Принято

на педагогическом совете

МБОУ «Золотковская СОШ»

Протокол № 2 от 28.12.2021года

Утверждаю

Директор школы:_____

Е.В.Сироткина

Приказ №16 от 01.02.2022г.

Программа
обучения учащихся правилам безопасного поведения в сети Интернет, профилактики Интернет-зависимости

Срок реализации программы 2022-2024 год

Составитель: Бондарь О.А., учитель информатики

2022 год

Пояснительная записка

Проблема обеспечения информационной безопасности детей 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.

Между тем существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для детей 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 Российской Федерации по правам ребенка).

Медиаграмотность определяется в международном праве как грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг.

Обеспечение государством информационной безопасности детей, защита их физического, умственного и нравственного развития во всех аудиовизуальных медиа-услугах и электронных СМИ – требование международного права (Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 о защите несовершеннолетних и человеческого достоинства в Интернете, Решение Европейского парламента и Совета № 276/1999/ЕС о принятии долгосрочной плана действий Сообщества по содействию безопасному использованию Интернета посредством борьбы с незаконным и вредоносного содержимого в рамках глобальных сетей).

Согласно российскому законодательству ***информационная безопасность детей*** – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"). Преодолеть нежелательное воздействие компьютера возможно только совместными усилиями учителей, родителей и самих детей.

Данная программа рассчитана на период с 2018 по 2021 год.

Работа с обучающимися должна вестись в зависимости от возрастных особенностей: начальное звено (2-4 класс), среднее (5-9 класс) и старшее (10-11 класс). На каждом этапе необходимы специальные формы и методы обучения в соответствии с возрастными особенностями.

Для организации безопасного доступа к сети Интернет в школе созданы следующие условия:

1.В школе разработаны и утверждены:

- Правила доступа к сети Интернет для обучающихся и сотрудников (Приложение 1)
- Правила использования сети Интернет (Приложение 2)
- Должностная инструкция ответственного за использование сети Интернет (Приложение 3)
- Регламент по работе учителей и школьников в сети Интернет (Приложение 4)
- Инструкция пользователя по безопасной работе в сети Интернет (Приложение 5)
- Классификаторы информации, доступ к которой учащихся запрещен и разрешен (Приложение 6)

2. Контроль использования учащимися сети Интернет осуществляется с помощью программно-технических средств и визуального контроля.

3. Ведется журнал учета работы в Интернет.

Нормативно-правовая база

- Программа разработана с учетом требований законов РФ:
- «Об образовании в Российской Федерации», Закон РФ от 29.12.2012 N 273-ФЗ);
- Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10.

Цели, задачи, основные мероприятия реализации программы

Цель: обеспечения информационной безопасности детей и подростков при обучении, организации внеурочной деятельности и свободном использовании современных информационно-коммуникационных технологий (в частности сети Интернет)

Задачи:

- формирование и расширение компетентностей работников образования в области медиабезопасного поведения детей и подростков;
- формирования информационной культуры как фактора обеспечения информационной безопасности;
- изучение с нормативно-правовых документов по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию;
- формирование знаний в области безопасности детей использующих Интернет;
- организации просветительской работы с родителями и общественностью.
-

Перечень мероприятий

по обучению школьников безопасному использованию сети Интернет

№ п/п	Мероприятия	Сроки проведения	Ответственные
1	Внеурочные мероприятия по безопасности работы в Интернете 2-4 классы, 5-6 классы Уроки безопасности работы в Интернет для учащихся 7–9, 10– 11 классов.	сентябрь-октябрь	Классные руководители 2-4 классы, учитель информатики Бондарь О.А 5-11 классы
2	Выступление на родительском собрании на тему: «Быть или не быть Интернету в компьютере вашего ребенка?» Анкетирование «Знают ли родители, с кем общается их ребенок в сети?»	октябрь—апрель	Педагог-психолог Рыжова Ю.А., учитель информатики Бондарь О.А
3	Изучение нормативных документов по организации безопасного доступа к сети Интернет	сентябрь	Руководитель ШИОУ Ефремова А.В., учитель информатики Бондарь О.А
4	На уроках информатики провести беседы, диспуты: «Безопасность при работе в Интернете», «О личной безопасности в Интернет», «Сетевой этикет», «Этика сетевого общения » (7-8 классы), «Форумы и чаты в Интернет», «Информационная безопасность сетевой технологии работы» (9-11 классы).	сентябрь-май	Учитель информатики Бондарь О.А
5	Классные часы в 2- 11 классах. Цель: ознакомление учащихся с опасностями, которые подстерегают их в Интернете. «Сказка о золотых правилах безопасности в сети Интернет» (2 кл.) «Чем опасен интернет» (3-4 кл.); «Безопасность в сети Интернет» (5-6 кл.); «Компьютерные сети» (5-8 кл.);	ноябрь-март	Классные руководители 5-11 классов, учитель информатики Бондарь О.А

	«Темная сторона Интернета» (7-8 кл.), «Опасности в Интернете», «Остерегайся мошенничества в Интернете» (9-11 кл.).		
6	Круглый стол «Основы безопасности в сети Интернет»	декабрь	Учитель информатики Бондарь О.А , зам.директора по УР Завьялова Л.Г.
7	Организация и проведение конкурса детских работ «Мой безопасный Интернет» с номинациями: Рисунок (2-4 классы), Плакат (5-7 классы), Рассказ о позитивном контенте («Мои любимые сайты», «Любимые сайты нашей семьи»)	февраль	Классные руководители 1-4 классов, учитель информатики Бондарь О.А, зам.директора по УР Завьялова Л.Г.

Исполнители:

- Школьное исследовательское объединение учащихся
- Классные руководители 1-11 классов.
- Учитель информатики.
- Педагог-психолог
- Зам. директора по УР

Результатами выполнения программы являются:

Цели и задачи программы	Перечень непосредственных и конечных показателей	Фактическое значение на момент разработки программы	Значение показателей по периодам реализации программы			Плановое значение на день окончания действия программы 2023-2024
			2021-2022	2022-2023	2023-2024	
Цель: Обеспечения информационной безопасности обучающихся при обучении, организации внеурочнойной деятельности и свободном использовании современных информационно-коммуникационных технологий в том числе сети Интернет.						
Задача №1. Формирование и расширение компетентностей работников образования в области медиа-безопасного поведения детей и подростков	Доля педагогов, использующих современные коммуникационные взаимодействия.	70%	80%	90%	100%	100%
	Умение использовать и интегрировать разнотипную информацию.	70%	80%	90%	100%	100%
Задача № 2. Формирования информационной культуры как фактора обеспечения информационной	Доля педагогов использующих сетевые технологии, современные средства связи и прикладные программы в области профессиональной	60%	70%	80%	85%	90%

безопасности	деятельности.					
Задача № 3. Изучение нормативно-правовых документов по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию	Владение правовыми знаниями в области информатизации.	60%	75%	90%	100%	100%
Задача № 4. Формирование знаний в области безопасности обучающихся, использующих Интернет	Владение знаниями о защите компьютера от вредоносных программ, о нелегальном, пиратском контенте и об опасности его скачивания.	70%	80%	88%	94%	97%
Задача № 5. Организации просветительской работы с родителями и общественностью.	Включение родителей в совместную со школой деятельность по обеспечению безопасности детей в Интернет пространстве.	50%	60%	65%	68%	70%

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. Интернет должен быть максимально безопасным для подрастающих поколений. Эта цель осуществима, если родители осознают свое главенство в обеспечении безопасности детей. В данных методических рекомендациях представлены материалы для разработки уроков, классных часов, направленные на обеспечение необходимыми знаниями в области психолого-педагогического и здоровье-сберегающего сопровождения образовательного процесса школьников, использующих персональные компьютеры и Интернет в профессиональной, учебной и внеучебной деятельности, родительских собраний. Методические рекомендации содержат советы, 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.

Анкетирование учащихся.

Для изучения безопасности в сети Интернет и отношения к ней подростков разрабатываются анкеты, позволяющие проанализировать современную ситуацию в образовательной среде.

Анкетирование предполагается проводить в форме анонимного опроса как на бумажных носителях, так и в электронном виде. Примерные формы анкет представлены в Приложении 1.

Проведение круглого стола
«Основы безопасности в сети Интернет»

Цель: формирование устойчивых жизненных навыков при работе в сети Интернет. Работе круглого стола предшествует предварительная подготовка учащихся по предложенной тематике. Перечень вопросов для обсуждения выявляется в результате анкетирования учащихся.

Примерные вопросы для обсуждения:

1. Для чего нужен Интернет?

2. Какие существуют риски при пользовании интернетом, и как их можно снизить?

3. Какие виды мошенничества существуют в сети Интернет?

4. Как защититься от мошенничества в сети Интернет?

5. Что такое безопасный чат?

6.Виртуальный собеседник предлагает встретиться, как следует поступить?

