихся (систему внеклассных мероприятий, направленных на умение выявлять информационную угрозу);
- процессуально-технологическое, направленное на эффективность использования методов, приемов и средств проведения занятий с учетом особенностей развития школьников.
- психолого-педагогические условия, такие как гуманно- ориентированное и доброжелательное взаимодействие педагога и учащихся. Дополнительным условием явилась организация работы с родителями.

Рассмотрим более подробно выявленные условия. Сущностью первого условия является разработка и реализация программы внеклассной работы по информационной безопасности. Целью обучения школьника информационной безопасности является формирование соответствующей системы противодействия информационным угрозам.

Также можно выделить методы проведения внеклассных занятий по обучению информационной безопасности. Первым методом, наиболее важным для начальных этапов занятий, является объяснительно-иллюстративный, его значимость заключается в том, что на первоначальном этапе обучения, знания учащимся предлагаются в «готовом» виде, педагог различными способами организует восприятие этих знаний, учащиеся осмысливают знания, фиксируют их в памяти. Знания учащимся об информационных видах опасностей, влиянии на здоровье и др. учитель предлагает в «готовом» виде, объясняет их, учащиеся сознательно осваивают и правильно воспроизводят полученную информацию

Вторым методом является метод проблемного изложения материала, на втором этапе учащиеся еще не участники, а лишь наблюдатели хода размышлений учителя.

Третий метод - частично-поисковый становится основным методом обучения на последующих этапах. В данном случае, педагог организует поиск новых знаний с помощью разнообразных средств. Учащиеся под руководством учителя решают

познавательные задачи, проблемные ситуации, анализируют, сравнивают, обобщают, делают выводы.

В качестве формы организации обучения учащихся информационной безопасности предлагается занятия во внеурочное время. Проведение обучения во время внеклассных мероприятий дает педагогу возможность организации занятия в форме экскурсий, которая включит такие способы ознакомления учащихся с объектом, как разъяснение, беседа, наглядный показ, сбор наглядно-иллюстрационного материала с использованием основных положений теории.

Спецификой проведения занятий является: создание реальных ситуаций, предполагающих нравственный выбор, духовно-нравственное самоопределение, наличие наглядных пособий: детской периодической литературы, компьютерных дисков, имитированных моделей сотовых телефонов и т.д. Кроме этого, специфика развития информационной безопасности школьника состоит в учете таких особенностей, как: доверие ребенка взрослому, сверстникам, недостатке опыта осознания возможности удовлетворения своих основных потребностей и обеспеченности собственных прав в любой, даже неблагоприятной ситуации, в возникновении обстоятельств, которые могут блокировать или затруднять их реализацию. Педагоги и родители - значимые взрослые, способствующие становлению информационной безопасности. Но сами педагоги и родители не всегда компетентны в вопросах информационной безопасности. Таким образом, возникает необходимость в разработке специальных занятий для педагогов, включающих теоретические семинары и практические занятия по теме «Информационная безопасность школьника».

№ п/п	**Наименование мероприятия**	**Срок исполнения**	**Исполнители, ответственные за реализацию мероприятия**	**Ожидаемые результаты (количественные и качественные показатели)**
1.	Организация свободного доступа учащихся и учителей к высококачественным и сетевым образовательным ресурсам, в том числе к системе современных учебных материалов по всем предметам.	2017-2020	Администрация школы	100% обеспечение доступа учащихся и учителей к электронным образовательным ресурсам через сеть Интернет
2.	Участие в мероприятиях по созданию надежной системы защиты учащихся от противоправного контента в образовательной среде школы и дома.	2017-2020	Администрация школы	Повышение грамотности по проблемам информационной безопасности всех участников образовательного процесса
3.	Обсуждение вопросов информационной безопасности на ШМО	2017-2020	Руководители ШМО	Повышение грамотности по проблемам информационной безопасности всех участников образовательного процесса

5. Создание нормативно-правовой, информационной, методической и дидактической базы обеспечения интернет безопасности учащихся

№ п/п	Наименование мероприятия	Срок исполнения	Исполнители, ответственные за реализацию мероприятия	Ожидаемые результаты (количественные и качественные показатели)
1.	Разработка классных часов по формированию информационной безопасности учащихся	2017-2020	Классные руководители	Создание методической копилки
2.	Разработка занятий медиауроков по теме «Информационная безопасность»	2017-2020	Классные руководители, библиотекарь, учителяпредметники	Создание методической копилки
3.	Разработка алгоритма выявления и системы занятий с учащимися, страдающими интернет-зависимостью	2017-2020	Педагогпсихолог	Выявление учащихся «группы риска»
4.	Разработка занятий по правовым основам работы в интернете	2017-2020	Социальный педагог	Разработка занятия

4. Прогноз возможных негативных последствий и способы коррекции, компенсации негативных последствий

Запрет доступа к негативной информации формирует у ребенка желание получить эту информацию во что бы то ни стало. И эту информацию он может получить вне школы и дома у друзей или знакомых. Поэтому очень важно формировать информационную культуру и создать индивидуальную рабочую среду ребенку и в школе и дома с учетом его интересов, сообразно возрастным особенностям и духовным потребностям в рамках общечеловеческих ценностей.

5. Планируемые результаты

Системный подход в решении задач построения в школе безопасной среды для доступа к сети Интернет:

- обеспечит потребность учителя в постоянном повышении уровня своей квалификации и профессионализма по данному вопросу;

- поможет родителям грамотно организовать информационное пространство ребенка в семье;
- совместные усилия педагогов и родителей создадут рабочую среду подростка и в школе, и дома с учетом его интересов, сообразно возрастным особенностям и духовным потребностям в рамках общечеловеческих ценностей.

«Будет создана новая медиасреда, соответствующая следующим характеристикам:

- наличие развитых информационно-коммуникационных механизмов, направленных на социализацию молодого поколения и раскрытие его творческого потенциала;
- свободный доступ учащихся к историко-культурному наследию предшествующих поколений;
- качественный рост уровня медиаграмотности учащихся;
- формирование среди учащихся устойчивого спроса на получение высококачественных информационных продуктов;
- снижение уровня противоправного и преступного поведения среди учащихся;
- формирование у учащихся уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования "пиратского" контента». (Концепция информационной безопасности учащихся, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р).

6. Перспективы дальнейшей работы школы по созданию Интернетпространства для участников образовательного процесса

Повышение информационной грамотности педагогов, родителей и учащихся по вопросам информационной безопасности.

7. Система организации контроля реализации Программы

1. Оперативное руководство реализацией программы и проблемно-ориентированный анализ администрацией школы раз в полгода.
2. Обсуждение, утверждение промежуточных результатов, принятие решений по корректировке направлений работы на педагогическом совете школы и методических объединений.

Литература

1. Федеральный закон «Об образовании», Закон РФ от 29.12.2012 № 273.

2. Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите учащихся от информации, причиняющей вред их здоровью и развитию».

3. Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

4. Федеральный закон от 27.07.2006 №152 «О персональных данных».

5. Концепция информационной безопасности учащихся, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р».

6. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство Агентства «Яхтсмен», 1996.

7. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000.

8. Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монография. – М.: МГУЛ, 2003. – 212 с.

9. Новиков А.А., Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий: Учебное пособие. – М. «Радио и связь», 2003.

10. Серебряник Е. Э. Формирование информационно-личностной безопасности учащихся основой школы. Автореферат диссертации на соискание ученой степени кандидата педагогических наук. Калининград 2011.

11. Ссылки на используемые сайты: http://персональныеданные.дети/ http://rkn.gov.ru/personal-data/ http://ligainternet.ru/

Перечень приложений:

1. Документы школы, связанные с работой в сети Интернет:
— РЕГЛАМЕНТ работы в сети Интернет в МБОУ СОШ (военвед) г Зернограда;
— ПОЛОЖЕНИЕ об использовании сети Интернет МБОУ СОШ (военвед) г Зернограда;
— ПОЛОЖЕНИЕ об информационной открытости МБОУ СОШ (военвед) г Зернограда
— ПОЛОЖЕНИЕ о сайте;
— ИНСТРУКЦИЯ для педагогических сотрудников о порядке действий при осуществлении контроля за использованием учащимися сети Интернет;
— Порядок доступа педагогических работников к информационно телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности;
— КЛАССИФИКАТОР информации, не имеющей отношения к образовательному процессу;
— Регламент работы с электронной почтой в школе;
— Инструкция по организации антивирусной защиты в школе;
— ПОЛОЖЕНИЕ об электронном журнале успеваемости/электронном дневнике учащегося.
2. Методические рекомендации « Локальные нормативные акты в сфере обеспечения информационной безопасности».
3. Памятка родителям по управлению безопасностью детей в интернете.
4. Памятка для детей по безопасному поведению в интернете.

РЕГЛАМЕНТ РАБОТЫ В СЕТИ ИНТЕРНЕТ

I. Общие положения

1.1. Настоящий Регламент разработан в соответствии с положением об использовании сети Интернет в общеобразовательном учреждении МБОУ СОШ (военвед) г Зернограда и является локальным нормативным актом образовательного учреждения.
1.2. «Точка доступа» (все учебные кабинеты) к сети Интернет предназначена для обслуживания обучающихся, педагогов и административного персонала образовательного учреждения, которые допускаются к работе в сети Интернет на бесплатной основе.

1.3. Организацию работы «Точек доступа» осуществляют назначенные приказом по школе ответственные за обеспечение доступа к ресурсам сети Интернет и контроль безопасности работы в сети, а также администраторы «Точек доступа». Пользователями в настоящем документе называются обучающиеся и сотрудники школы, ознакомленные с положением об использовании сети Интернет и прошедшие предварительную регистрацию у администратора «точки доступа». В исключительном случае разрешается допуск к работе других лиц по разрешению директора школы. Предоставление сеанса работы в Интернет осуществляется пользователям, как правило, на основании предварительной записи в журнале администратора в зависимости от категории пользователя:

учащимся предоставляется доступ в компьютерном классе согласно расписанию занятий, график работы компьютерного класса составляется (на учебную четверть) на основании общешкольного расписания;

для проведения внеурочных мероприятий доступ предоставляется в соответствии с планом работы и корректируется еженедельно;

для свободного доступа учащихся к сети Интернет предоставляется не менее 2 часов в неделю, сеансами не более 30 минут при предварительной записи у администратора «точки доступа»;

учителям, административному, вспомогательному персоналу предоставляется доступ по графику согласно ежемесячно подаваемым служебным запискам на имя ответственного лица, но не менее 2 часов в неделю, сеансами не менее 30 минут;

II. Правила работы

Для проведения сеанса работы, необходимо обратиться к администратору «точки доступа» за разрешением для работы. При наличии свободных мест и после регистрации в журнале учета, пользователю предоставляется рабочая станция в «точке доступа».

1. В начале работы пользователь обязан зарегистрироваться в журнале учета.

2. Пользователю разрешается записывать полученную информацию на личные носители информации (диски, флэш-карты) с предварительной проверкой на наличие вирусов. Копирование с носителей на жесткие диски производится только с разрешения администратора «точки доступа».

3. Разрешается использовать оборудование только для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения гуманитарных и культурных проектов. Любое использование оборудования в коммерческих целях запрещено.

4. Запрещена передача информации, представляющую коммерческую или государственную тайну, распространение информации, порочащей честь и достоинство граждан.

5. Запрещается работать с объемными ресурсами (video, audio, игры и др.) без согласования с администратором.

6. Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.

7. Пользователь обязан сохранять оборудование в целости и сохранности.

8. Пользователю запрещено вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах без прямого разрешения администратора.