7. Как вы можете обезопасить себя при пользовании службами мгновенных сообщений.

При подведении итогов круглого стола обучающимся можно предложить правила поведения в сети Интернет (Приложение 3).

Проведение компьютерной игры для младших школьников

В рамках классного часа или урока информатики (окружающего мира) обучающимся 2-4 классов целесообразно предложить компьютерную игру о правилах поведения в сети Интернет Прогулка через ИнтерНетЛес (*http://www.wildwebwoods.org/popup.php?lang=ru*), где в игровой форме показано какие опасности могут встречаться при работе в сети Интернет, рассказано о сетевом взаимодействии и об этикете, а также о защите прав детей.

Конкурс буклетов "Правила поведения в сети Интернет"

Целью данного конкурса является формирование у учащихся четкого представления о правилах поведения в сети Интернет.

Данный конкурс проходит в два этапа: заочный и очный. За 14 дней предлагается определенная тематика конкурсных заданий, разрабатывается критериальный аппарат, даются методические рекомендации по составлению буклета.

Заочный этап предполагает анализ и отбор 20 лучших работ, отобранных экспертной комиссией, в состав которой входят как педагоги, так и учащихся.

Очный этап конкурса предполагает публичную защиту буклета и

ответы на вопросы одноклассников. По результатам данного этапа определяется победитель.

Проведение тематического классного часа

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

1) информирование учащихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

2) информирование учащихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);

3) обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

4) профилактика формирования у учащихся интернет-зависимости и игровой зависимости (игромании, гэмблинга);

5) предупреждение совершения учащимися правонарушений с использованием информационно-телекоммуникационных технологий.

Ожидаемые результаты:

В ходе проведения классного часа дети должны научиться делать более безопасным и полезным свое общение в Интернете и иных информационно- телекоммуникационных сетях, а именно:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;
- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
- распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;
- критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;
- анализировать степень достоверности информации и подлинность ее источников;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

При организации классного часа важно исходить из возрастных особенностей учащихся, учесть уровень их знакомства с Интернетом.

Организовать проведение классного часа необходимо таким образом, чтобы несовершеннолетние не только получили необходимый минимум знаний об информационной безопасности, но смогли *высказать свою точку зрения на указанную проблему.*

При определении **содержания, форм и методики** проведения единого классного часа важно учитывать:

- необходимость деятельностного подхода в учебной работе учащихся в активном и интерактивном режиме;
- целесообразность использования методик учебного сотрудничества, различных вариантов работы в группах, кооперации, моделирования жизненных ситуаций.

Образовательные технологии

№ п/п	Виды учебной работы	Образовательные технологии
1.		*Проблемное обучение, визуализация*
2.	Практические занятия	*Деловая игра, разбор конкретных ситуаций, практическая работа, технология развития критического мышления, технология Дебаты, авторская мастерская*
3.	Реферат, проектирование	*Проектная деятельность, исследовательская работа.*

При определении тематика бесед для единого классного часа «Безопасный Интернет» необходимо исходить:

- из понимания важности и значимости для каждого человека основ медиакультуры;
- из возможности в доступных игровых ситуациях знакомить обучающихся с основами медиакультуры;
- из необходимости приобретения обучающимися первичного опыта регулирования медиаотношений;
- из необходимости получения обучающимися знаний и навыков использования конкретных правил и норм медиаобразования и первичного опыта разработки собственных правил медиакультуры.

Темы бесед с 2 по 11 класс могут быть следующие:

- Я и мои виртуальные друзья.
- Интернет в моей семье.
- Мой Интернет.
- Интернет и природа.
- Мой социум в Интернете.
- Интернет и моя будущая профессия.

- Интернет в современной школе.

- Интернет и мое здоровье и т.д.

Освоение медиабезопасности наиболее эффективно в совместной деятельности со взрослыми. Поэтому желательно привлечь родителей, представителей органов исполнительной власти, правоохранительных, органов, общественных организаций.

При проведении уроков в начальной школе рекомендуется использовать материалы, размещенные:

- на сайте интерактивного курса по Интерент-безопасности (*http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu*. htm) в разделе Для учащихся рассказы для детей 7-10 лет, а также в разделе Тесты (можно организовать on-line тестирование школьников 7-10 лет);
- на сайте (*http://www.onlandia.jrg.ua/ru-RU/*) On-ляндия. Безопасная веб-страна в разделе Для детей 7-10 лет рассказы в картинках, задания и вопросы;

- на сайте (*http://content-filtering.ru/aboutus/*) Информационно- аналитический ресурс Ваш личный Интернет в разделе Юным пользователям - Дошкольники и младшие классы подсказки и советы по безопасному поведению в сети Интернет;
- на сайте (*http://stopfraud.megafon.ru/*) федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах Виды мошенничества и Наши рекомендации , а также советы родителям;
- на портале Безопасный интернет (*http://www.saferinternet.ru/*) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме Безопасный интернет .
- в качестве видео заставки для классного часа или урока можно использовать *http://youtu.be/789j0eDglZQ*мультфильм Безопасный интернет , который разработала студия Mozga.ru.
- на сайте Началка.ком материалы по безопасному интернету (*http://www.nachalka.com/taxonomy/term/335*).

При проведении уроков в 5-9 классах рекомендуется использовать материалы, размещенные:

- на сайте интерактивного курса по Интерент-безопасности (*http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/et...*. htm) в разделе Для учащихся рассказы для детей 11-16 лет, а также в разделе Тесты (можно организовать on-line тестирование школьников 11- 14 лет);
- на сайте (*http://www.onlandia.org.ua/ru-RU/*) On-ляндия. Безопасная веб-страна в разделе Для детей 11-14 лет рассказы в картинках, задания и вопросы; в разделе Для учителей опасности в сети и поведение в сети;
- на сайте (*http://content-filtering.ru/aboutus/*) Информационно- аналитический ресурс Ваш личный Интернет в разделе Юным пользователям - Средние классы подсказки и советы по безопасному поведению в сети Интернет, а также при использовании онлайн-игр и мобильного телефона;
- на сайте *http://stopfraud.megafon.ru/* федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах Виды мошенничества и Наши рекомендации , а также советы родителям;
- на портале Безопасный интернет (*http://www.saferinternet.ru/*) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме Безопасный интернет.

При проведении уроков в 10-11 классах рекомендуется использовать материалы, размещенные:

- на на сайте интерактивного курса по Интерент-безопасности (*http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/et...*. htm) в разделе Для учащихся рассказы для детей 11-16 лет, а также в разделе Тесты (можно организовать on-line тестирование школьников 11-14 лет);
- на сайте (*http://www.onlandia.org.ua/ru-RU/*) On-ляндия. Безопасная веб-страна в разделе Для подростков советы по безопасному общению и работе в режиме on-line; в разделе Для учителей опасности в сети и поведение в сети;
- на сайте (*http://content-filtering.ru/aboutus/*) Информационно- аналитический ресурс Ваш личный Интернет в разделе Юным пользователям - Старшие классы подсказки и советы по безопасному поведению в сети Интернет, а также при использовании онлайн-игр и мобильного телефона;
- на сайте *http://stopfraud.megafon.ru/* федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах Виды мошенничества и Наши рекомендации, а также советы родителям;
- на портале Безопасный интернет (*http://www.saferinternet.ru/*) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме Безопасный интернет.

Дополнительные Интернет-ресурсы для проведения классного часа:

- Справочник по детской безопасности в Интернет от Google (*http://www.google.ru/familysafety/*);
- Сайт советов по работе на компьютере (*http://shperk.ru/sovety/kak-sdelat-internet-dlya-detej-bolee bezopasnym.html*);
- Сайт Компьютерная безопасность. Безопасность жизни (*http://blog.chljahsoft.net/3167*);
- Сайт Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт (*http://i-deti.org/*);
- Буклет Безопасный интернет детям Министерства внутренних дел РФ (*http://www.mvd.ru/userfiles/liflets_k_deti_06.pdf*);
- Материалы III ежегодного Форума Безопасного Интернета (*http://safor.ru/prezentacii11.php*);
- Сайт Дети России Онлайн (*http://detionline.com/*).

Проведение родительских собраний

Родительские собрания целесообразно проводить по ступеням возрастного развития учащихся (начальная ступень образования, основная ступень образования, старшая ступень образования).

В начале родительского собрания рекомендуется провести анонимное анкетирование, которое позволит выявить отношение родительской общественности к внедрению в образовательный процесс ИКТ. По результатам анкетирования будет определена дальнейшая стратегия работы ОУ по безопасности детей в сети Интернет. Примерный перечень вопросов анкетирования в Приложении 2, Приложение 3.

После анкетирования проводится беседа по проблеме доступа ребенка к сети Интернет, в которой поднимаются наиболее актуальные вопросы.

Далее даются рекомендации родителям по работе детей в сети Интернет (с учетом возрастных особенностей) (Приложение 4).