За административное нарушение, не влекущее за собой порчу имущества и вывод оборудования из рабочего состояния пользователь может быть лишен права выхода в Интернет сроком на месяц. При повторном административном нарушении - пользователь лишается доступа в Интернет. При возникновении технических проблем пользователь обязан поставить в известность администратора.

III. Памятка пользователя по использованию ресурсов сети Интернет

1. В начале работы пользователь обязан зарегистрироваться в журнале учѐта работы в сети Интернет.

2. Каждый пользователь при наличии технической возможности может иметь персональный каталог, предназначенный для хранения личных файлов общим объемом не более 200 Мб. Аналогично может быть предоставлена возможность работы с почтовым ящиком. При возникновении проблем необходимо обратиться к дежурному администратору.

3. Пользователю разрешается переписывать полученную информацию на личные носители информации, которые предварительно проверяются на наличие вирусов

4. Разрешается использовать оборудование классов только для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения проектов. Любое использование оборудования в коммерческих целях запрещено.

5. Запрещена передача внешним пользователям информации, представляющую коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан. Правовые отношения регулируются Законом «Об информации, информатизации и защите информации», Законом «О государственной тайне», Законом «Об авторском праве и смежных правах», статьями Конституции об охране личной тайне, статьями Гражданского кодекса и статьями Уголовного кодекса о преступлениях в сфере компьютерной информации.

6. Запрещается работать с объемными ресурсами (video, audio, chat, игры) без согласования с администратором.

7. Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.

8. При случайном обнаружении ресурса, содержание которого противоречит законодательству Российской Федерации, противоречит целям обучения и воспитания, или имеет провокационный или оскорбительный характер, пользователь обязан незамедлительно сообщить об этом администратору ―точки доступа.

9. Пользователю запрещено вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах без прямого разрешения администратора. Запрещается перегружать компьютер без согласования с администратором.

10. Пользователь обязан сохранять оборудование в целости и сохранности.

11. Пользователь обязан соблюдать общественный порядок и чистоту в помещении и способствовать соблюдению порядка другими пользователями; проявлять корректность по отношению к пользователям.

12. При возникновении технических проблем пользователь обязан поставить в известность администратора. При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность. За административное нарушение, не влекущее за собой порчу имущества и вывод оборудования из рабочего состояния пользователь может быть лишен права выхода в Интернет сроком на месяц. При повторном административном нарушении - пользователь лишается доступа в Интернет.

ПОЛОЖЕНИЕ

об использовании сети Интернет в образовательном учреждении

1. Общие положения

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

1.2. Настоящее Положение регулируют условия и порядок использования сети Интернет в МБОУ СОШ (военвед) г Зернограда.

1.3. Настоящее Положение имеют статус локального нормативного акта МБОУ СОШ (военвед) г Зернограда

2. Организация использования сети Интернет в МБОУ СОШ (военвед) г Зернограда

2.1. Вопросы использования возможностей сети Интернет в учебно-образовательном процессе рассматриваются на педагогическом совете школы. Положение вводится в действие приказом директора школы.
2.2. Положение об использовании сети Интернет разрабатывается педагогическим советом на основе примерного регламента самостоятельно, либо с привлечением внешних экспертов, в качестве которых могут выступать:
- преподаватели других образовательных учреждений, имеющие опыт использования Интернета в образовательном процессе;
- специалисты в области информационных технологий;
- представители органов управления образованием;
- родители обучающихся.
2.3. При разработке Положения об использовании сети Интернет педагогический совет руководствуется:
- законодательством Российской Федерации;
- 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.
2.4. Директор школы отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в МБОУ СОШ (военвед) г Зернограда, а также за выполнение установленных правил. Для обеспечения доступа участников образовательного процесса к сети Интернет в соответствии с установленным в школе Положением директор назначает своим приказом ответственного за организацию работы с Интернетом и ограничение доступа.

2.5. Заместитель директора школы по УВР:

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

- определяет характер и объем информации, публикуемой на интернет-ресурсах школы;

- дает руководителю школы рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за обеспечение доступа к ресурсам сети Интернет и контроль безопасности работы в Сети;

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

- наблюдает за использованием компьютера и сети Интернет обучающимися;

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

2.7. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют ответственный за организацию доступа к ресурсам сети Интернет, определенные приказом его руководителя.

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. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в школе или предоставленного оператором услуг связи.
2.9. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в школе Положением обеспечивается работником школы, назначенным его руководителем.
2.10. Принципы размещения информации на интернет-ресурсах школы призваны обеспечивать:

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

- защиту персональных данных обучающихся, преподавателей и сотрудников;

- достоверность и корректность информации.

2.11. 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 преподавателей и сотрудников школы размещаются на его интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.

2.12. 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 преподавателя, сотрудника или родителя.

2.13. 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 МБОУ СОШ (военвед) г Зернограда

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

3.2. По разрешению лица, ответственного за организацию в школе работы сети Интернет и ограничение доступа, преподаватели, сотрудники и обучающиеся вправе:

- размещать собственную информацию в сети Интернет на интернет-ресурсах школы;
- иметь учетную запись электронной почты 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.

3.4. 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 организацию доступа к ресурсам сети Интернет. 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 школе технических средствах технического ограничения доступа к информации.

ПОЛОЖЕНИЕ об информационной открытости МБОУ СОШ (военвед) г Зернограда

Настоящее положение включает в себя ч 1. 29 статью Федерального закона № 273 «Об образовании в Российской Федерации» от 20.12.2012г и является нормой, которой руководствуется МБОУ СОШ (военвед) г Зернограда (далее - ОО).

1. ОО формирует открытые и общедоступные информационные ресурсы, содержащие информацию об его деятельности, и обеспечивают доступ к таким ресурсам посредством размещения их в информационно-телекоммуникационных сетях, в том числе на официальном сайте ОО в сети "Интернет".

2. ОО обеспечивает открытость и доступность:

1) информации:

а) о дате создания ОО, об учредителе, о месте нахождения ОО и ее филиалов (при наличии), режиме, графике работы, контактных телефонах и об адресах электронной почты;

б) о структуре и об органах управления ОО;

в) о реализуемых образовательных программах с указанием учебных предметов, курсов, дисциплин (модулей), практики, предусмотренных соответствующей образовательной программой;

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;

д) о языках образования;

е) о федеральных государственных образовательных стандартах, об образовательных стандартах (при их наличии);

ж) о руководителе ОО, его заместителях, руководителях филиалов образовательной организации (при их наличии);

з) о персональном составе педагогических работников с указанием уровня образования, квалификации и опыта работы;

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);

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

л) 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;

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

н) о трудоустройстве выпускников;

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 Федерального закона «Об образовании», правил внутреннего распорядка обучающихся, правил внутреннего трудового распорядка, коллективного договора;

3) отчета о результатах самообследования.

Показатели деятельности ОО, 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;*

6) иной информации, которая размещается, опубликовывается по решению ОО и (или) размещение, опубликование которой являются обязательными в соответствии с законодательством Российской Федерации.

3. Информация и документы, указанные в п. 2 настоящего Положения, 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.

ПОЛОЖЕНИЕ о сайте МБОУ СОШ (военвед) г Зернограда (http://sosh16zernograd.ru)

1. Общие положения

1.1. Положение о сайте МБОУ СОШ (военвед) г Зернограда (далее - положение) определяет статус сайта http://sosh16zernograd.ru) (далее - сайт), структуру и порядок размещения в сети Интернет информационных материалов, образующих информационные ресурсы МБОУ СОШ (военвед) г Зернограда (далее - ОУ), а также права, обязанности, ответственность и регламент взаимодействия администратора, осуществляющего программно-техническую поддержку данного сайта, и лиц, осуществляющих предоставление информации для размещения в его разделах.

1.2. Сайт обеспечивает официальное представление информации о ОУ в сети Интернет с целью расширения рынка образовательных услуг ОУ, оперативного ознакомления сотрудников, обучающихся, родителей (законных представителей) обучающихся, деловых партнеров и других заинтересованных пользователей с различными аспектами деятельности ОУ, повышения эффективности взаимодействия ОУ с целевой аудиторией.

1.3. Пользователем сайта может быть любое лицо, имеющее технические возможности выхода в Интернет.

1.4. Функционирование сайта регламентируется действующим законодательством, Уставом ОУ, настоящим положением, а также локальными нормативными актами ОУ, приказами и распоряжениями директора ОУ.

1.5. Положение вступает в силу со дня утверждения директором ОУ и действует до его отмены.

1.6. Изменения в положение могут вноситься по рекомендации администрации ОУ, а также лиц, ответственных за информационное наполнение и поддержание сайта. Изменѐнная редакция положения вступает в силу после утверждения ее директором ОУ.

2. Информационный ресурс сайта

2.1. Информационный ресурс сайта (контент) формируется в соответствии с деятельностью всех структурных подразделений ОУ, ее сотрудников, обучающихся, родителей и общественных организаций ОУ.

2.2. Права на информационные материалы, размещенные на сайте, принадлежат ОУ при условии, что иное не регламентировано отдельными юридически оформленными документами.

2.3. Информационный ресурс сайта является открытым и общедоступным, если иной статус ресурса не оговорен специальными документами.

2.4. Условия размещения ресурсов ограниченного доступа регулируются отдельными документами; размещение таких ресурсов допустимо только при наличии соответствующих организационных и программно-технических возможностей.

2.5. Основными информационно-ресурсными компонентами сайта являются: - общая информация о ОУ как муниципальном образовательном учреждении; - справочные и иные материалы об образовательных программах ОУ;
- материалы по организации учебного процесса;
- подборки тематических материалов;
- материалы о персоналиях - руководителях, сотрудниках ОУ;
- материалы о событиях текущей жизни ОУ, проводимых в ОУ и при ее участии мероприятиях, архивы новостей;
- материалы о ходе реализации в ОУ комплексного проекта модернизации образования;
- адресные информационные материалы.
2.6. Часть информационного ресурса, формируемого по инициативе творческих коллективов и отдельных работников ОУ, может быть размещена на отдельных специализированных сайтах, доступ к которым организуется с сайта ОУ.

3. Организация работ

3.1. Информационное наполнение и актуализация сайта осуществляется совместными усилиями всех структурных подразделений ОУ, ее сотрудников, обучающихся, родителей и общественных организаций ОУ.
3.2. По каждому разделу сайта (виду информационного ресурса) определяются должностные лица, ответственные за подборку и предоставление соответствующей информации.
3.3. Руководство обеспечением функционирования сайта и его программно-технической поддержкой, непосредственное выполнение работ по размещению информации на сайте, обеспечению ее целостности и доступности, реализации правил разграничения доступа возлагается на администратора сайта (далее — администратор), который назначается директором школы.
3.4. Администратор сайта курирует качественное выполнение всех видов работ, связанных с эксплуатацией сайта: изменение дизайна и структуры, размещение новой и удаление устаревшей информации, публикация информации из баз данных, реализация политики разграничения доступа и обеспечение безопасности информационных ресурсов.
3.5. Администратор сайта осуществляет консультирование лиц, ответственных за предоставление информации, а также других работников, заинтересованных в размещении информации на сайте.
3.6. Информация, готовая для размещения на сайте, предоставляется должностными лицами, ответственными за подборку и предоставление соответствующей информации по разделам школьного сайта, в электронном виде администратору сайта, который обеспечивает ее размещение в соответствующем разделе сайта.
3.7. Текстовая информация предоставляется в формате .doc, графическая - в формате .jpg. В порядке исключения графическая информация может быть предоставлена в виде фотографий, схем, чертежей - в этом случае администратор изыскивает возможность перевода материалов в электронный вид.

3.8. Администратор сайта имеет право направить материалы на пересмотр с целью проведения корректуры и редакторской правки.

3.9. Текущие изменения структуры сайта, изменения, носящие концептуальный характер, согласовываются с директором ОУ.