В конце родительского собрания всем родителям предлагается памятка по безопасности детей в сети Интернет при помощи программных средств.

Урок «Интернет-безопасность»

(на всех уровнях обучения)

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

1) информирование обучающихся о видах информации, способной

причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

2) информирование обучающихся о способах незаконного распространения такой информации в информационно- телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);

3) ознакомление обучающихся с международными принципами и

нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;

4) обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и суицид (доведение до самоубийства путем психологического насилия);

5) предупреждение совершения обучающимися правонарушений с использованием информационно-телекоммуникационных технологий.

В ходе уроков Интернет - безопасности учащиеся должны научиться делать более безопасным и полезным свое время пребывания в сети Интернет и иных информационно-телекоммуникационных сетях, а именно:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;
- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
- распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;
- критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;
- анализировать степень достоверности информации и подлинность ее источников;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

В рамках урока «Интернет-безопасность» в начальных классах целесообразно ознакомить обучающихся:

– с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;

– как критически относиться к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;

– как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывания в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Рекомендуется продемонстрировать возможности детских поисковых систем: *http://kids.quintura.ru*,*http://agakids.ru* и детского браузера *http://www.gogul.tv*, а также познакомить с детскими социальными сетями:*http://cyberpapa.ru/*, *http://interneshka.net/*, *http://kinder-*online.ru/detskiy_portal.html, *http://1dnevnik.ru/*,*http://www.detkino.ru*.

Для отбора содержания урока могут быть использованы материалы сайта *www.detionline.com* (видеоматериалы, материалы электронного журнала Дети в информационном обществе , материалы Линии помощи), а также материалы других сайтов, содержащих информацию по безопасному использованию сети Интернет.

Большое значение для эффективности урока Интернет-безопасности имеет не только содержание, но и форма его проведения. Целесообразно использовать для 2-4 классов – урок-путешествие, урок-викторину, урок-соревнование, урок-игру, беседу.

Полезные ссылки:

- *http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/loputon_metsa.html* – о правилах безопасного поведения в сети Интернет с элементами интерактива;
- *http://www.nachalka.com/node/948* - учебное видео Как обнаружить ложь и остаться правдивым в Интернете ;
- *http://content-filtering.ru/aboutus/* - информационно-аналитический ресурс Ваш личный Интернет.

В ходе урока Интернет-безопасность в среднем звене целесообразно познакомить обучающихся:

- с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве: Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.); № 252-ФЗ О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», (направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить порочные наклонности, сформировать искаженную картину мира и неправильные жизненные установки.)

-ознакомить обучающихся с адресами помощи в случае интернет-угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Возможны следующие формы проведения урока: урок - пресс- конференция, урок-викторина, урок-соревнование, урок-презентация проектов, урок-практикум, урок-встреча с системными администраторами и т.д.

Полезные ссылки:

1) *http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma_ro oma.html* - молодежная история с элементами интерактива;

2) *http://content-filtering.ru/aboutus* - информационно-аналитический ресурс Ваш личный Интернет;

3) *www.icensor.ru* - Интернет-фильтр.

В рамках урока Интернет-безопасность в старших классах целесообразно познакомить обучающихся: с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве (см. рекомендации для проведения урока «Интернет–безопасности» в среднем звене).

Необходимо обратить внимание обучающихся на классификацию вредоносных информационных ресурсов:

- информация, запрещенная для распространения среди детей;

- информация, ограниченная для распространения среди детей определенных возрастных категорий.

На уроке необходимо затронуть следующие аспекты:

- перечень рисков, подстерегающих ребенка в сети Интернет;

- рекомендации по грамотному использованию электронной почты;

- технологии безопасного общения в средах мгновенного обмена

сообщениями;

Необходимо обеспечить обучающихся инструкциями по безопасному общению в чатах; советами по профилактике и преодолению Интернет - зависимости; общими правилами по безопасности детей в сети Интернет.

Также рекомендуется рассмотреть следующие объекты, являющиеся опасными в Интернете: нежелательные программы; защита личных данных; мошенничество; виртуальные "друзья"; пиратство; on-line-игры; этика; критический подход к информации.

Обеспечить обучающихся информацией о программном обеспечении, позволяющим осуществлять безопасную работу в сети Интернет, контентной фильтрации.

Ознакомить обучающихся с адресами помощи в случае интернет-угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Возможные формы проведения урока в 9-11 классах – лекция, деловая игра, урок-презентация проектов, мозговой штурм Интернет-безопасность, дискуссия, дебаты, встреча со специалистами медиа-сферы, системными администраторами и т.д.

Полезные ссылки:

1) *http://www.kaspersky.ru* – антивирус Лаборатория Касперского ;
2) *http://www.onlandia.org.ua/rus/*- безопасная web-зона;
3)*http://www.interneshka.net* международный онлайн-конкурс по безопасному использованию Интернета;
4) *http://www.saferinternet.ru* – портал Российского Оргкомитета по безопасному использованию Интернета;
5) *http://content-filtering.ru* – Интернет СМИ Ваш личный Интернет;
6) *http://www.rgdb.ru* – Российская государственная детская библиотека.

По итогам проведения уроков проводится итоговое анкетирование по теме Безопасный интернет (Приложение 8).

Проведение внеклассного мероприятия
Сказка о золотых правилах безопасности в сети Интернет

Сказку целесообразно подготовить силами обучающихся 5-6 классов и представить ее обучающимся начальной школы.

При разработке сценария внеклассного мероприятия Сказка о золотых правилах безопасности в сети Интернет значимую роль играет сам педагог, так как именно от него зависит своевременность и актуальность представленного материала.

Обсуждение сказки позволит младшим школьникам определить собственную позицию организации работы в сети Интернет.

По окончании внеклассного мероприятия обучающимся раздаются памятки с семью золотыми правилами работы в сети Интернет.

Список используемой литературы

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

2**.** А.Г.Асмолов, А.Л.Семенов, А.Ю.Уваров. Российская школа и новые информационные технологии: взгляд в будущее десятилетие.- М.:, 2010

3. Г.У.Солдатов, М.И.Лебешева. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников?//Журнал «Дети в информационном обществе» - М., 2011, №8 – СС.46-55.

4. Г.У.Солдатов, Е.И.Рассказова. Из-за интернета я не ел и не спал». Зависимость или новый образ жизни?//Журнал «дети в информационном пространстве - М., 2011, №9 – СС. 22-29

5. Г.У.Солдатов, Е.И.Рассказова. Как им помочь. Ребенок к Интернете: запрещать, наблюдать или объяснять?//Журнал «дети в информационном пространстве - М., 2011, №10 – СС. 26-33

6. Интернет-ресурсы:

http://ipk.68edu.ru/docs/bezopasnostdeti/bezopasnyi-internet-dlya-pedagogov.pdf
http://orgpsiholog.ru/pr.bezop.htm
http://gldn.ur.ru/support/security/work/
http://www.kuzbass.net/security.html
http://www.interneshka.net
http://www.saferinternet.ru
http://content-filtering.ru
http://www.pkdb.ru/detyam/gostinaya/web-resursy.html
http://i-deti.org/
http://mvd.ru/userfiles/liflets_k_deti_06.pd
http://ppt4web.ru/informatika/pravila-bezopasnosti-v-internete.html
http://www.myshared.ru/slide/265508/
http://www.kultura.kurganobl.ru/assets/files/pdf_dokument/2013/04-13/Bezop_int.pdf

Приложение 1

Анкета «Осторожно, вирус!»

Что является основным каналом распространения компьютерных вирусов?
1. Веб-страницы

2. Электронная почта

3. Флеш-накопители

Для предотвращения заражения компьютера вирусами следует:
1. Не пользоваться Интернетом

2. Устанавливать и обновлять антивирусные средства

3. Не чихать и не кашлять рядом с компьютером

Если вирус обнаружен, следует:
1. Удалить его и предотвратить дальнейшее заражение

2. Установить какую разновидность имеет вирус

3. Выяснить как он попал на компьютер

Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
1**.** Применение брандмауэра
2. Обновления операционной системы

3. Антивирусная программа

Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
1. Уничтожение компьютерных вирусов

2. Создание и распространение компьютерных вирусов и вредоносных программ.

3. Установка программного обеспечения для защиты компьютера.

Анкета №2 Осторожно, Интернет!

1. Какую информацию нельзя разглашать в Интернете?
1. Свои увлечения

2. Свой псевдоним

3. Домашний адрес

2. Чем опасны социальные сети?
1. Личная информация может быть использована кем угодно в разных целях

2. При просмотре неопознанных ссылок компьютер может быть взломан

3. Все вышеперечисленное верно

3. Виртуальный собеседник предлагает встретиться, как следует поступить?
1. Посоветоваться с родителями и ничего не предпринимать без их согласия.

2. Пойти на встречу одному

3. Пригласить с собой друга

4. Что в Интернете запрещено законом?
1. Размещать информацию о себе

2. Размещать информацию других без их согласия

3. Копировать файлы для личного использования

5. Действуют ли правила этикета в Интернете?
1. Интернет - пространство свободное от правил

2. В особых случаях

3. Да, как и в реальной жизни.

Круглый стол Основы безопасности в сети Интернет
Правила работы в сети Интернет

1. Не входите на незнакомые сайты.

2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.

3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.

4. Никогда не посылайте никому свой пароль.

5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

6. При общении в Интернет не указывать свои личные данные, а использовать псевдоним (ник).

7. Без контроля взрослых ни в коем случае не встречаться с людьми, с которыми познакомились в сети Интернет.

8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.

9. В настоящее время существует множество программ, которые производят фильтрацию содержимого сайтов. Между членами семьи должны быть доверительные отношения, чтобы вместе просматривать содержимое сайтов.

10. Не всей той информации, которая размещена в Интернете, можно верить.

11. Не оставляйте без присмотра компьютер с важными сведениям на экране.

12. Опасайтесь подглядывания через плечо.

13. Не сохраняйте важные сведения на общедоступном компьютере.

Материалы для проведения родительского собрания.

Анкета для родителей

Уважаемые родители! В школе информационные технологии применяются в различных направлениях: учебная деятельность (урочная и внеклассная), воспитательная (классные часы и различные школьные мероприятия), ИКТ являются основой единого информационного пространства школы (администрация школы, учитель, ученик, родитель) - сайт школы, работа "Электронного журнала", учебно-материальная база школы, цифровые образовательные ресурсы и т.п. В том числе, информационные технологии прочно вошли в деятельность и досуг детей. Просим Вас ответить на несколько вопросов. (Все вопросы не являются обязательными для ответа. Если Вы выбираете "другое" - не забудьте поставить напротив галочку).

1. В каком классе учится Ваш ребенок?_____

2. Отношение к внедрению ИТ в образование. Внедрение информационных технологий (ИТ) в образование относится к числу крупномасштабных инноваций, пришедших в российскую школу в последние десятилетия. Среди ИТ, внедряемых в сфере образования, можно выделить следующие: обучающие, тренажеры, справочные, единые информационными образовательные пространства (сайт школы, дистанционное обучение, электронные дневники), техническое обеспечение кабинетов и др.

скорее положительно

скорее отрицательно (не вижу необходимости) Другое:_____

3. Использование информационные технологии в школе

- различные мероприятия с применением информационных технологий (проектная деятельность, уроки, классные часы и родительские собрания)

- урок, с применением новых информационных технологий более

популярен у моего ребенка (более интересен, понятен и т.п. - со слов

ребенка)

- ребенок с интересом и удовольствием выполняет проекты (рефераты, доклады), используя компьютер

- ребенок готовится к уроку, используя компьютер (Интернет, полезные ссылки на сайте школы, рекомендуемые учителем сайты и т.п.)

- классный руководитель проводит родительские собрания с использованием компьютера

Другое: _____

4. Работа "Электронного журнала".

Одной из возможностей ресурса является просмотр на страницах этого ресурса в Интернете оценок учащегося, которые выставляют учителя на уроках и их комментарии, домашнего задания... (пароль доступа индивидуален для каждого пользователя)

- в нашем классе есть "Электронный журнал", его работа очень важна для нас

- в нашем классе есть "Электронный журнал", но в его работе нет необходимости

- возможности "Электронного журнала" очень важные, но в нашем классе он не работает

- в нашем классе он не работает и думаю, что нет в нем необходимости

Другое:_____

5. Посещение Школьного сайта

- часто посещаем (в том числе раздел Новости)

- очень редко посещаем

- не посещаем

Другое:_____

6. Школьный сайт.

Напишите, пожалуйста, что бы Вы хотели бы изменить в работе сайта. Ваши предложения и рекомендации Вы можете написать в этом разделе_____

_____

7. Есть ли у Вас дома компьютер?

- да (один)

- да (несколько)

- нет

Другое:_____

8. Кто пользуется компьютером у Вас дома?

- только родители

- только ребенок

- все члены семьи (родители и дети)

Приложение 3

Примерный список вопросов, которые планируется обсудить на родительском собрании

1. В каком возрасте следует разрешить детям посещение интернета?

2. Следует ли разрешать детям иметь собственные учетные записи электронной почты?

3. Какими внутрисемейными правилами следует руководствоваться при использовании интернета?

4. Как дети могут обезопасить себя при пользовании службами

мгновенных сообщений?

5. Могу ли я ознакомиться с записью разговоров моего ребенка в программе обмена мгновенными сообщениями (MSN Messenger, ICQ, Mail Agent)?

6. Могут ли дети стать интернет-зависимыми?

7. Что должны знать дети о компьютерных вирусах?

8. Как проследить какие сайты посещают дети в интернете?

9. Что следует предпринять, если моего ребенка преследуют в интернете?

10. Помогает ли фильтрующее программное обеспечение?

11. На какие положения политики конфиденциальности детского сайта нужно обращать внимание?

12. Какие угрозы встречаются наиболее часто?

13. Как научить детей отличать правду ото лжи в Интернет?

Рекомендации для родителей (законных представителей) учащихся различных возрастных категорий

Возраст от 7 до 8 лет

Находясь в Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям (законным представителям) особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интеренета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе Windows Vista).

В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок.

Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернет. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку.

Запретить ребенку использовать внешние бесплатные ящики сможет такое программное обеспечение, как Kaspersky Internet Security версии 7.0 со встроенным родительским контролем.

Советы по безопасности в сети Интернет

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

Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый белый список Интернет с помощью средств Родительского контроля. Как это сделать, мы поговорим позднее.

Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

Используйте специальные детские поисковые машины, типа MSN Kids Search (*http://search.msn.com/kids/default.aspx?FORM=YCHM*).

Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.

Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.

Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

Научите детей не загружать файлы, программы или музыку без вашего согласия.

Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.

Подробнее о таких фильтрах

http://www.microsoft.com/rus/athome/security/email/fightspam.mspx

Не разрешайте детям использовать службы мгновенного обмена сообщениями.

В белый список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.

Не делайте табу из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты для взрослых.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах.

Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте

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

Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

Не забывайте беседовать с детьми об их друзьях в Интернет.

Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет.

Позволяйте детям заходить только на сайты из белого списка, который создайте вместе с ними.

Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.

Приучите детей не загружать программы без вашего разрешения.

Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Расскажите детям о порнографии в Интернет.

Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст от 13 до 17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок для взрослых . Девочки предпочитают общаться в чатах, при этом они гораздо боле чувствительны к сексуальным домогательствам в Интернет.

Что посоветовать в этом возрасте?

Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов (черный список), часы работы в Интернет, руководство по общению в Интернет (в том числе в чатах).

Компьютер с подключением к сети Интернет должен находиться в общей комнате.

Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни.

Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

Используйте средства блокирования нежелательного контента, как дополнение к стандартному Родительскому контролю.

Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.

Приучите детей не загружать программы без вашего разрешения.

Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Расскажите детям о порнографии в Интернет.
Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

Приучите себя знакомиться с сайтами, которые посещают подростки.

Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно зако

ПРАВИЛА
использования сети Интернет в МБОУ «Золотковская СОШ»

1. Общие положения

1.1. Настоящие Правила использования сети Интернет в образовательном учреждении (далее – Правила) регулируют условия и порядок использования сети Интернет обучающимися, воспитанниками, педагогическими работниками и другими сотрудниками образовательного учреждения (далее – ОУ).

1.2. Правила имеют статус локального нормативного акта ОУ. Если нормами действующего законодательства РФ предусмотрены иные требования, чем настоящими Правилами, применяются нормы действующего законодательства РФ.

1.3. Использование сети Интернет в ОУ подчинено следующим принципам:

- соответствие образовательным целям;
- способствование гармоничному формированию и развитию личности;
- уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернет;
- приобретение новых навыков и знаний;
- расширение применяемого спектра учебных и наглядных пособий;
- социализация личности, введение в информационное общество.

2. Политика использования сети Интернет в ОУ

2.1. Использование сети Интернет в ОУ возможно исключительно при условии ознакомления и согласия лица, пользующегося сетью Интернет в ОУ, с настоящими Правилами.

2.2. Ознакомление и согласие удостоверяются подписью лица в листе ознакомления и согласия с Правилами. Ознакомление и согласие несовершеннолетнего удостоверяются, помимо его подписи, также подписью его родителя (законного представителя).

2.3. Руководитель ОУ является ответственным за обеспечение эффективного и безопасного доступа к сети Интернет, а также за внедрение соответствующих технических, правовых и др. механизмов в ОУ.

2.4. Непосредственное определение политики доступа в Интернет осуществляет общественный совет ОУ, состоящий из представителей педагогического коллектива, работников ОУ, профсоюзной организации (если таковая имеется), родительского комитета и ученического самоуправления.