4. Ответственность

4.1. Ответственность за недостоверное, несвоевременное или некачественное предоставление информации (в том числе с грамматическими и/или синтаксическими ошибками) для размещения на сайте несет соответствующее должностное лицо, ответственное за предоставление данной информации.

4.2. Ответственность за некачественное текущее сопровождение сайта несет администратор.

4.3. Некачественное текущее сопровождение может выражаться:

- в несвоевременном размещении предоставляемой информации;
- в непринятии мер по исключению появления на сайте устаревшей или ошибочной информации;
- в совершении действий, повлекших причинение вреда информационному ресурсу, нарушение работоспособности или возможность несанкционированного доступа к сайту.

4.4. Ответственность за нарушение работоспособности и актуализации сайта вследствие отсутствия четкого порядка во взаимодействии с лицами, ответственными за предоставление информации, отказ в консультировании сотрудников школы в соответствии с п.3.5 настоящего положения, несет администратор сайта.

5. Контроль

5.1. Контроль над выполнением обязанностей лицами, участвующими в процессах информационного наполнения, актуализации и программно-технического сопровождения сайта, возлагается на директора ОУ.

ИНСТРУКЦИЯ для педагогических работников и сотрудников муниципального общеобразовательного учреждения МБОУ СОШ (военвед) г Зернограда о порядке действий при осуществлении контроля использования обучающимися сети Интернет

1. Настоящая инструкция устанавливает порядок действий сотрудников образовательного учреждения при обнаружении:

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

2) отказа 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;

2) во время использования сети Интернет для свободной работы обучающихся — дежурный преподаватель.

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 ОУ 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 преподавателя, содержит информацию, запрещенную для распространения в соответствии с законодательством Российской Федерации, или иного потенциально опасного для обучающихся контента, он сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

5. В случае отказа доступа к ресурсу, разрешенному в ОУ, преподаватель также сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

ПОРЯДОК доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности

1. Настоящий Порядок регламентирует доступ педагогических работников МБОУ СОШ (военвед) г Зернограда (далее - Учреждение) к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности.

2. Доступ педагогических работников к вышеперечисленным ресурсам обеспечивается в целях качественного осуществления образовательной и иной деятельности, предусмотренной уставом Учреждения.

3. Доступ к информационно-телекоммуникационным сетям

3.1. Доступ педагогических работников к информационно-телекоммуникационной сети Интернет в Учреждении осуществляется с персональных компьютеров (ноутбуков, компьютеров и т.п.), подключенных к сети Интернет, в пределах установленного лимита на входящий трафик, а также возможности Учреждения по оплате трафика /без ограничения времени и потребленного трафика.

3.2. Доступ педагогических работников к локальной сети Учреждения осуществляется с персональных компьютеров (ноутбуков, компьютеров и т.п.), подключенных к локальной сети Учреждения, без ограничения времени и потребленного трафика.

3.3. Для доступа к информационно-телекоммуникационным сетям в Учреждении педагогическому работнику предоставляются идентификационные данные (логин и пароль / учѐтная запись / электронный ключ и др.). Предоставление доступа осуществляется системным администратором / заместителем директора Учреждения.

4. Доступ к базам данных

4.1. Педагогическим работникам обеспечивается доступ к следующим электронным базам данных:

- база данных АСИОУ;

- информационные справочные системы;

- поисковые системы.

4.2. Доступ к электронным базам данных осуществляется на условиях, указанных в договорах, заключенных Учреждением с правообладателем электронных ресурсов (внешние базы данных).

4.3. Информация об образовательных, методических, научных, нормативных и других электронных ресурсах, доступных к пользованию, размещена на сайте Учреждения в

разделе «Информационные ресурсы». В данном разделе описаны условия и порядок доступа к каждому отдельному электронному ресурсу.

5. Доступ к учебным и методическим материалам

5.1. Учебные и методические материалы, размещаемые на официальном сайте Учреждения, находятся в открытом доступе.

5.2. Педагогическим работникам по их запросам могут выдаваться во временное пользование учебные и методические материалы, входящие в оснащение групповых комнат. Выдача педагогическим работникам во временное пользование учебных и методических материалов, входящих в оснащение групповых комнат, осуществляется работником, на которого возложено заведование групповой комнатой. Срок, на который выдаются учебные и методические материалы, определяется работником, на которого возложено заведование групповой комнатой, с учетом графика использования запрашиваемых материалов в данной групповой комнате. Выдача педагогическому работнику и сдача им учебных и методических материалов фиксируются в журнале выдачи. При получении учебных и методических материалов на электронных носителях, подлежащих возврату, педагогическим работникам не разрешается стирать или менять на них информацию.

6. Доступ к материально-техническим средствам обеспечения образовательной деятельности

6.1. Доступ педагогических работников к материально-техническим средствам обеспечения образовательной деятельности осуществляется:

- без ограничения к актовому залу, физкультурному залу и другим помещениям во время, определенное в расписании занятий;

- к актовому залу, физкультурному залу и другим помещениям и местам проведения занятий вне времени, определенного расписанием занятий, по согласованию с работником, ответственным за данное помещение.

6.2. Использование движимых (переносных) материально-технических средств обеспечения образовательной деятельности (проекторы и т.п.) осуществляется по письменной заявке, поданной педагогическим работником (не менее чем за 5 рабочих дней до дня использования материально-технических средств) на имя лица, ответственного за сохранность и правильное использование соответствующих средств. Выдача педагогическом работнику и сдача им движимых (переносных) материально-технических средств обеспечения образовательной деятельности фиксируются в журнале выдачи.

6.3. Для копирования, распечатывания или тиражирования учебных и методических материалов педагогические работники имеют право пользоваться копировальной техникой.

7. Накопители информации (CD-диски, флеш-накопители, карты памяти), используемые педагогическими работниками при работе с компьютерной информацией, предварительно должны быть проверены на отсутствие вредоносных компьютерных программ.

КЛАССИФИКАТОР
информации, не имеющей отношения к образовательному процессу в муниципальном общеобразовательном учреждении МБОУ СОШ (военвед) г Зернограда

1. Классификацию информации, запрещенной законодательством Российской Федерации к распространению и не имеющей отношения к образовательному процессу, осуществляют специальные экспертно-консультативные органы (советы) при органах управления образованием.

2. Классификатор информации, запрещенной законодательством Российской Федерации к распространению, применяется в единообразном виде на всей территории Российской Федерации.

3. Классификатор информации, не имеющей отношения к образовательному процессу, может содержать как части (разделы), рекомендуемые к применению в единообразном виде на всей территории Российской Федерации, так и части (разделы), рекомендуемые к использованию экспертно-консультативными органами (советами) регионального и (или) муниципального уровня.

4. В соответствии с законодательством Российской Федерации образовательное учреждение свободно в выборе и применении классификаторов информации, не имеющей отношения к образовательному процессу, а также несет ответственность за невыполнение функций, отнесенных к его компетенции.

5. Рекомендации по формированию Классификатора информации, распространение которой запрещено в соответствии с законодательством Российской Федерации, разработаны в соответствии с проведенным анализом законодательства Российской Федерации и международных договоров Российской Федерации.

№№	Тематическая категория	Содержание
1	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
2	Злоупотребление	— экстремизм Информация, содержащая публичные призывы

	свободой СМИ	к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы
3	Злоупотребление свободой СМИ	— наркотические средства Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких- либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров
4	Злоупотребление свободой СМИ	— информация с ограниченным доступом Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций
5	Злоупотребление свободой СМИ	— скрытое воздействие Информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающая вредное влияние на их здоровье
6	Экстремистские материалы или экстремистская деятельность (экстремизм)	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; Б) экстремистская деятельность (экстремизм) включает деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков: • насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; • подрыв безопасности Российской Федерации, захват или присвоение властных полномочий, создание незаконных вооруженных формирований; • осуществление террористической деятельности либо публичное оправдание терроризма; • возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию; • унижение национального достоинства; • осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы; • пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности; • воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, сопровождаемое насилием или угрозой его применения;

		• 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; • 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; • посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность; • нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением
7	Вредоносные программы	Вредоносные Программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети
8	Преступления	• Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию); • оскорбление (унижение чести и достоинства другого лица, выраженное в неприличной форме); • публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма; • склонение к потреблению наркотических средств и психотропных веществ; • незаконное распространение или рекламирование порнографических материалов; • публичные призывы к осуществлению экстремистской деятельности; • информация, направленная на пропаганду национальной, классовой, социальной нетерпимости, а также социального, расового, национального и религиозного неравенства; • публичные призывы к развязыванию агрессивной войны
9	Ненадлежащая реклама	Информация, содержащая рекламу алкогольной продукции и табачных изделий
10	Информация с ограниченным доступом	Информация, составляющая государственную, коммерческую, служебную или иную охраняемую законом тайну

6. 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 образовательного учреждения, социокультурных особенностей автономного округа и иных обстоятельств.

№№	Тематическая категория	Содержание
1	Алкоголь	Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию
2	Баннеры и рекламные программы	Баннерные сети, всплывающая реклама, рекламные программы
3	Вождение и автомобили (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям
4	Досуг и развлечения (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация: • фотоальбомы и фотоконкурсы; • рейтинги открыток, гороскопов, сонников; • гадания, магия и астрология; • ТВ-программы; • прогнозы погоды; • тесты, конкурсы онлайн; • туризм, путешествия; • тосты, поздравления; • кроссворды, сканворды, ответы к ним; • фантастика; • 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 дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними; • о рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании; • о службах знакомств, размещении объявлений онлайн; • анекдоты, «приколы», слухи; • о сайтах и журналах для женщин и для мужчин; • желтая пресса, онлайн-ТВ, онлайн-радио; • о знаменитостях; • о косметике, парфюмерии, прическах, ювелирных украшениях.
5	Здоровье и медицина (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу 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.)
6	Компьютерные игры (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу компьютерные онлайновые и оффлайновые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты

7	Корпоративные сайты, интернет представительства негосударственных учреждений (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, сайты коммерческих фирм, компаний, предприятий, организаций
8	Личная и немодерируемая информация	Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги
9	Отправка SMS с использованием интернет-ресурсов	Сайты, предлагающие услуги по отправке SMS-сообщений
10	Модерируемые доски объявлений (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты
11	Нелегальная помощь школьникам и студентам	Банки готовых рефератов, эссе, дипломных работ и пр
12	Неприличный и грубый юмор	Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека
13	Нижнее белье, купальники	Сайты, на которых рекламируется и изображается нижнее белье и купальники
14	Обеспечение анонимности пользователя, обход контентных фильтров	Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам; Peer-to-Peer программы, сервисы бесплатных прокси-серверов, сервисы, дающие пользователю анонимность
15	Онлайн-казино и тотализаторы	Электронные казино, тотализаторы, игры на деньги, конкурсы и пр.
16	Платные сайты	Сайты, на которых вывешено объявление о платности посещения веб-страниц
17	Поиск работы, резюме, вакансии (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-представительства кадровых агентств, банки вакансий и резюме
18	Поисковые системы (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-каталоги, системы поиска и навигации в Интернете
19	Религии и атеизм (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Сайты, содержащие, не имеющую отношения к образовательному процессу, информацию религиозной и антирелигиозной направленности.

20	Системы поиска изображений	Системы для поиска изображений в Интернете по ключевому слову или словосочетанию
21	СМИ (ресурсы СМИ, содержащие новостные ресурсы и сайты	СМИ (радио, данной категории, не имеющие отношения к образовательному процессу) телевидения, печати), не имеющие отношения к образовательному процессу.
22	Табак, реклама табака, пропаганда потребления табака	Сайты, пропагандирующие потребление табака; реклама табака и изделий из него
23	Торговля и реклама (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие, не имеющие отношения к образовательному процессу, сайты следующих категорий: аукционы, распродажи онлайн, интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, недвижимость, аренда недвижимости, покупка недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в Интернете, е-бизнес
24	Убийства, насилие	Сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.
25	Чаты (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу сайты для анонимного общения в режиме онлайн.