2.5. Очередные собрания общественного совета ОУ проходят с периодичностью, установленной общественным советом.

Общественный совет ОУ:

- принимает решение о разрешении/блокировании доступа к определенным ресурсам и/или категориям ресурсов сети Интернет, содержащим информацию, не совместимую с задачами образовательного процесса, с учетом социокультурных особенностей региона;
- определяет характер и объем информации, публикуемой на интернет-ресурсах ОУ;
- дает руководителю ОУ рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за непосредственный контроль безопасности работы в сети Интернет и соответствия ее целям и задачам образовательного процесса.

2.6. Во время занятий контроль за использованием обучающимися, воспитанниками сети Интернет в соответствии с Правилами осуществляет педагог, ведущий занятие.

Педагог:

- наблюдает за использованием компьютера и сети Интернет обучающимися, воспитанниками;
- запрещает дальнейшую работу обучающегося, воспитанника в сети Интернет в случае нарушения настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в ОУ;
- принимает предусмотренные Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, не совместимых с задачами образования.

2.7. Во время использования сети Интернет для свободной работы контроль осуществляет лицо, уполномоченное общественным советом ОУ (далее – уполномоченное лицо).

Уполномоченное лицо:

определяет время и место для свободной работы в сети Интернет обучающихся, педагогических и других работников ОУ с учетом использования соответствующих технических мощностей ОУ в образовательном процессе, а также длительность сеанса работы одного человека;

наблюдает за использованием компьютера и сети Интернет обучающимися;

запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в ОУ;

не допускает обучающегося к работе в сети Интернет в предусмотренных Правилами случаях;

принимает предусмотренные Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, не совместимых с задачами образования.

2.8. При использовании сети Интернет в ОУ осуществляется доступ только к ресурсам, содержание которых не противоречит законодательству РФ и не является несовместимым с целями и задачами образования и воспитания. Проверка такого соответствия осуществляется с помощью специальных технических средств и программного обеспечения контекстного ограничения доступа, установленного в ОУ или предоставленного оператором услуг связи*. [* Пользователи сети Интернет в ОУ должны понимать, что технические средства и программное обеспечение не могут осуществлять полную фильтрацию ресурсов сети Интернет в связи с частотой обновления ресурсов и осознавать возможную опасность столкновения с ресурсом, содержание которого противоречит законодательству РФ и является несовместимым с целями и задачами образовательного процесса.]
Использование сети Интернет в ОУ без применения данных технических средств и программного обеспечения (например, в случае технического отказа) допускается только с индивидуального разрешения руководителя ОУ.

2.9. Решение о политике доступа к ресурсам/группам ресурсов сети Интернет принимает общественный совет ОУ самостоятельно либо с участием внешних экспертов, в качестве которых могут привлекаться:

педагогические работники ОУ и других учреждений;

лица, имеющие специальные знания либо опыт работы в рассматриваемой области;

представители органов управления образованием;

родители обучающихся, воспитанников.

При принятии решения общественный совет ОУ, эксперты руководствуются:

законодательством РФ;

специальными знаниями, в т. ч. полученными в результате профессиональной деятельности;

опытом организации образовательного процесса с использованием информационных технологий и возможностей сети Интернет;

интересами обучающихся, воспитанников, целями образовательного процесса;

рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

2.10. Отнесение определенных категорий и/или ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контекстного технического ограничения доступа к информации, технически осуществляется лицом, уполномоченным руководителем ОУ по представлению общественного совета ОУ.

2.11. Категории ресурсов, в соответствии с которыми определяется политика использования сети Интернет в ОУ и доступ к которым регулируется техническими средствами и программным обеспечением контекстного технического ограничения доступа к информации, определяются в установленном порядке.

2.12. Принципами размещения информации на интернет-ресурсах ОУ являются:

 соблюдение действующего законодательства РФ, интересов и прав граждан;

 защита персональных данных обучающихся, воспитанников, педагогических работников и других

сотрудников ОУ;

 достоверность и корректность информации.

2.13. Персональные данные об обучающихся, воспитанниках (фамилия и имя, класс или группа, возраст, фотография, место жительства, телефоны и др. контакты, иные сведения личного характера) могут размещаться на интернет-ресурсах ОУ только с письменного согласия родителей (законных представителей). Персональные данные педагогических работников и других сотрудников ОУ размещаются на интернет-ресурсах ОУ только с письменного согласия работника, чьи персональные данные размещаются.
В информационных сообщениях о мероприятиях на сайте ОУ и его подразделений без согласия лица (законного представителя) могут быть упомянуты только его фамилия и имя.
При истребовании согласия представитель ОУ и/или общественного совета ОУ разъясняет лицу возможные риски и последствия опубликования персональных данных. ОУ не несет ответственности в случае наступления таких

последствий, если имелось письменное согласие лица (законного представителя) на опубликование персональных данных.

3. Процедура использования сети Интернет

3.1. Использование сети Интернет в ОУ осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области сети Интернет и компьютерной грамотности лицо может осуществлять доступ к ресурсам необразовательной направленности.

3.2. По разрешению уполномоченного лица обучающиеся (с согласия родителей, законных представителей), педагогические работники и другие сотрудники вправе:

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

3.3. Обучающемуся запрещается:

- находиться на ресурсах, содержание и тематика которых является недопустимой для несовершеннолетних и/или нарушающей законодательство РФ (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 загрузку файлов на компьютер ОУ без разрешения уполномоченного лица;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.4. Уполномоченное лицо проверяет, отстранен ли обучающийся от самостоятельной работы в сети Интернет.

3.5. При случайном обнаружении лицом, работающим в сети Интернет, ресурса, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить о нем уполномоченному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

3.6. Уполномоченное лицо обязано:

- принять сообщение лица, работающего в сети Интернет;
- довести информацию до сведения общественного совета ОУ для оценки ресурса и принятия решения по политике доступа к нему;
- направить в течение суток информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения технического ограничения доступа к информации;
- если обнаруженный ресурс явно нарушает законодательство РФ – сообщить о нем в течение суток по специальной “горячей линии” для принятия мер в соответствии с законодательством РФ.

Передаваемая информация должна содержать:

- интернет-адрес (URL) ресурса;
- тематику ресурса, предположения о нарушении ресурсом законодательства РФ либо несовместимости с задачами образовательного процесса;
- дату и время обнаружения;
- информацию об установленных в ОУ технических средствах технического ограничения доступа к информации.

Правила доступа работников и обучающихся

МБОУ «Золотковская СОШ» в сеть Интернет

1. Общие положения

Обучающимся и работникам школы (Пользователь) предоставляется право бесплатного доступа в Интернет в кабинете информатики (№ 27), учительской в урочное и внеурочное время с 9.00 до 17.00.

Учащиеся имеют право выхода в Интернет только с разрешения и в присутствии учителя-предметника, классного руководителя или учителя информатики.

В специальном журнале Пользователь регистрируется (обучающихся регистрирует учитель, в присутствии которого они выходят в Интернет) – указывает дату выхода в Интернет, ФИО, должность, названия и адреса сайтов. Наличие журналов в кабинете информатики обеспечивает заведующий кабинетом, в учительской – заместитель директора по УВР.

2. Пользователю Интернет разрешается:

- использовать оборудование для работы с информационными ресурсами и электронной почтой в образовательных целях или для осуществления научных изысканий, выполнения проектов;

- переписывать полученную информацию на собственные электронные носители.

3. Пользователю запрещается:

- передавать внешним пользователям информацию, представляющую коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство, безопасность граждан;

- работать с объемными ресурсами (video, audio, chat, игры) без согласования с учителем информатики;

- доступ к сайтам, содержащим информацию, несовместимую с задачами обучения или противоречащую общепринятой этике;

- устанавливать новое и вносить какие-либо изменения в существующее программное обеспечение на компьютерах;

- использовать оборудования в коммерческих целях.

4. Пользователь обязан:

- предварительно проверять носители информации на наличие вирусов;

- соблюдать правила техники безопасности (ИОТ – 015 – 2011 «Инструкция по охране труда для пользователей и операторов ЭВМ»; ИОТ – 014– 2011 «Инструкция по охране труда при работе в кабинете информатики»);

- сохранять оборудование в целости и сохранности.

Должностная инструкция
ответственного за организацию работы с Интернетом и ограничение доступа
в МБОУ «Золотковская СОШ»

1.Общие положения

Ответственный за организацию работы с Интернетом и ограничение доступа назначается на должность и освобождается от должности директором школы.

Ответственный за организацию работы с Интернетом и ограничение доступа подчиняется непосредственно директору.

Ответственный за организацию работы с Интернетом и ограничение доступа руководствуется в своей деятельности Конституцией и законами РФ, государственными нормативными актами органов управления образования всех уровней; Правилами и нормами охраны труда, техники безопасности и противопожарной защиты; Уставом и локальными правовыми актами школы, а также настоящей должностной инструкцией.

2.Основные задачи и обязанности

Ответственный за работу «точки доступа к Интернету» в школе обеспечивает доступ сотрудников школы и учащихся к Интернету, а именно:

Разрабатывает, согласует с педагогическим коллективом, представляет на педагогическом совете образовательного учреждения регламент использования сети Интернет в образовательном учреждении, включая регламент определения доступа к ресурсам сети Интернет;

Следит за состоянием компьютерной техники и Интернет-канала. В случае необходимости инициирует обращение в ремонтную (сервисную) организацию или поставщику Интернет-услуг. Осуществляет контроль ремонтных работ.

Планирует использование ресурсов сети Интернет в образовательном учреждении на основании заявок преподавателей и других работников образовательного учреждения;

Осуществляет регистрацию пользователей сети Интернет в специальном журнале. В случае необходимости лимитирует время работы в Интернете пользователя.

Оказывает помощь пользователям во время сеансов работы в сети.

Участвует в организации повышения квалификации сотрудников школы по использованию Интернета в профессиональной деятельности.

Организует оформление стендов наглядными материалами по тематике Интернета: советами по работе с программным обеспечением (браузером, электронной почтой), обзорами интересных Интернет-ресурсов, новостями педагогического Интернет-сообщества и т.п.

Организует получение сотрудниками образовательного учреждения электронных адресов и паролей для работы в сети Интернет и информационной среде образовательного учреждения;

Организует контроль использования сети Интернет в образовательном учреждении;

Организует контроль работы оборудования и программных средств, обеспечивающих использование сети Интернет и ограничение доступа;

Осуществляет регулярное обновление антивирусного программного обеспечения. Контролирует проверку пользователями внешних электронных носителей информации (дискет, CD-ROM, флеш-накопителей) на отсутствие вирусов.

Следит за приходящей корреспонденцией на школьный адрес электронной почты.

Принимает участие в создании (и актуализации) школьной веб-страницы.

Систематически повышает свою профессиональную квалификацию, общепедагогическую и предметную компетентность, включая ИКТ-компетентность, компетентность в использовании возможностей Интернета в учебном процессе;

Обеспечивает информирование организаций, отвечающих за работу технических и программных средств, об ошибках в работе оборудования и программного обеспечения;

Соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети Интернет.

3.Права

Ответственный за работу «точки доступа к Интернету» в школе имеет право:

Отдавать распоряжения пользователям «точки доступа к Интернету» в рамках своей компетенции.

Ставить вопрос перед директором школы о нарушении пользователями «точки доступа к Интернету» правил техники безопасности, противопожарной безопасности, поведения, регламента работы в Интернете.

4.Ответственность

Ответственный за работу «точки доступа к Интернету» в школе несет полную ответственность за:

Надлежащее и своевременное выполнение обязанностей, возложенных на него настоящей должностной инструкцией.

Соблюдение Правил техники безопасности, противопожарной безопасности и норм охраны труда в школе.

РЕГЛАМЕНТ
по работе учителей и учащихся МКОУ «Золотковская СОШ» в сети Интернет

I. Общие положения

«Точка доступа» к сети Интернет предназначена для обслуживания учителей и учеников школы. Сотрудники и учащиеся школы допускаются к работе на бесплатной основе.

К работе в Интернет допускаются пользователи, прошедшие предварительную регистрацию у администраторов соответствующих локальных сетей.

Выход в Интернет осуществляется с 800 до 1900 (кроме воскресенья). Последняя пятница месяца – день профилактики.

Предоставление сеанса работы в Интернет осуществляется, как правило через прокси-сервер, на основании предварительной записи в журнале администратора соответствующей локальной сети или при наличии свободных мест в зависимости от категории пользователя:

- учащимся предоставляется доступ в компьютерных классах согласно расписанию занятий (график работы компьютерных классов составляется на основании ежемесячно подаваемых служебных записок на имя заместителя директора по ИКТ с приложением расписания занятий и учебных планов);
- учителям предоставляется доступ согласно ежемесячно подаваемым служебным запискам на имя заместителя директора по ИКТ (выдается регистрационное имя, пароль и график работы), но не менее 2 часов в неделю. Этот ресурс может делиться на кванты времени, равные не менее 30 минутам;
- остальным пользователям предоставляется доступ при наличии резерва пропускной способности канала передачи.

Для работы в Интернет необходимо иметь при себе документ, удостоверяющий личность пользователя (пропуск учащегося, пропуск учителя или регистрационные карточки с логином и паролем).

По всем вопросам, связанным с доступом в Интернет, следует обращаться к администраторам соответствующих локальных сетей.

II. Правила работы

При входе в зал, необходимо обратиться к администратору зала за разрешением для работы в зале. При наличии свободных мест, после регистрации в журнале учета, посетителю предоставляется в зале рабочая станция. Для доступа в Интернет и использования электронной почты установлен программный продукт "Internet Explorer", «Outlook Express». Отправка электронной почты с присоединенной к письму информацией, запись информации на дискеты и CD-диски осуществляется у администратора. Дополнительно установлено программное обеспечение: текстовые редакторы семейства "Microsoft Office".

- Пользователь обязан выполнять все требования администратора.
- В начале работы пользователь обязан зарегистрироваться в системе, т.е. ввести свое имя регистрации (логин) и пароль.
- За одним рабочим местом должно находиться не более одного пользователя.
- Запрещается работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одной рабочей станции.
- Каждому пользователю, при наличии технической возможности, предоставляется персональный каталог, предназначенный для хранения личных файлов общим объемом не более 5 Мб, а также возможность работы с почтовым ящиком для отправки и получения электронной почты.
- Пользователю разрешается записывать полученную информацию на личные дискеты. Дискеты должны предварительно проверяться на наличие вирусов. Запрещается любое копирование с дискет на жесткие диски.
- Пользователю запрещено вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах, а также производить запись на жесткий диск рабочей станции.
- 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.
- Запрещена передача информации, представляющую коммерческую или государственную тайну, распространение информации, порочащей честь и достоинство граждан.
- Запрещается работать с объемными ресурсами (video, audio, chat, игры и др.) без согласования с администратором.
- Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.
- Пользователь обязан сохранять оборудование в целости и сохранности.
- Пользователь обязан помнить свой пароль. В случае утраты пароля пользователь обязан сообщить системному администратору.

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 получает первое предупреждение и лишается права выхода в Интернет сроком на 1 месяц. При повторном административном нарушении – пользователь лишается доступа в Интернет.

При возникновении технических проблем пользователь обязан поставить в известность администратора локальной сети.

III. Правила регистрации

Для доступа в Интернет пользователей необходимо пройти процесс регистрации.

- Регистрационные логин и пароль учащиеся получают у заместителя директора по ИКТ через своего классного руководителя или учителя информатики.
- Регистрационные логин и пароль учителя получают у заместителя директора по ИКТ при предъявлении удостоверения личности и письменного заявления.
- После ввода сетевого имени и пароля пользователь получает либо сообщение об ошибке (тогда ее необходимо исправить) либо доступ.
- Перед работой необходимо ознакомиться с "Памяткой" и расписаться в журнале учета работы в Интернет, который хранится у администратора.

IV. Памятка

по использованию ресурсов сети Интернет

- Пользователь обязан выполнять все требования администратора локальной сети.
- В начале работы пользователь обязан зарегистрироваться в системе, т.е. ввести свое имя регистрации и пароль. После окончания работы необходимо завершить свой сеанс работы, вызвав в меню «Пуск» команду «Завершение сеанса <имя>» либо в меню «Пуск» команду «Завершение работы» и «Войти в систему под другим именем».
- За одним рабочим местом должно находиться не более одного пользователя.
- Запрещается работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одной рабочей станции.
- Каждый пользователь при наличии технической возможности может иметь персональный каталог, предназначенный для хранения личных файлов общим объемом не более 5 Мб. Аналогично может быть предоставлена возможность работы с почтовым ящиком. При возникновении проблем необходимо обратиться к дежурному администратору.
- Пользователю разрешается переписывать полученную информацию на личные дискеты. Дискеты предварительно проверяются на наличие вирусов.
- 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.
- 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.
- Запрещается работать с объемными ресурсами (video, audio, chat, игры) без согласования с администратором.
- Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.
- Пользователю запрещено вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах, а также производить запись на жесткий диск рабочей станции. Запрещается перегружать компьютер без согласования с администратором локальной сети.
- Пользователь обязан сохранять оборудование в целости и сохранности.

При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность. В случае нарушения правил работы пользователь лишается доступа в сеть. За административное нарушение, не влекущее за собой порчу имущества, вывод оборудования из рабочего состояния и не противоречащие принятым правилам работы пользователь получает первое предупреждение. При повторном административном нарушении - пользователь лишается доступа в Интернет без права восстановления.

При возникновении технических проблем пользователь обязан поставить в известность администратора локальной сети.