РЕГЛАМЕНТ работы с электронной почтой в муниципальном общеобразовательном учреждении МБОУ СОШ (военвед) г Зернограда

1. Общие положения

1.1. Муниципальное бюджетное общеобразовательное учреждение средняя общеобразовательная школа (военвед) г Зернограда (далее - ОУ) имеет свой адрес электронной почты: soshvoenved@mail. ru

1.2. Электронная почта в ОУ может использоваться только в административных и образовательных целях.

1.3. Пользователи и владельцы электронных почтовых ящиков должны соблюдать правила и инструкции по работе с электронной почтой, этические нормы общения.

1.4. Перед отправлением сообщения или отчета необходимо проверить правописание и грамматику текста.

1.5. Пользователям данного сервиса запрещено:

- участвовать в рассылке посланий, не связанных с образовательной или административной деятельностью ОУ;

- пересылать по произвольным адресам не затребованную потребителями информацию (спам);

- отправлять сообщения противозаконного или неэтического содержания;

- использовать массовую рассылку электронной почты, за исключением необходимых случаев; - электронное послание не должно использоваться для пересылки секретной и конфиденциальной информации, регламент обмена которыми утверждается иными нормативно-правовыми актами.

2. Порядок обработки, передачи и приѐма документов по электронной почте

2.1. По электронной почте производится получение и отправка информации законодательного, нормативно-правового, учебного, учебно-методического характера, а также любой другой информации, совместимой с процессом образования

2.2. Для обработки, передачи и приема информации по электронной почте в ОУ приказом директора назначается ответственное лицо - оператор электронной почты. 2.3. При создании электронного почтового ящика (ЭПЯ), сайта ОУ ответственное лицо направляет в муниципальный орган управления образованием свои электронные реквизиты для формирования базы данных образовательных учреждений муниципалитета.

2.4. Администрация ОУ должна обеспечить бесперебойное функционирование сервиса электронной почты и регулярное получение и отправку информации в течение всего рабочего дня.

2.5. Ответственность за ненадлежащую подготовку информации к передаче по электронной почте несет автор информации, предполагаемой к отправке.

2.6. Ответственность за отправку адресату и получение электронной почты несет оператор электронной почты.

2.7. Передаваемые с помощью электронной почты официальные документы должны иметь исходящий регистрационный номер.

2.8. Все передаваемые учебно-методические и справочно-информационные материалы должны передаваться с сопроводительным письмом. Для отправки электронного сообщения пользователь оформляет документ в соответствии с требованиями по делопроизводству, утвержденными в ОУ.

2.9. При получении электронного сообщения оператор:

- передает документ на рассмотрение администрации ОУ или в случае именного сообщения

- непосредственно адресату;

- в случае невозможности прочтения электронного сообщения уведомляет об этом отправителя.

2.10. Отправка и получение электронных документов осуществляется с использованием программных продуктов, предназначенных для работы с электронной почтой в ОУ.

2.11. Учет электронных документов осуществляется путем регистрации в журнале регистрации входящих / исходящих документов.

2.12. Электронные документы дублируются в виде копий на бумажных носителях с присвоением номера входящего или исходящего документа. Сроки их хранения регламентируются иными нормативными актами.

3. Ответственность

3.1. Изменение наименования официального ЭПЯ (электронного почтового ящика) ОУ согласовывает со специалистами Управления образования Администрации Зерноградского района, ведущими электронный документооборот и отвечающими за информатизацию системы муниципального образования.

3.2. По факту изменения официального ЭПЯ ОУ обязано уведомить информационным письмом Управление образования Администрации Зерноградского района за 3 рабочих дня до смены ЭПЯ с указанием даты, с которой изменения вступают в силу.
3.3. Ответственность за функционирование электронного документооборота в учреждении несет директор ОУ.

ИНСТРУКЦИЯ по организации антивирусной защиты в муниципальном бюджетном общеобразовательном учреждении МБОУ СОШ (военвед) г Зернограда

1. Общие положения

1.1. Настоящая инструкция предназначена для организации порядка проведения антивирусного контроля в МБОУ СОШ (военвед) г Зернограда (далее - ОУ) и предотвращения возникновения фактов заражения программного обеспечения компьютерными вирусами, а также фильтрации доступа пользователей ОУ к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

1.2. Директором школы назначается лицо, ответственное за организацию антивирусной защиты в ОУ.

1.3. В ОУ может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

1.4. Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным за организацию антивирусной защиты в ОУ.
1.5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (магнитных дисках, лентах, CD-ROM, DVD, flash-накопителях и т.п.).

1.6. Контроль информации на съѐмных носителях производится непосредственно перед еѐ использованием.

1.7. Файлы, помещаемые в электронный архив или на сервер, должны в обязательном порядке проходить антивирусный контроль.

1.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

1.9. Факт выполнения антивирусной проверки должен регистрироваться в специальном журнале за подписью лица, ответственного за организацию антивирусной защиты.

2. Мероприятия, направленные на решение задач по антивирусной защите:

2.1. Установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения.

2.2. Регулярное обновление и профилактические проверки (обновление ежедневное; профилактические проверки: 1 раз в неделю во вторник с 12.00).

2.3. Непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах информационно коммуникационной системы (далее ИКС) ОУ.

2.4. Проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.

2.5. Внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.

2.6. Необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.

2.7. Обеспечение бесперебойной работы ОУ для случаев вирусного заражения, в том числе резервного копирования всех необходимых данных и программ и их восстановления.

3. Требования к проведению мероприятий по антивирусной защите

3.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезагрузке) в автоматическом режиме должно выполняться обновление антивирусных баз и серверов и проводиться антивирусный контроль всех дисков и файлов персонального компьютера и съѐмных носителей.

3.2. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

3.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

3.3.1. непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети) должна быть выполнена антивирусная проверка на серверах и персональных компьютерах ОУ;

3.3.2. при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.);

3.3.3. при отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

4.1.1. приостановить работу;

4.1.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в ОУ;

4.1.3. совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

4.1.4. провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса ответственный за организацию антивирусной защиты должен провести внеочередной антивирусный контроль.

5. Ответственность

5.1. Ответственность за организацию антивирусной защиты и выполнение положений данной инструкции возлагается на лицо, назначенное директором ОУ.

5.2. Ответственность за проведение мероприятий антивирусного контроля в ОУ возлагается на ответственного за организацию антивирусной защиты.

5.3. Ответственность за соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

5.4. Периодический контроль за состоянием антивирусной защиты в ОУ осуществляется директором ОУ и фиксируется Актом проверки (не реже 1 раза в квартал).

ПОЛОЖЕНИЕ об электронном классном журнале

1. Общие положения

1.1. Электронным классным журналом называется комплекс программных средств, включающий базу данных и средства доступа к ней (подсистема «электронный журнал» в АИС ОУ).

1.2. Пользователями электронного журнала являются администрация школы, учителя и классные руководители.

1.3. Электронный классный журнал служит для решения следующих задач:

1.3.1. хранение данных об календарно-тематическом планирование по всем предметам, об успеваемости и посещаемости обучающихся;

1.3.2. оперативный доступ к оценкам за весь период ведения журнала, по всем предметам, в любое время;

1.3.3. автоматизация создания периодических отчетов учителей и администрации;
1.3.4. своевременное информирование родителей по вопросам успеваемости их детей.
1.4. Поддержание информации хранящейся в базе данных электронного классного журнала в актуальном состоянии является обязательным.

1.5. Категорически запрещается допускать учащихся к работе с электронным журналом.

2. Правила и порядок работы с электронным классным журналом

2.1. Заместитель директора по УВР, отвечающий за информатизацию ОУ обеспечивает надлежащее функционирование программно-аппаратной среды.

2.2. Пользователи получают реквизиты (логин и пароль) доступа к электронному журналу в следующем порядке:

2.2.1. Классные руководители, администрация получают реквизиты доступа у ответственного администратора по работе в АИС ОУ;

2.2.2. Родители получают реквизиты доступа к электронному дневнику у классного руководителя по заявлению (приложение 1).

2.3. Классные руководители своевременно заполняют и следят за актуальностью данных электронного журнала.

2.4. Учителя аккуратно и своевременно заполняют пройденные темы уроков, данные об успеваемости и посещаемости учащихся.

2.5. Заместитель директора по УВР осуществляют периодический контроль за ведением электронного журнала: своевременность выставления отметок учителями, заполнения тем, заинтересованность родителей в данной электронной услуге.

2.6. Родители имеют доступ только к собственным данным и используют электронный дневник для их просмотра.

3. Права и обязанности пользователей

3.1. Права:

3.1.1. Все пользователи имеют право на своевременные консультации по вопросам работы с электронным журналом;

3.2. Обязанности:

3.2.1. Заместитель директора по информатизации несет ответственность за техническое функционирование электронного журнала.

3.2.2. Учителя несут ответственность за ежедневное и достоверное заполнение журнала (тема урока, оценки и отметки о посещаемости учащихся);

3.2.3. Классные руководители несут ответственность за актуальность данных: списки класса, данные об успеваемости и посещаемости и за своевременное оповещение родителей о проблемах, связанных с поведением ребѐнка в школе.

3.2.4. Все пользователи несут ответственность за сохранность своих реквизитов доступа;

3.2.5. Все пользователи несут ответственность за сохранность персональных данных обучающихся.

Приложение 3

Методические рекомендации «Безопасный Интернет»

В наши дни компьютер становится привычным элементом не только в научных лабораториях, но и дома, в школьных классах. Так, например, в Российской Федерации в настоящее время уже эксплуатируется не менее 5 млн. персональных компьютеров. В Западной Европе компьютер используют свыше 60% взрослого населения. Людей, ежедневно проводящих за компьютером по нескольку часов, становится все больше. При этом уже мало кто сомневается, что работа на персональном компьютере влияет на физическое и психологическое здоровье человека не самым лучшим образом. Длительное пребывание у экрана, неподвижность позы пользователя ПК, электромагнитные поля и излучения, мелькание изображения на экране - все это небезвредно для здоровья. Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Мы понимаем, что Интернет - это не

только кладезь возможностей, но и источник угроз. Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них - дети, которые могут не знать об опасностях мировой паутины. Одним из средств решения этой проблемы может стать просвещение общественности и специальная подготовка профессионалов, в первую очередь, педагогов в сфере безопасного поведения человека, специалиста, школьника в мире компьютерных технологий и Интернет. В данном разделе представлены материалы для разработки классных часов для школьников трех возрастных групп, направленные на обеспечение необходимыми знаниями в области психолого-педагогического и здоровьесберегающего сопровождения образовательного процесса, персонала и школьников, использующих персональные компьютеры и Интернет в профессиональной, учебной и внеучебной деятельности. Кроме того, пособие может быть интересно родителям школьников, так как содержит советы и рекомендации, как сделать компьютер и Интернет безопасным для своего ребенка. Данные рекомендации - практическая информация для родителей и классных руководителей, которая поможет предупредить угрозы и сделать работу детей в Интернете полезной.

Родительское собрание Тема: «Интернет: плюсы и минусы»

Цель: рассказать родителям, какие угрозы существуют и как их избежать.

«Ваши дети дома?» Незатейливый вопрос, адресованный родителям, каждый вечер звучит в телеэфире. Дети дома, но в безопасности ли они? С тех пор, как Интернет перестал быть роскошью и пришел буквально в каждый дом, он стал неотъемлемой частью жизни не только взрослых, но и детей.

Даже родители, некогда расценивавшие доступ во Всемирную сеть как баловство, вынуждены признать: Интернет содержит массу полезной для ребенка информации, помогает в выполнении школьных заданий, расширяет кругозор и является своеобразным «окном в большой мир». С другой стороны, только очень наивный взрослый не знает, сколько в Сети ресурсов, которые отнюдь не назовешь безопасными - особенно для детей, любопытных и жадных до новых знаний. Судите сами: программы, запрещающие доступ к «плохим» ресурсам, не оправдывают надежд, поскольку просто не в силах фильтровать все вредоносное содержимое. Как должны родители помочь детям снизить эти риски? Простого ответа не существует. Риски могут быть разными в зависимости от возраста и компьютерной грамотности ребенка. Вот вы, родители, на данный момент знаете, какими сайтами пользуются ваши дети? Нет? Очень печально. Именно с этого надо начинать работу с безопасным интернетом. Для детей и молодежи Интернет главным образом является социальной средой, в которой можно не только встречаться с друзьями, но и с незнакомцами. В Интернете пользователя могут обидеть, запугать или даже оскорбить. Лучшей защитой является руководство собственным здравым смыслом. Наиболее важной задачей является предупреждение детей об опасностях Интернета, чтобы они вели себя

осторожно. Кроме того, необходимо обсуждать с детьми все вопросы, которые могут у них возникнуть при использовании Интернета. Не отвергайте детей, а наоборот, постарайтесь как можно ближе расположить их доверие. Тогда вы будете в курсе той информации, которой владеют ваши дети. Даже если ребенок не сталкивался с оскорблениями в Интернете, рекомендуется обсудить с ним следующие вопросы: • Не распространяйте контактную или личную информацию, например, фотографии, без тщательного обдумывания возможных последствий. Интерактивная дружба может закончиться. Когда это произойдет, личная информация может быть отправлена злоумышленникам.

• В Интернете каждый человек имеет право на уважительное отношение.

• Детям должна быть предоставлена возможность поговорить с родителями об отрицательном опыте.

Безопасное использование в соответствии с возрастом

Дети до 7 лет Во время первого знакомства с Интернетом закладывается фундамент для его последующего использования и формирования хороших манер у детей. Детям дошкольного возраста нравится установленный порядок, и это является идеальным способом развития у детей навыков безопасного использования Интернета. Дети до 7 лет могут не полностью понимать информацию, доступную в Интернете, и, например, не отличать рекламу от действительного содержимого. В этом возрасте родителям необходимо помогать детям в поиске подходящего материала. Дети часто не видят разницы между использованием Интернета и играми или рисованием на компьютере. На этом этапе вы можете установить первые внутренние правила использования компьютера. Время, проводимое за компьютером, необходимо ограничить по причинам, связанным со здоровьем. Поместите компьютер, например, в гостиной. При использовании Интернета дошкольниками рекомендуется присутствие взрослого. Доступ к Интернету для дошкольников необходимо ограничить до списка знакомых веб-сайтов, выбранных заранее. Более подготовленные дети могут найти знакомые сайты в меню «Избранное» обозревателя Интернета.

Самым безопасным решением является создание для ребенка персональной рабочей среды, в которой выбор сайтов ограничивается только указанными сайтами.

Дети 7-9 лет Юные школьники будут иметь дело с Интернетом не только у себя дома, но и в школе, и у друзей. Вы вместе с детьми должны обсудить, как использовать Интернет надлежащим образом и согласовать правила, которым необходимо следовать. Дети 7-9 лет уже могут иметь относительно хорошее представление о том, что они видят. Тем не менее, они не готовы к обращению со всем материалом, доступным в Интернете, особенно с пугающим или неуместным материалом (изображения, текст или звук). Разговор об этих материалах и объяснение различных вещей, с которыми дети могут столкнуться в Интернете, поможет детям стать

ответственными и способными самостоятельно и безопасно работать в Интернете. Вы можете поделиться собственными мнениями и взглядами на использование Интернета, чтобы помочь своим детям. В этом возрасте ограничения, защита и использование Интернета под присмотром по-прежнему являются первостепенными. Родителям и детям рекомендуется согласовать правила использования Интернета и пересматривать их по мере взросления детей. Использование Интернета дома по-прежнему разрешено только в присутствии родителей. Это обеспечивает получение помощи в любой проблемной ситуации. Если компьютер установлен в комнате, которой пользуется вся семья, использование Интернета становится естественным для повседневной жизни. Ребенок еще не может определить надежность веб-сайта самостоятельно, поэтому ему всегда следует спрашивать разрешения у родителей перед публикацией личной информации. Для предотвращения доступа к неуместным сайтам можно также применять программы фильтрации, но важно, чтобы родители по-прежнему активно участвовали в использовании Интернета ребенком.

Дети 10-12 лет Школьники уже могут знать, как использовать Интернет в различных целях. Родители могут поддержать ребенка, выяснив, какие сайты могут помочь с домашним заданием, содержат информацию о хобби или других увлечениях ребенка. Интернет может также использоваться для планирования вопросов, касающихся всей семьи. Это дает возможность родителям и детям обсудить надежность разных сайтов, а также источники поиска полезной и качественной информации. Ребенку необходим родительский присмотр и контроль, а также знание правил правильной работы в Сети. Тем не менее, ребенок может узнать, как избавиться от присмотра и обойти правила, если он будет считать их слишком ограничивающими или несоответствующими его потребностям. Родителям и детям необходимо прийти к соглашению относительно разрешенных и запрещенных действий в Интернете, а также его использования. В соглашении должны быть учтены все потребности и мнения. Договоритесь, какую личную информацию можно разглашать и в каких случаях, а также поговорите о рисках, связанных с разглашением информации. Если ребенок уже заинтересовался общением в чатах или IRC, вам следует обсудить с детьми их безопасность и контролировать их опыт в интерактивных обсуждениях. Многие дети любопытны и любознательны, поэтому родителям необходимо акцентировать внимание на необходимости безопасного и осторожного использования. Систему безопасности информации также необходимо обновлять.

Дети 13-15 лет В этом возрасте Интернет становится частью социальной жизни детей: в Интернете они знакомятся и проводят время, ищут информацию, связанную с учебой или увлечениями. При более высоком уровне грамотности использование Интернета открывает множество возможностей. Родителям, может быть, очень сложно узнать о том, чем их ребенок занимается в Интернете. В этом возрасте дети также склонны к риску и выходу за пределы дозволенного. Технические ограничения и запреты могут оказаться неэффективным способом повышения уровня безопасности в Интернете. Дети 13-15 лет могут захотеть сохранить свои действия в тайне, особенно если

родители раньше не интересовались и не узнавали о способах использования Интернета ребенком. Важным моментом для семьи становится участие в открытых дискуссиях, а для родителей — заинтересованность в том, что ребенок делает и с кем использует интернет ресурсы. Что за угрозы подстерегают наших детей в виртуальном мире? Этот вопрос задают многие родители, которые ещѐ не сталкивались с проблемами использования интернета. Поэтому целью собрания является рассказать, какие угрозы существуют и как их избежать. Даже случайный клик по всплывшему баннеру или переход по ссылке может привести на сайт с опасным содержимым! Если вы не знаете с чего начать, ознакомьтесь с приведенными ниже советами, которые помогут вам научить детей принципам безопасной работы в Интернете.

1. Убедите своих детей делиться с вами впечатлениями от работы в Интернете. Путешествуйте в Интернете вместе с детьми.

2. Научите детей доверять интуиции. Если что-нибудь в Интернете будет вызывать у них психологический дискомфорт, пусть дети рассказывают вам об этом.

3. Если ваши дети общаются в чатах, пользуются программами мгновенной передачи сообщений, играют в сетевые игры или занимаются в Интернете чем-то другим, что требует указания идентификационного имени пользователя, помогите им выбрать это имя и убедитесь в том, что оно не содержит никакой личной информации.

4. Запретите своим детям сообщать другим пользователям Интернета адрес, номер телефона и другую личную информацию, в том числе номер школы и любимые места для игр.

5. Объясните детям, что нравственные принципы в Интернете и реальной жизни одинаковы.

6. Научите детей уважать других пользователей Интернета. Разъясните детям, что при переходе в виртуальный мир нормы поведения нисколько не изменяются.

7. Добейтесь от детей уважения к собственности других пользователей Интернета. Расскажите детям, что незаконное копирование продуктов труда других людей, в том числе музыки, видеоигр и других программ, почти не отличается от воровства в магазине.

8. Убедите детей в том, что они не должны встречаться с интернет-друзьями лично. Скажите, что интернет-друзья могут на самом деле быть не теми, за кого они себя выдают.

9. Объясните детям, что верить всему, что они видят или читают в Интернете, нельзя. Скажите им, что при наличии сомнений в правдивости какой-то информации им следует обратиться за советом к вам.

10. Контролируйте действия своих детей в Интернете с помощью специализированного программного обеспечения. Средства родительского контроля помогают блокировать вредные материалы, следить за тем, какие веб-узлы посещают ваши дети, и узнавать, что они там делают.

Представьте себе Интернет, в котором нет порнографических сайтов, сомнительных социальных сетей, откровенных блогов, онлайн-казино, страниц, пропагандирующих фашизм, насилие и религиозную нетерпимость - словом, представьте себе действительно безопасный Интернет, в который вы спокойно «отпустите» своего ребенка одного. Недавно об этом можно было только мечтать, сейчас же каждый может убедиться в том, что мечта стала явью - достаточно скачать с сайта www.icensor.ru и установить на домашнем компьютере программу «ИнтернетЦензор». Безусловный плюс «Интернет Цензора» в том, что программу эту каждый родитель может «подстроить» под себя и своего ребенка, адаптировать к его интересам и увлечениям. Вам понадобится лишь пара минут на то, чтобы разрешить доступ к той или иной страничке. С другой стороны, если тот или иной «открытый» сайт покажется вам вредным для ребенка, запретить доступ к нему тоже не составит труда. «Интернет Цензор» — удобная и простая программа, не требующая мощного компьютера и специальных знаний. Распространяется она бесплатно, так же бесплатны и все обновления - это принципиальная позиция создателей программы, изменять которой они не собираются. Говоря о безопасности детей в Интернете, акцент следует сделать на то, что самое главное - это доверие между родителями и ребенком, готовность взрослых к диалогу, обсуждению непростых вопросов, да и просто разговорам о том, «что такое хорошо и что такое плохо».

Материалы для разработки классного часа. Интернет для обучающихся начальных классов. Безопасность детей в Интернете

Пока мы спорим "пущать" или "не пущать" учеников начальной школы в Интернет - они уже здесь. Мы снова опоздали. Очевидно, что сейчас невозможно гарантировать стопроцентную защиту детей от нежелательного контента. Никакие фильтры никогда такой гарантии не дадут. Но мы можем формировать у ребят навык "безопасного" поведения в Интернете. Как? Проблема относительно «свежая», но, решается «старыми» методами.

1) Родители должны знать, чем заняты их дети. Самое простое - разговаривать с детьми: чем живет, чем интересуется, какие сайты любит посещать и почему, с кем дружит, в том числе, и в Интернете. Кроме того (не вместо - кроме!) семейный фильтр на поисковой машине, контроль по логам и проч. Дети должны владеть основами безопасного пользования Интернет-сетями. Мы учим их не разговаривать с незнакомцами? Мы объясняем, что нельзя называть незнакомцам свой домашний адрес? Ну, и в сети все то же самое.