Инструкция пользователя по безопасной работе в сети Интернет

В МБОУ «Золотковская СОШ»

Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью школы и предоставляются учащимся и учителям.
ПК, серверы, ПО, оборудование ЛВС и коммуникационное, пользователи образуют систему локальной сети, сети Wi-Fi МКОУ «Золотковская СОШ»

Общие положения:

1.1. Настоящая инструкция является дополнением к Положению о политике информационной безопасности корпоративной сети фирмы далее СЕТИ.

1.2. Целью настоящей инструкции является регулирование работы системных администраторов и пользователей, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации. Более эффективного использования сетевых ресурсов и уменьшить риск умышленного или неумышленного неправильного их использования.

1.3. К работе в системе допускаются лица, назначенные начальником соответствующего отдела и прошедшие инструктаж и регистрацию у ответственного за работу в сети Интернет.

1.4. Работа в системе каждому работнику разрешена только на определенных компьютерах, в определенное время и только с разрешенными программами и сетевыми ресурсами. Если нужно работать вне указанного времени, на других компьютерах и с другими программами, необходимо получить разрешение системного администратора.

1.5. По уровню ответственности и правам доступа к СЕТИ пользователи СЕТИ разделяются на следующие категории: системные администраторы и пользователи.

1.6. Пользователь подключенного к СЕТИ компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

1.7. Каждый сотрудник пользуется индивидуальным именем пользователя для своей идентификации в сети, выдаваемым системным администратором.

1.8 Каждый сотрудник САМ создает пароль для входа в компьютерную сеть. При этом пароль должен содержать не менее 8 символов и состоять из букв и цифр.

1.9. Каждый сотрудник должен пользоваться только своим именем пользователя и паролем для входа в локальную сеть и сеть Интернет, передача их кому-либо запрещена.

1.10. Для работы на компьютере кроме пользователя необходимо разрешение системного администратора. Никто не может давать разрешение на даже временную работу на компьютере, без разрешения системного администратора или начальника ИТО.

1.11. В случае нарушения правил пользования сетью, связанных с администрируемым им компьютером, пользователь сообщает системному администратору, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений. Если виновником нарушения является пользователь данного компьютера, администратор имеет право отстранить виновника от пользования компьютером или принять иные меры.

1.12. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере ли каком-либо другом, пользователь должен немедленно сообщить об этом системному администратору СЕТИ.

1.13. Системный администратор и лицо, обслуживающее сервер и следящее за правильным функционированием СЕТИ. Системный администратор дает разрешение на подключение компьютера к СЕТИ, выдает IP-адрес компьютеру, создает учетную запись электронной почты для пользователя. Самовольное подключение является серьезнейшим нарушением правил пользования СЕТЬЮ.

1.14. Системный администратор информирует пользователей обо всех плановых профилактических работах, могущих привести к частичной или полной неработоспособности СЕТИ на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам СЕТИ.

1.15. Системный администратор имеет право отключить компьютер пользователя от СЕТИ в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящей инструкции.

1.16. Пользователь должен ознакомиться с настоящей инструкцией. Обязанность ознакомления пользователя с инструкцией лежит на системном администраторе и начальнике отдела ИТО.

2. Пользователи СЕТИ обязаны:

2.1. Соблюдать правила работы в СЕТИ, оговоренные настоящей инструкцией.

2.2. При доступе к внешним ресурсам СЕТИ, соблюдать правила, установленные системными администраторами для используемых ресурсов.

2.3. Немедленно сообщать системному администратору СЕТИ или начальнику отдела ИТО об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо. Администраторы, при необходимости, с помощью других специалистов, должны провести расследование указанных фактов и принять соответствующие меры.

2.4. Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в СЕТИ.

2.5. Немедленно отключать от СЕТИ компьютер, который подозревается в заражении вирусом. Компьютер не должен подключаться к СЕТИ до тех пор, пока системные администраторы не удостоверятся в удалении вируса.

2.6. Обеспечивать беспрепятственный доступ специалистам отдела ИТО к сетевому оборудованию и компьютерам пользователей.

2.7. Выполнять предписания специалистов отдела ИТО, направленные на обеспечение безопасности СЕТИ.

2.8. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к системному администратору или начальнику отдела ИТО.

3. Пользователи СЕТИ имеют право:

3.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках, если иное не предусмотрено по согласованию с отделом ИТО. Системные администраторы вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов.

3.2. Обращаться к администратору СЕТИ по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы (например, установка на компьютере коллективного доступа), должны санкционироваться системным администратором СЕТИ.

3.3. Обращаться за помощью к системному администратору при решении задач использования ресурсов СЕТИ.

3.4. Вносить предложения по улучшению работы с ресурсом.

4. Пользователям СЕТИ запрещено:

4.1. Разрешать посторонним лицам пользоваться вверенным им компьютером (кроме случаев подключения/отключения ресурсов, выполняемого специалистами ИТО).

4.2. Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования со специалистами ИТО.

4.3. Самостоятельно устанавливать или удалять установленные системным администратором сетевые программы на компьютерах, подключенных к СЕТИ, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов.

4.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

4.5. Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без ведома системного администратора, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет.

4.6. Самовольно подключать компьютер к СЕТИ, а также изменять IP-адрес компьютера, выданный системным администратором. Передача данных в сеть с использованием других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах.

4.7. Работать с каналоемкими ресурсами (real video, real audio, chat и др.) без согласования с системным администратором СЕТИ. При сильной перегрузке канала вследствие использования каналоемких ресурсов текущий сеанс пользователя, вызвавшего перегрузку, будет прекращен.

4.8. Получать и передавать в сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую или государственную тайну, распространять через сеть информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.

4.9. Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация.

4.10. Использовать иные формы доступа к сети Интернет, за исключением разрешенных системным администратором: пытаться обходить установленный отделом ИТО межсетевой экран при соединении с сетью Интернет.

4.11. Осуществлять попытки несанкционированного доступа к ресурсам СЕТИ, проводить или участвовать в сетевых атаках и сетевом взломе.

4.12. Использовать СЕТЬ для совершения коммерческих сделок, распространения рекламы, коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

4.13. Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь (системный администратор) не имеет права пользоваться чужими именами и паролями для входа в сеть, читать чужую почту, причинять вред данным (кроме случаев, указанных выше), принадлежащих другим пользователям.

4.14. Запрещается производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и сервера Сети, равно как и любых других компьютеров в Интернет.

4.15. Закрывать доступ к информации паролями без согласования с системным администратором.

5. Работа с электронной почтой:

5.1. Электронная почта предоставляется сотрудникам организации только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.

5.2. Все электронные письма, создаваемые и хранимые на компьютерах организации, являются собственностью организации и не считаются персональными.

5.3. Организация оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.

5.4. Конфигурировать программы электронной почты так, чтобы стандартные действия пользователя, использующие установки по умолчанию, были бы наиболее безопасными.

5.5. Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.

5.6. Почтовые сервера должны быть сконфигурированы так, чтобы отвергать письма, адресованные не на компьютеры организации.

5.7. Журналы почтовых серверов должны проверяться на предмет выявления использования неутвержденных почтовых клиентов сотрудниками организации, и о таких случаях должно докладываться.

5.8. Почтовые клиенты должны быть сконфигурированы так, чтобы каждое сообщение подписывалось с помощью цифровой подписи отправителя.

5.9. Необходимо организовать обучение пользователейправильной работе с электронной почтой.

5.10. Справочники электронных адресов сотрудников не могут быть доступны всем и являются конфиденциальной информацией.

5.11. Если с помощью электронного письма должна быть послана конфиденциальная информация или информация, являющаяся собственностью организации, она должна быть зашифрована так, чтобы ее мог прочитать только тот, кому она предназначена, с использованием утвержденных в организации программ и алгоритмов.

5.12. Никто из посетителей, контрактников или временных служащих не имеет права использовать электронную почту организации.

5.13. Вся информация, классифицированная как критическая или коммерческая тайна, при передаче ее через открытые сети, такие как Интернет, Должна быть предварительно зашифрована.

5.14. Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности фирмы.

5.15. Пользователи не должны позволять кому-либо посылать письма от чужого имени. Это касается их начальников, секретарей, ассистентов или других сослуживцев.

5.16. Организация оставляет за собой право осуществлять наблюдение за почтовыми отправлениями сотрудников. Электронные письма могут быть прочитаны организацией, даже если они были удалены и отправителем, и получателем. Такие сообщения могут использоваться для обоснования наказания.

5.17. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы.

5.18. Конфиденциальная информация не может быть послана с помощью электронной почты.

5.19. Если будет установлено, что сотрудник неправильно использует электронную почту с умыслом, он будет наказан.

5.20. Нельзя сообщать сторонним лицам электронные адреса фирмы.

5.21. Открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем.

5.22. Осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

5.23. Использовать несуществующие обратные адреса при отправке электронных писем.