2) Учитель должен понимать, зачем он отправляет детей в Интернет. Учить «с Интернетом» нынче модно. Всегда ли это оправдано? Предположим, учитель сформулировал конкретные задачи урока, реализуемые с помощью Интернет-ресурсов. Какие здесь могут быть варианты обеспечения безопасности: - закрытые среды обучения, например, учебные блоги, где могут оставлять свои комментарии только те, кто получил соответствующий доступ от учителя, ведущего блог; - постановка конкретной учебной задачи: что хочу найти? где? как использую? - формирование навыков критического мышления; - список проверенных учителем ресурсов, с которых предлагается использовать информацию; - все те же фильтры и контроль системного администратора, если таковой в школе имеется.

Самое главное - приучать детей не «проводить время» в Интернете, а активно пользоваться полезными возможностями сети. 1. Вступительное слово учителя. Как вы думаете, ребята, для чего школьникам нужен Интернет?

Варианты ответов:

1. как площадка для общения (школьные сайты, блоги, форумы; сайты\блоги\форумы по интересам; электронная почта\ аська);

2. источник информации (использовать Интернет кроме\вместо учебника, графика, справочная информация, литература);

3. дистанционное обучение (дистанционные курсы, мастер-классы, консультирование болеющих детей и детей на домашнем обучении);

4. участие в сетевых конкурсах, олимпиадах, проектах.

Послушаем стихотворение о том, как правильно и безопасно пользоваться Интернетом:

Несколько правил Интернет-безопасности

1- й чтец: Интернет бывает разным: Другом верным иль опасным. И зависит это все От тебя лишь одного. Если будешь соблюдать Правила ты разные- Значит для тебя общение В нем будет безопасное! Будь послушен и внимательно Прочти, запомни основательно Правил свод, что здесь изложен, Для детишек он не сложен!

2- 2- й чтец: Если ты не в первый раз Компьютер сам включаешь И легко без лишних фраз Сайты, чаты посещаешь, Себя в нем мастером считаешь. Вдруг однажды сам решил В тайне от родителей Потихоньку завести Для общения в сети электронный адрес.

3- 3- й чтец: Указал без разрешения Адрес, улицу и дом, и квартиру в нем. Разместил на сайте ты фотографии семьи. Не забыл секреты старших - все в анкете указал, Все, что вспомнил, все, что знал! Переписываться стал,

подписался на рассылку, Фильмы разные качал. В общем, пока взрослых нет, заходил ты в Интернет.

4- 4- й чтец: И теперь сидишь довольный: стал мгновенно знаменит! О тебе все знают в школе! Что там в школе и в районе, Во всем мире знаменит! От друзей секретов нету - Это всем давно известно. Все тебе охотно пишут И секреты узнают. Целый мир про вас всѐ знает И при встрече сообщает: «Знаем, знаем, мы читали, фотографии видали. Прочитали, что твой папа на работу опоздал, А у мамы из кастрюли суп на плитку убежал. И про школьные проблемы всѐ читали и всѐ знаем!»

5- 5- й чтец: А по почте счѐт пришѐл вам за работу Интернета. Там стоят такие цифры! Что у мамы почему-то Враз глаза большими стали и обратно не встают. Потихоньку плачет мама, и сердитый ходит папа. Ведь они не знают правду, почему их узнают? Почему по счету нужно им вложить такие деньги?!

6- 6- й чтец: Все при встрече, сразу быстро им твердят одно и то же: - Знаем, знаем, прочитали, фотографии видали!... И воришка, к сожаленью, всѐ найдѐт без промедленья, Где и что у вас лежит.

А теперь запомни, Друг мой! Правила не сложные:

В Интернете, как и в жизни, Должен ты всѐ понимать: Информацию и фото с мамой вместе размещать.

На рассылку подписаться или мультики скачать, Должен с нею всѐ решать! Хочешь с мамой или с папой - это сам ты выбирай.

В Интернете, как и в жизни, Безопасность соблюдай!

- О каких несложных, но очень важных и нужных правилах пользования Интернетом говорится в этом стихотворении?

- Какие еще советы и предложения вы могли бы сами дать своим сверстникам, чтобы их нахождение в сети Интернет было полезным и безопасным?

Ну, и в заключение беседы можно использовать так называемое Джентельменское соглашение родителей (учителей) и детей

Перед первым выходом в Интернет как можно четче оговорите правила пользования сетью. Обсудите с ребенком, куда ему можно заходить (возможно на первых порах стоит составить список сайтов), что можно и что нельзя делать, сколько времени можно находиться в Интернете.

Сообщите ему о том контроле, который Вы намерены осуществлять: проверка посещенных ребенком страниц, контроль времени, проведенного в Сети, проверка адресов электронной почты. Объясните ребенку, что Вы доверяете ему и заботитесь о его безопасности.

Договоритесь с ребенком о соблюдении им следующих правил:

1. Сообщить родителям свое регистрационное имя и пароль, если ребенку разрешено участвовать в чатах или блогах, e-mail адрес и пароль почтового ящика.

2. Никому, кроме родителей, эти сведения сообщать категорически нельзя.

3. Не сообщать без разрешения родителей для каждого отдельного случая личную информацию (домашний адрес, номер телефона, номер школы, место работы родителей).
4. Не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через Интернет.
5. Сразу обратиться к родителям, если ребенок увидит нечто неприятное, тревожащее, угрожающее на сайте или в электронной почте.
6. Не соглашаться лично встретиться с человеком, с которым ребенок познакомился в Сети.
7. Если кто-то предлагает ребенку какой-то "секрет" - тут же сообщить об этом родителям.
8. Не скачивать, не устанавливать, не копировать ничего с дисков или из Интернета без разрешения родителей на каждый отдельный случай.
9. Не делать без разрешения родителей в Интернете ничего, что требует оплаты.
10. Проявлять уважение к собеседникам в Интернете, вести себя так, чтобы не обидеть и не рассердить человека. В течение некоторого времени сопровождайте ребенка в его путешествиях по сети для того, чтобы убедиться, что ребенок соблюдает ваш уговор.

Методическая разработка классного часа на тему:

«БезОпасный Интернет» (5 - 7 класс)

Цель: Познакомить учащихся с опасностями, которые подстерегают их в Интернете и помочь избежать этих опасностей.

Подготовительная работа:

классный руководитель проводит опрос учащихся по вопросам:

1) У вас на домашнем компьютере установлен Интернет?

2) Что вам больше всего нравится в Интернете?

3) Как ваши родители воспринимают ваши занятия в Интернете? Почему?

Оборудование:

компьютер, проектор, презентация, памятка учащимся.

Ход занятия

Учитель: Раньше подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. И начать наш классный час я хочу с обработанных данных проводимого опроса. Давайте обратим внимание, что наибольший процент ответов на последний вопрос связан с безопасностью в Интернете. И ваши родители во многом правы! Очень

большое внимание при работе с Интернетом необходимо уделять именно вопросам безопасности. И ответить на вопросы: «Какие опасности подстерегают нас в Интернете?» и «Как их избежать?» нам поможет этот классный час.

Вопрос 1. «Какие опасности подстерегают нас в Интернете?»

1) Преступники в Интернете. ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ. Преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей. Некоторые преступники могут действовать быстрее других и сразу же заводить сексуальные беседы. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

2) Вредоносные программы. К вредоносным программам относятся вирусы, черви и «троянские кони» - это компьютерные программы, которые могут нанести вред вашему компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети.

3) Интернет-мошенничество и хищение данных с кредитной карты. В ЧЕМ СОСТОИТ МОШЕННИЧЕСТВО? Среди Интернет-мошенничеств широкое распространение получила применяемая хакерами техника «pЫshmg»,состоящая в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

4) Азартные игры. Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. В отличие от игровых сайтов, сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с

играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

5) Онлайновое пиратство. Онлайновое пиратство - это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом - например, музыки, фильмов, игр или программ - без разрешения правообладателя.

6) Интернет-дневники. Увлечение веб-журналами (или, иначе говоря, блогами) распространяется со скоростью пожара, особенно среди подростков, которые порой ведут интернет-дневники без ведома взрослых. Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

7) Интернет-хулиганство. Так же, как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Интернета. По сути, они те же дворовые хулиганы, которые получают удовольствие, хамя и грубя окружающим.

8) Недостоверная информация. Интернет предлагает колоссальное количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. Пользователи Сети должны мыслить критически, чтобы оценить точность материалов; поскольку абсолютно любой может опубликовать информацию в Интернете.

9) Материалы нежелательного содержания. К материалам нежелательного содержания относятся: материалы порнографического, ненавистнического содержания, материалы суицидальной направленности, сектантские материалы, материалы с ненормативной лексикой.

Учитель: А сейчас мы немного отдохнѐм. Музыкальная пауза. (Во время музыкальной паузы учащиеся выполняют движения)

Частушки: (Руки на пояс, поднимаем плечи по очереди, голову слегка влево, вправо). Пропоем сейчас частушки, Чтоб чуть-чуть нам отдохнуть.

Про здоровый образ жизни

Не забудем намекнуть. (На первые две строчки частушки закрывать глаза руками и открывать, на другие две - потягиваться).

На компьютере играли,

Наши глазоньки устали,

А теперь мы отдохнем

И опять играть начнем. (Руки на поясе, наклоны влево, вправо).

Нужно спортом заниматься

И в жару нам, и в мороз,

Если где-то ты не сможешь,

То не хмурь уж ты свой нос. (Хлопать в ладоши).

Мы пропели вам частушки

Хорошо ли, плохо ли,

А теперь мы вас попросим,

Чтобы вы похлопали.

Учитель:

Мы с вами уже рассмотрели те опасности, которые нам могут встретиться в Интернете. А теперь давайте посмотрим, как этих опасностей можно избежать.

Вопрос 2. «Как этих опасностей избежать?»

1) Преступники в Интернете. Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.

2) Вредоносные программы.

А) Никогда не открывайте никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда вы ожидаете получение вложения и точно знаете содержимое такого файла.

Б) Скачивайте файлы из надежных источников и обязательно читайте предупреждения об опасности, лицензионные соглашения и положения о конфиденциальности.

В) Регулярно устанавливайте на компьютере последние обновления безопасности и антивирусные средства.

3) Интернет-мошенничество и хищение данных с кредитной карты.

А)Посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес вебсайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.

Б) Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют многие банки в России.

4) Азартные игры. Помните, что нельзя играть на деньги. Ведь, в основном, подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают. Играйте в не менее увлекательные игры, те, которые не предполагают использование наличных или безналичных проигрышей/выигрышей.

5) Онлайновое пиратство. Помните! Пиратство, по сути, обычное воровство, и вы, скорее всего, вряд ли захотите стать вором. Знайте, что подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции. Официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией, чего нельзя сказать о компаниях - распространителях пиратских продуктов, которые преследуют только одну цель - обогатиться и за счет потребителя, и за счет производителя. Лицензионный пользователь программного обеспечения всегда может рассчитывать на консультационную и другую сервисную поддержку производителя, о чем пользователь пиратской копии может даже не вспоминать. Кроме того, приобретая лицензионный продукт, потребитель поддерживает развитие этого продукта, выход новых, более совершенных и удобных версий. Ведь в развитие продукта свой доход инвестирует только официальный производитель.

6) Интернет-дневники. Никогда не публикуйте в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения. Никогда не помещайте в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверяйте, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию.

7) Интернет-хулиганство. Игнорируйте таких хулиганов. Если вы не будете реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.

8) Недостоверная информация. Всегда проверяйте собранную в Сети информацию по другим источникам. Для проверки материалов обратитесь к другим сайтам или СМИ - газетам, журналам и книгам.

9) Материалы нежелательного содержания. Используйте средства фильтрации нежелательного материала (например, MSN Premium’s Parental Controls или встроенные в Internet Explorer®). Научитесь критически относиться к содержанию онлайновых материалов и не доверять им.

Учитель:

А теперь подведѐм итоги нашего классного часа. У вас на столе лежат три картинки. Выберите и положите перед собой ту, которая соответствует вашему настроению.

• Классный час понравился. Узнал что-то новое.

• Классный час понравился. Ничего нового не узнал.

• Классный час не понравился. Зря время потерял.

Учитель:

А на память об этом классном часе я хочу подарить каждому из вас памятку по безопасному поведению в Инернете. В Сети ты можешь встретить все, что угодно - от уроков истории и новостей до нелепых картинок. Но не стоит думать, что, раз информация появилась в Интернете, она является достоверной. Чтобы разобраться, какой информации в Сети можно, а какой нельзя доверять, следуй простым советам:

1. Относись к информации осторожно. То, что веб-сайт здорово сделан, еще ни о чем не говорит. Спроси себя: за что этот сайт выступает? В чем меня хотят убедить его создатели? Чего этому сайту не достает? Узнай об авторах сайта: зайди в раздел
   —О нас или нажми на похожие ссылки на странице. Узнай, кто разместил информацию. Если источник надежный, например, университет, то, вполне возможно, что информации на сайте можно доверять.

2. Следуй правилу трех источников. Проведи свое расследование и сравни три источника информации прежде чем решить, каким источникам можно доверять. Не забывай, что факты, о которых ты узнаешь в Интернете, нужно очень хорошо проверить, если ты будешь использовать их в своей домашней работе.

3. Как предоставлять достоверную информацию? Будь ответственным - и в реале, и в Сети. Простое правило: если ты не будешь делать что-то в реальной жизни, не стоит это делать в онлайне.

4. Не занимайся плагиатом. То, что материал есть в Сети, не означает, что его можно взять без спроса. Если ты хочешь использовать его - спроси разрешения.

5. Сообщая о неприемлемом контенте, ты не становишься доносчиком. Наоборот, ты помогаешь делу безопасности Сети.

6. Когда ты грубишь в Интернете, ты провоцируешь других на такое же поведение. Попробуй оставаться вежливым или просто промолчать. Тебе станет приятнее.

7. Все, что ты размещаешь в Интернете, навсегда останется с тобой - как татуировка. Только ты не сможешь эту информацию удалить или контролировать ее использование. Ты ведь не хочешь оправдываться за свои фотографии перед будущим работодателем?

8. Защищай себя - сейчас и в будущем. Подумай, прежде чем что-либо разместить в Интернете.

И помните, Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но — как и реальный мир - Сеть тоже может быть опасна!

Методические материалы для разработки классного часа «Что нужно знать старшекласснику об Интернете?»

Юридические аспекты и общие свойства:

- У Интернета нет собственника, так как он является совокупностью сетей, которые имеют различную географическую принадлежность.

- Интернет нельзя выключить целиком, поскольку маршрутизаторы сетей не имеют единого внешнего управления.

- Интернет стал достоянием всего человечества.

- У Интернета имеется много полезных и вредных свойств, эксплуатируемых заинтересованными лицами.

- Интернет, прежде всего, средство открытого хранения и распространения информации. По маршруту транспортировки незашифрованная информация может быть перехвачена и прочитана.

- Интернет может связать каждый компьютер с любым другим, подключѐнным к Сети, так же, как и телефонная сеть. Если телефон имеет автоответчик, он способен распространять информацию, записанную в него, любому позвонившему.

- Сайты в Интернете распространяют информацию по такому же принципу, то есть индивидуально, по инициативе читателя.

- Спам-серверы и «зомби-сети» распространяют информацию по инициативе отправителя и забивают почтовые ящики пользователей электронной почты спамом точно так же, как забивают реальные почтовые ящики распространители рекламных листовок и брошюр.

- Распространение информации в Интернете имеет такую же природу, как и слухи в социальной среде. Если к информации есть большой интерес, она распространяется широко и быстро, нет интереса — нет распространения.

- Чтение информации, полученной из Интернета или любой другой сети ЭВМ, относится, как правило, к непубличному воспроизведению произведения. За распространение информации в Интернете (разглашение), если это государственная или иная тайна, клевета, другие запрещѐнные законом к распространению сведения,

вполне возможна юридическая ответственность по законам того места, откуда информация введена.

Сервисы

В настоящее время в Интернет существует достаточно большое количество сервисов, обеспечивающих работу со всем спектром ресурсов. Наиболее известными среди них являются: электронная почта (E-mail), обеспечивающая возможность обмена сообщениями одного человека с одним или несколькими абонентами; телеконференции, или группы новостей (Usenet), обеспечивающие возможность коллективного обмена сообщениями; сервис FTP — система файловых архивов, обеспечивающая хранение и пересылку файлов различных типов; сервис Telnet, предназначенный для управления удаленными компьютерами в терминальном режиме; World Wide Web (WWW, W3) — гипертекстовая (гипермедиа) система, предназначенная для интеграции различных сетевых ресурсов в единое информационное пространство; сервис DNS, или система доменных имен, обеспечивающий возможность использования для адресации узлов сети мнемонических имен вместо числовых адресов; сервис IRC, предназначенный для поддержки текстового общения в реальном времени (chat); Перечисленные выше сервисы относятся к стандартным. Это означает, что принципы построения клиентского и серверного программного обеспечения, а также протоколы взаимодействия сформулированы в виде международных стандартов. Следовательно, разработчики программного обеспечения при практической реализации обязаны выдерживать общие технические требования. Наряду со стандартными сервисами существуют и нестандартные, представляющие собой оригинальную разработку той или иной компании. В качестве примера можно привести различные системы типа Instant Messenger (своеобразные Интернет-пейджеры — ICQ, AOl, Demos on-line и т. п.), системы Интернет-телефонии, трансляции радио и видео и т. д. Важной особенностью таких систем является отсутствие международных стандартов, что может привести к возникновению технических конфликтов с другими подобными сервисами. Для стандартных сервисов также стандартизируется и интерфейс взаимодействия с протоколами транспортного уровня. В частности, за каждым программным сервером резервируются стандартные номера TCP- и UDP-портов, которые остаются неизменными независимо от особенностей той или иной фирменной реализации как компонентов сервиса, так и транспортных протоколов. Номера портов клиентского программного обеспечения так жестко не регламентируются. Это объясняется следующими факторами: во-первых, на пользовательском узле может функционировать несколько копий клиентской программы, и каждая из них должна однозначно идентифицироваться транспортным протоколом, то есть за каждой копией должен быть закреплен свой уникальный номер порта; во-вторых, клиенту важна регламентация портов сервера, чтобы знать, куда направлять запрос, а сервер сможет ответить клиенту, узнав адрес из поступившего запроса.

Услуги

Сейчас наиболее популярные услуги Интернета — это: Всемирная паутина Веб-форумы Блоги Вики-проекты Интернет-магазин ы Интернет-аукцион ы Социальные сети Электронная почта и списки рассылки Группы новостей (в основном, Usenet) Файлообменные сети Электронные платёжные системы Интернет-радио Интернет-телевидение IP-телефония Мессенджеры FTP-серверы IRC (реализовано также как веб-чаты) Поисковые системы Интернет-реклама Удалённые терминалы Удалённое управление Многопользовательские игры Web 2.0

Интернет-зависимость

С возрастанием популярности Интернета проявились и негативные аспекты его применения. В частности, некоторые люди настолько увлекаются виртуальным пространством, что начинают предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Психологическую в своей основе интернет-зависимость сравнивают с наркоманией — физиологической зависимостью от наркотических веществ, где также присутствует психический компонент. Интернет-зависимость определяется как навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всѐм мире. Российские психиатры считают, что сейчас в стране таковых 4—6 %. Интернет-зависимость — психическое расстройство, навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. Интернет-зависимость является широко обсуждаемым вопросом, но еѐ статус пока находится на неофициальном уровне: расстройство не включено в официальную классификацию заболеваний DSM-IV. Происхождение проблемы Информация для человека имеет огромное значение. Компьютер и Интернет являются мощным инструментом обработки и обмена информацией, кроме того, благодаря компьютеру стали доступными различные виды информации. Это и считается первопричиной компьютерной или интернет зависимости, так как в определѐнном смысле, они страдают нарушением процессов обмена информацией. Проблема интернет-зависимости выявилась с возрастанием популярности сети Интернет. Некоторые люди стали настолько увлекаться виртуальным пространством, что начали предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Резкий отказ от Интернета вызывает у таких людей тревогу и эмоциональное возбуждение. Психиатры усматривают схожесть такой зависимости с чрезмерным увлечением азартными играми. Интернет-зависимость и официальная медицина Официально медицина пока не признала интернет-зависимость психическим расстройством, и многие эксперты в области психиатрии вообще сомневаются в существовании интернет-зависимости или отрицают вред от этого явления.

Зависимость (наркотическая) в медицинском смысле определяется как навязчивая потребность в использовании привычного вещества, сопровождающаяся ростом толерантности и выраженными физиологическими и психологическими симптомами. Рост толерантности означает привыкание ко всѐ большим и большим дозам [1]. Также зависимость (аддикция) в психологии определяется как навязчивая потребность, ощущаемая человеком, подвигающая к определѐнной деятельности. Этот термин употребляется не только для определения наркомании, но и применяется к другим областям, типа проблемы азартных игр, обжорства или гиперрелигиозности. Очевидно, его можно употреблять и при рассмотрении интернет-зависимости. Здесь характер зависимости иной, чем при употреблении наркотиков или алкоголя, то есть физиологический компонент полностью отсутствует. А вот психологический проявляется очень ярко. Таким образом, можно определить интернетзависимость как нехимическую зависимость — навязчивую потребность в использовании Интернета, сопровождающуюся социальной дезадаптацией и выраженными психологическими симптомами. Интернет-зависим ые По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всѐм мире. Российские психиатры считают, что сейчас в нашей стране таковых 4—6%. Несмотря на отсутствие официального признания проблемы, интернетзависимость уже принимается в расчѐт во многих странах мира. Например, в Финляндии молодым людям с интернет-зависимостью предоставляют отсрочку от армии.

Классификация интернет-зависимости, её причин и симптомов

Основные 5 типов интернет-зависимости таковы:

1. Навязчивый веб-серфинг — бесконечные путешествия по Всемирной паутине, поиск информации.

2. Пристрастие к виртуальному общению и виртуальным знакомствам — большие объѐмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.

3. Игровая зависимость — навязчивое увлечение компьютерными играми по сети.

4. Навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернетаукционах.

5. Киберсексуальная зависимость — навязчивое влечение к посещению порносайтов и занятию киберсексом[3].

Интернет-зависимость и проблемы в семье Проблемы в семье, как правило, возникают в результате недостатка внимания к тому или иному члену семьи. Ссоры и непонимание проблем зависимого человека только усугубляют положение отношений в семье. Так как интернет-зависимый человек поглощает много информации и, возможно, знаний, подобные изменения вызывают внутреннюю напряжѐнность и

обеспокоенность. Семейные скандалы могут лишь еще больше повредить психику человека. Лучший способ решить проблемы семьи — это и любовь, и взаимопонимание, и мудрость домочадцев. Плавно выводить человека на семейное позитивное общение и, главное, увеличивать совместное общение с живой природой, к примеру: с помощью прогулок. Пути решения проблемы Самый простой и доступный способ решения зависимости — это приобретение другой зависимости. Любовь к здоровому образу жизни, общение с живой природой, творческие прикладные увлечения, такие, как рисование, как правило, выводят человека из зависимости.