6. При работе с веб-ресурсами:

6.1. Пользователи используют программы для поиска информации в WWW только в случае, если это необходимо для выполнения своих должностных обязанностей.

6.2. Использование ресурсы сети Интернет разрешается только в рабочих целях, использование её ресурсов не должно потенциально угрожать Фирме.

6.3. По использованию Интернет ведется статистика и поступает в архив фирмы.

6.4. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему в санкций.

6.5. Сотрудникам организации, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским и не относящимся к деятельности Фирмы.

6.6. Все программы, используемые для доступа к сети Internet, должны быть утверждены сетевым администратором и на них должны быть настроены необходимые уровни безопасности.

6.7. Все файлы, загружаемые с помощью сети Internet, должны проверяться на вирусы с помощью утвержденных руководством антивирусных программ.

6.8. Сотрудники, нанятые по контракту, должны соблюдать эту политику после предоставления им доступа к Internet. Доступ к сети Internet предоставляется по служебной записке.

6.9. В организации должен вестись список запрещенных сайтов. Программы для работы с Internet должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.

6.10. Запрещено размещать в гостевых книгах, форумах, конференциях сообщения, содержащие грубые и оскорбительные выражения.

6.11. Запрещено получать и передавать через СЕТЬ информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.

6.12. Запрещено получать доступ к информационным ресурсам СЕТИ или сети Интернет, не являющихся публичными, без разрешения их собственника.

7. Ответственность:

7.1. Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.

7.2. Системный администратор отвечает за бесперебойное функционирование вверенной ему СЕТИ, качество предоставляемых пользователям сервисов.

7.3. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в СЕТИ и за ее пределами.

7.4. За нарушение настоящей инструкции пользователь может быть отстранен от работы с СЕТЬЮ.

7.5. Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей, системы или СЕТИ компьютеров, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством.

КЛАССИФИКАТОР

информации, доступ к которой учащихся запрещен и разрешен

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 свободой СМИ /экстремизм:
информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы.

3. Злоупотребление свободой СМИ / наркотические средства:
сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганду каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров.

4. Злоупотребление свободой СМИ / информация с ограниченным доступом:
сведения о специальных средствах, технических приемах и тактике проведения контртеррористической операции.

5. Злоупотребление свободой СМИ / скрытое воздействие :
информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающих вредное влияние на их здоровье.

6. Экстремистские материалы или экстремистская деятельность (экстремизм):
А) экстремистские материалы, т.е. предназначенные для обнародования документы либо информация, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии, публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы;
Б) экстремистская деятельность (экстремизм) включает в себя деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков:
- насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации;
- подрыв безопасности Российской Федерации;
- захват или присвоение властных полномочий;
- создание незаконных вооруженных формирований;
- осуществление террористической деятельности либо публичное оправдание терроризма;
- возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию;
- унижение национального достоинства;
- осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы;
- пропаганду исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности;
- воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, соединенное с насилием или угрозой его применения;
- публичную клевету в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, соединенную с обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке;
- применение насилия в отношении представителя государственной власти либо на угрозу применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей;
- посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность;
- нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением.

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

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

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

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

Классификатор информации,
несовместимой с задачами образования.

1. Алкоголь:
Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию.

2. Баннеры и рекламные программы:
Баннерные сети, всплывающая реклама, рекламные программы.

3. Вождение и автомобили:
(ресурсы данной категории, несовместимые с задачами образования)
Несовместимая с задачами образования информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям.

4. Досуг и развлечения:
(ресурсы данной категории, несовместимые с задачами образования)
Несовместимая с задачами образования информация в виде фотоальбомов и рейтингов фотографий, открыток, гороскопов, сонников, гаданий, магии, астрологии, ТВ-программ, прогнозов погоды, тестов, рейтингов, фотоконкурсов, конкурсов онлайн, несовместимая с задачами образования информация о туризме, путешествиях, тостах, поздравлениях, кроссвордах, сканвордах, ответов к ним, фэнтези и фантастике, кулинарии, рецептах, диетах, моде, одежде, обуви, модных аксессуарах, показах мод, текстах песен, кино, киноактерах, расписаниях концертов, спектаклей, кинофильмов, заказе билетов в театры, кино и т.п., дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними, рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании, службах знакомств, размещении объявлений онлайн, анекдотах, приколах, слухах, сайтах и журналы для женщин и для мужчин, желтая пресса, онлайн-ТВ, онлайн радио, знаменитости, косметика, парфюмерия, прически, ювелирные украшения.

5. Здоровье и медицина:
(ресурсы данной категории, несовместимые с задачами образования)
Несовместимая с задачами образования информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иных материалах по теме «Здоровье и медицина», которые, являясь академическими, по сути, могут быть также отнесены к другим категориям, например, порнография, трупы и т.п.

6. Компьютерные игры:
(ресурсы данной категории, несовместимые с задачами образования).
Несовместимая с задачами образования компьютерные 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, несовместимые с задачами образования)
Содержащие несовместимую с задачами образования информацию сайты коммерческих фирм, компаний, предприятий, организаций.

8. Личная и немодерируемая информация:
Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники (блоги).

9. Отправка SMS с использованием Интернет-ресурсов. Сайты, предлагающие услуги по отправке SMS-сообщений.

10. Модерируемые доски объявлений:
(ресурсы данной категории, несовместимые с задачами образования)
Содержащие несовместимую с задачами образования информацию модерируемые доски сообщений/объявлений, а также модерируемые чаты.

11. Нелегальная помощь школьникам и студентам:
Банки готовых рефератов, эссе, дипломных работ и проч.

12. Неприличный и грубый юмор :
Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека.
13. Нижнее белье, купальники:
Сайты, на которых рекламируется и изображается нижнее белье и купальники.
14. Обеспечение анонимности пользователя, обход контентных фильтров :
Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам. Peer — to- Peer программы, сервисы бесплатных прокси — серверов, сервисы, дающие пользователю анонимность
15. Онлайн — казино и тотализаторы:
Электронные казино, тотализаторы, игры на деньги, конкурсы и проч.
16. Платные сайты:
Сайты, на которых вывешено объявление о платности посещения веб-страниц.
17.Поиск работы, резюме, вакансии:
(ресурсы данной категории, несовместимые с задачами образования)
Содержащие несовместимую с задачами образования Интернет-представительства кадровых агентств, банки вакансий и резюме.
18.Поисковые системы :
(ресурсы данной категории, несовместимые с задачами образования)
Содержащие несовместимую с задачами образования Интернет-каталоги, системы поиска и навигации в сети Интернет.
19.Религии и атеизм:
(ресурсы данной категории, несовместимые с задачами образования)
Сайты, содержащие несовместимую с задачами образования информацию религиозной направленности
20. Системы поиска изображений
Системы для поиска изображений в сети Интернет по ключевому слову или словосочетанию.
21. СМИ:
(ресурсы данной категории, несовместимые с задачами образования)
Содержащие несовместимую с задачами образования информацию новостные ресурсы и сайты СМИ (радио, телевидения, печати)
22. Табак, реклама табака, пропаганда потребления табака :
Сайты, пропагандирующие потребление табака. Реклама табака и изделий из него.
23. Торговля и реклама:
(ресурсы данной категории, несовместимые с задачами образования)
Содержащие несовместимую с задачами образования информацию сайты следующих категорий: аукционы, распродажи онлайн, Интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, недвижимость, аренда недвижимости, покупка недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в сети Интернет, е-бизнес
24.Убийства, насилие:
Сайты, содержащие описания или изображения убийств, мертвых тел, насилия и т. п. Сайты, пропагандирующие жестокое обращение с животными.
25. Чаты:
(ресурсы данной категории, несовместимые с задачами образования).
Несовместимые с задачами образования сайты для анонимного общения в режиме онлайн.
26. Здоровье:
(ресурсы данной категории, несовместимые с задачами образования)
Сайты, чаты, форумы секс меньшинств
27. Экология:
(ресурсы данной категории, несовместимые с задачами образования)
Сайты, призывающие к нанесению ущерба экологии, загрязнению окружающей среды и т. п.
28. Сбор средств через Интернет :
Сайты с информацией для сбора материальных средств в пользу политических партий, религиозных, общественных организаций политической, коммерческой направленности, сект и т. п.
29. Пропаганда войны:
(ресурсы данной категории, несовместимые с задачами образования)
Сайты, рекрутирующие в организации военизированного толка, а также, могущие содержать информацию об изготовлении оружия в домашних условиях и т.п.

Контроль использования учащимися сети Интернет осуществляется с помощью программно-технических средств и визуального контроля.

Ведется журнал учета работы в Интернет.

Контроль за учащимися сети Интернет осуществляют

1) во время проведения занятий – преподаватель, проводящий занятие;

2) во время использования сети Интернет для свободной работы учащихся — лицо, назначенное приказом директора школы по вопросам регламентации доступа к информации в Интернете.