Ведущим специалистом в изучении интернет-зависимости сейчас считается Кимберли Янг — профессор психологии Питсбургского университета в Брэтфорде (США), автор известной книги «Пойманные в Сеть» (англ. «Caught in the Net»), переведѐнной на многие языки. Она также является основателем Центра помощи людям, страдающим интернет-зависимостью (англ. Center for On-Line Addiction). Центр, созданный в 1995 году, консультирует психиатрические клиники, образовательные заведения и корпорации, которые сталкиваются со злоупотреблением интернетом. Центр свободно распространяет информацию и методики по освобождению от интернет-зависимости. В 2009 году писатель Станислав Миронов опубликовал в свободном доступе на одном из литературных ресурсов роман Virtuality, рассказывающий о проблеме интернетзависимости, где автор классифицирует интернет-зависимость не только как психическое расстройство, но и как острую социальную проблему, предлагая пути еѐ решения. О печатном издании романа упоминаний не имеется.

Методическая разработка классного часа на тему: «Этика сетевого общения» (8 - 9 класс).

Цель мероприятия: - познакомить ребят с основными нормами поведения в сети Интернет, особенностями общения в чатах, по электронной почте.

Лучше построить классный час в форме беседы, в которой учащиеся должны привести примеры непорядочного поведения в сети Интернет: нетерпимости, навязывания своих убеждений, экстремизма. В качестве вступительного слова ребятам можно предложить ситуации, часто встречающиеся в последнее время при пользовании сетью Интернет, и выяснить мнение ребят по той или иной проблеме (ситуации).

Например:

1. В последнее время чешские школьники, как и учащиеся в других странах, частенько шантажируют одноклассников и учителей, выкладывая нелицеприятные видеоролики о них в Интернете. Для рассылки фотографий, звуковых и видеофайлов дети также пользуются электронной почтой и мобильными телефонами. Чтобы решить эту проблему, чиновники предлагают учителям просто конфисковывать у детей сотовые аппараты или же запрещать их использование во время уроков. Кроме того,

преподавателям рекомендуется приглашать родителей в школу и обсуждать с ними поведение малолетних шантажистов; есть и более радикальная мера — перевод провинившегося в другой класс. Ну, а, если школьник упорствует, продолжая выкладывать фотографии и видео, чиновники советуют педагогам обращаться в полицию. - Как вы оцениваете такое поведение своих сверстников в других странах? - Какие методы воздействия на Интернет-шантажистов можете предложить? 2.Онлайновое запугивание — к сожалению, довольно распространенное сегодня явление. Согласно недавнему исследованию, в США трое из четырех подростков подвергались запугиванию в Сети в течение последнего года. И только один ребенок из десяти рассказал об онлайновых угрозах родителям или другим взрослым. Многие подростки не говорят о происшедшем родителям, поскольку намерены сами решать подобные проблемы. 31% опрошенных не обсуждают инциденты, так как боятся, что родители ограничат им доступ в Интернет. Треть респондентов заявили, что не говорили со взрослыми об онлайновых угрозах, поскольку опасались, что в результате у них могут возникнуть проблемы с родителями. - Подвергались ли вы подобному воздействию? - Как нужно правильно вести себя в подобной ситуации, по вашему мнению?

3. В связи с развитием электронного государства, идея электронного школьного журнала становится все более популярной. Подобные журналы успеваемости востребованы в Америке (программа Pinnacle Gradebook) и набирают обороты в России. На заседании президиума Госсовета УР летом текущего года, на котором рассматривался вопрос о реализации Стратегии развития информационного общества в РФ, президент России Дмитрий Медведев одобрил ввод электронных версий школьных журналов наряду с бумажными. Многие родители с энтузиазмом восприняли эту идею. В правительстве Калининградской области активно обсуждается вопрос о введении электронных карточек для контроля за школьниками. Об этом министр образования правительства Калининградской области Наталья Шерри сообщила на состоявшейся 22 августа пресс-конференции на тему: "Реализация в Калининградской области проекта по совершенствованию организации школьного питания". По словам министра, данное нововведение позволит обеспечить контроль как школьной администрации, так и родителей за посещением занятий, приѐмом пищи и получением материалов в библиотеке их детьми. Также разрабатываются варианты ведения электронного журнала, причѐм в некоторых школах такие журналы уже используются.

- Выскажите свое отношение к таким формам контроля за детьми со стороны родителей и учителей. Хотя Интернет - специфическая среда для общения, в ней существуют определенные правила вежливости, которые получили название «сетевой этикет». Правила сетевого этикета широко обсуждаются в Интернете, но, к сожалению, культура общения остается на низком уровне. В сети нередко можно наблюдать грубость, речевую агрессию, нетерпимость к чужим мнениям. В связи с этим, необходимо рассмотреть пример крайне негативного сетевого поведения,

предложить дать ему нравственную оценку и указать на недопустимость такого поведения. Например, сообщение в новостях: «Группа хакеров повредила на этой неделе несколько церковных страниц, поместив на них высказывания почитателей культа Сатаны, его изображения и другие символы Сатанизма». Предложить учащимся дать им оценку. Работая в Интернете, учащиеся обязательно должны столкнуться с проблемой виртуального общения (чат, форум, электронная почта, телеконференции). Если мы общаемся с незнакомыми людьми, то возникает ситуация разговора с виртуальными личностями. Человек может изменять свой статус, скрывать возраст, пол, преувеличивать силу, красоту, а также почти безнаказанно проявлять агрессивные черты характера, которые он вынужден подавлять в повседневной жизни. Для того ***чтобы избежать отрицательных последствий общения в Интернете***, следует придерживаться определенных правил:

- не нужно слепо верить в то, что собеседник говорит о себе;

- следите за своими словами (не употребляйте грубых выражений);

- не сообщайте незнакомому лично человеку ваш домашний адрес, телефонный номер;

- если вы чувствуете дискомфорт в общении, уходите.

Можно предложить учащимся составить свои принципы общения в Интернете. Рассмотрим подробнее неформальный кодекс поведения в сети Интернет, регулирующий общение пользователей друг с другом и так называемый сетевой этикет (netiquette — от слияния англ. слов net — сеть и etiquette — этикет). Сетевой этикет — это некоторое количество базовых правил поведения в сети, однако эти правила время от времени подвергаются изменениям, что-то устаревает и теряет свою актуальность в связи с развитием технологий Интернет, а что-то добавляется новое. Сетевой этикет регулирует: - правила обмена сообщениями по электронной почте - стилистику сетевой коммуникации при коллективных обсуждениях - общие правила написания публикуемых текстов в сети и пр.

При переписке по электронной почте каждый пользователь должен помнить о некоторых правилах.

- Приветствуйте собеседника в начале письма и прощайтесь в конце.

- По электронной почте можно обращаться к незнакомым людям, но при условии, что адрес был опубликован его владельцем.

- Пишите кратко, грамотно и аккуратно.

- Отвечая на сообщение, необходимо цитировать его наиболее существенные места.

- Удобно, когда письма пользователя заканчиваются краткой «подписью», автоматически добавляемой к каждому сообщению, отправляемому пользователем,

однако эта подпись не должна быть длиннее четырех-пяти строк. Очень важно указать в подписи своѐ имя-отчество полностью, чтобы получателю было удобно обратиться к Вам. Если указаны только инициалы, то отвечающему придѐтся искать имена в других источниках, на это потребуется время. Подразумевать же, что все точно помнят наше имя-отчество, - это неверно. У всех свои особенности памяти и объѐмы информации, а также круг общения. Например: С уважением, Светлана Григорьевна Тел. 8(XXX) XX-XX-XXX E-mail: aaa@mail.ru - В переписке личного характера можно придерживаться разговорного стиля.

- Не следует переправлять чье-то личное сообщение другим людям или в телеконференцию без предварительного согласия его автора.

- Если вы заняты и не можете быстро ответить на поступившее сообщение, отправьте пару строк с подтверждением получения и обещанием ответить при первой возможности.

- Если сообщение поступило от незнакомого лица, следует понять, обосновано оно или нет. В первом случае - ответить в течение трех дней. Во втором - не отвечать.

- Текст письма нужно структурировать по смыслу, абзацы отделять пустой строкой.

- Если вы отправляете заархивированный файл, поинтересуйтесь заранее, сможет ли получатель письма его распаковать (то есть, имеет ли он на своем компьютере нужную программу-архиватор).

- Строка текста должна ограничиваться 60-70 символами, справа без выравнивания.

- Нежелательно посылать письма большого объема - около одного мегабайта, поскольку пользователь, работающий с бесплатным почтовым ящиком, может такое послание не прочитать из-за ограничений на объем входящей корреспонденции.

- К незнакомым людям можно обращаться с просьбами о консультации, с вежливыми предложениями и пожеланиями, не претендуя на получение ответа.

- Неполучение ответа следует рассматривать как нежелательность или невозможность установления контакта и повторять не следует.

- При обращении к незнакомым людям следует воздерживаться от просьб, вызывающих необходимость использования других средств связи, отличных от электронной почты.

- Если в письмо вложен файл, то в тексте письма обязательно должно был указано, что приложено и зачем.

И наконец, существуют ***общие Правила общения в Сети*** :

1. Помните, что Вы говорите с человеком.

2. Придерживайтесь тех же стандартов поведения, что и в реальной жизни.

3. Помните, где Вы находитесь в киберпространстве.

4. Уважайте время и возможности других.

5. Сохраняйте лицо.

6. Помогайте другим там, где Вы это можете делать.

7. Не ввязывайтесь в конфликты и не допускайте их.

8. Уважайте право на частную переписку.

9. Не злоупотребляйте своими возможностями.

10. Учитесь прощать другим их ошибки.

Приложение 4

ПАМЯТКА РОДИТЕЛЯМ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ДЕТЕЙ В ИНТЕРНЕТЕ

Интернет может быть прекрасным местом как для обучения, так и для отдыха и общения с друзьями. Но, как и весь реальный мир, Сеть тоже может быть опасна. Перед тем как разрешить детям выходить в Интернет самостоятельно, им следует уяснить некоторые моменты. Расскажите своим детям об опасностях, существующих в Интернете, и научите правильно выходить из неприятных ситуаций. В заключение беседы установите определенные ограничения на использование Интернета и обсудите их с детьми. Сообща вы сможете создать для ребят уют и безопасность в Интернете. Если вы не уверены, с чего начать, вот несколько мыслей о том, как сделать посещение Интернета для детей полностью безопасным.

- Установите правила работы в Интернете для детей и будьте непреклонны.

- Научите детей предпринимать следующие меры предосторожности по сохранению конфиденциальности личной информации:

- Представляясь, следует использовать только имя или псевдоним.

- Никогда нельзя сообщать номер телефона или адрес проживания или учебы.

- Никогда не посылать свои фотографии.

- Никогда не разрешайте детям встречаться со знакомыми по Интернету без контроля со стороны взрослых.

- Объясните детям, что разница между правильным и неправильным одинакова как в Интернете, так и в реальной жизни.

- Научите детей доверять интуиции. Если их в Интернете что-либо беспокоит, им следует сообщить об этом вам.

Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, помогите ребенку его выбрать и убедитесь, что оно не содержит никакой личной информации. Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире. Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование чужой работы - музыки, компьютерных игр и других программ - является кражей. Скажите детям, что им никогда не следует встречаться с друзьями из Интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают. Скажите детям, что не все, что они читают или видят в Интернете, - правда. Приучите их спрашивать вас, если они не уверены.

Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он делает на них. Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми. Регулярно посещайте Интернет-дневник своего ребенка, если он его ведет, для проверки. Будьте внимательны к вашим детям!

Приложение 5

ПАМЯТКА ДЛЯ ДЕТЕЙ ПО БЕЗОПАСНОМУ ПОВЕДЕНИЮ В ИНТЕРНЕТЕ

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, ребенок должен предпринимать следующие меры предосторожности при работе в Интернете:

> Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга

. > Используйте нейтральное экранное имя, не содержащее сексуальных намеков и не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.

> Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.

> Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.

> Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.

> Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.

> Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Расскажите об этом родителям.